Juni 2017

Risicomanagement bij fondsenwervende instellingen

Jaco de Vos

JUNI 2017

Risicomanagement bij fondsenwervende instellingen

"All courses of action are risky, so prudence is not in avoiding danger (it's impossible), but calculating risk and acting decisively. Make mistakes of ambition and not mistakes of sloth. Develop the strength to do bold things, not the strength to suffer."(Niccolò Machiavelli)

Naam:	Jaco de Vos
Studie:	Accountancy duaal
School:	Avans Hogeschool Breda
Studentennummer:	2083933
Datum:	Juni 2017
Begeleider:	Drs. A.A.F. Kemps
Opdrachtgever:	WITh Accountants B.V.

Voorwoord

Na een half jaar hard werken is de scriptie eindelijk afgerond. Voor u ligt de scriptie 'Risicomanagement bij fondsenwervende instellingen'. De scriptie is een onderdeel van de afronding van mijn opleiding Accountancy Duaal aan de Avans Hogeschool Breda en is gebeurd in opdracht van WITh Accountants B.V.

In de zomer heb ik samen met mijn begeleider vanuit WITh Accountants B.V. een aantal onderwerpen doorgenomen die interessant zouden kunnen zijn voor een scriptie, hieruit is het onderwerp 'Risicomanagement bij fondsenwervende instellingen' naar voren gekomen. Het hiervoor uitgevoerde literatuuronderzoek was uitgebreid en voor het opstellen van de enquête en het verwerken van de resultaten was inzicht nodig, al met al was het een complex project.

Ondanks dat ik het onderzoek zelfstandig heb verricht, zijn er een aantal mensen die een belangrijke rol hebben gespeeld bij de totstandkoming van dit rapport. Allereerst wil ik mijn begeleiders bedanken voor hun feedback, zowel vanuit school als kantoor. Zonder hun feedback had ik het niveau van mijn scriptie niet naar een hoger niveau kunnen tillen.

Verder wil ik mijn ouders en zus bedanken voor hun feedback en hun kritische houding. Dit heeft mij geholpen om mijn scriptie ook eens te bekijken vanuit een andere invalshoek. Daarnaast wil ik de organisaties bedanken voor het invullen van de enquête in de voor hun drukke periode, zonder hun hulp had ik mijn scriptie nooit kunnen afronden.

Ik wens u veel leesplezier toe.

Jaco de Vos

Hardinxveld-Giessendam, 8 juni 2017

Samenvatting

Ondanks de toenemende aandacht en de daarmee samenhangende toenemende wet- en regelgeving met betrekking tot risicomanagement kunnen er nog veel slagen worden gemaakt ter verbetering van het risicomanagement van organisaties in Nederland.

Dit rapport heeft daarom tot doel om advies te geven ter verbetering van het risicomanagement en in het specifiek bij fondsenwervende instellingen door het niveau van risicomanagement bij fondsenwervende instellingen te onderzoeken.

Om dit doel te bereiken is in eerste instantie literatuuronderzoek uitgevoerd, dit is gedaan aan de hand van diverse deskundigen en modellen. Hieruit is gebleken dat met name cultuur- en structuuraspecten belangrijk zijn bij risicomanagement. Tevens is op basis van het literatuuronderzoek een model ontwikkeld voor risicomanagement. De kern van dit model is een cyclus die uit de stappen, voorbereiding, ontwikkeling van risicobeleid en de fasen van het risicoproces (risico-inventarisatie, -beoordeling, -beheersing, evaluatie, continu verbeteren en de verantwoording) bestaat. De randvoorwaarden die hiervoor benodigd zijn, zijn toezicht, informatie en communicatie.

Naast het literatuuronderzoek is er ook een enquête gehouden onder fondsenwervende instellingen om het niveau van fondsenwervende instellingen te onderzoeken. Het beeld is dat de fondsenwervende instelling gemiddeld een zeer magere voldoende scoort en zichzelf te hoog inschat, dit geldt (met name) voor organisaties die laag scoren. Organisaties die hoog scoren, schatten zichzelf over het algemeen juist iets te laag in. Ook wordt door een focus op risicobeheersing bepaalde onderdelen van risicomanagement onderbelicht, zoals verantwoording, continu verbeteren en de evaluatie van beheersingsmaatregelen. Wat opvalt, is dat de verschillen tussen organisaties groot zijn en dat er geen (significante) relatie is tussen de grootte van de organisatie en de behaalde scores.

Op basis van de bevindingen uit het literatuuronderzoek en de enquête wordt aanbevolen om (meer) aandacht te (blijven) besteden aan risicomanagement, dit kan het beste vanuit zowel het conformance- als het performance-motief gebeuren. Ook zou risicomanagement in bestaande processen en in de planning & controlcyclus geïntegreerd moeten worden. Organisaties moeten zich niet alleen richten op risicobeheersing, maar ook op andere onderdelen van risicomanagement. Verder zouden organisaties aandacht moeten blijven besteden aan de risicocultuur en het risicobewustzijn.

Eventueel vervolgonderzoek zou bij dit onderzoek kunnen aansluiten door meer fondsenwervende instellingen te onderzoeken en een conclusie te trekken over de voor- of achteruitgang van risicomanagement bij fondsenwervende instellingen door het niveau, zoals geschetst in dit rapport, te vergelijken met het door haar of zijn onderzochte niveau. Tevens is het mogelijk om te focussen op een bepaald onderdeel van risicomanagement of risicomanagement juist in een breder context te plaatsen.

Inhoudsopgave

Figuren- en tabellenlijst

Lijst met afkortingen

BBP: Bruto Binnenlands Product

CBF: Centraal Bureau Fondsenwerving
COS: Controle- en Overige Standaarden
COSO: Committee of Sponsoring Organizations of the Treadway Commission
CRO: Chief Risk Officer

EFQM: European Foundation for Quality Management
ERM: Enterprise Risk Management
ERMS: European Risk Management Standard
ERMF: Enterprise Risk Management Framework (COSO II-raamwerk)

FERMA: Federation of European Risk Management Associations

GDN: Goede Doelen Nederland

IF: Instituut Fondsenwerving
IFRS: International Financial Reporting Standards
INK: Instituut Nederlandse Kwaliteit
INTOSAI: International Organization of Supreme Audit Institutions
ISO: International Organization for Standardization

KPI: Kritische Prestatie Indicator
KSF: Kritische Succes Factor

MVO: Maatschappelijk Verantwoord Ondernemen
M_o_R: Management of Risk

NBA: Nederlandse Beroepsorganisatie van Accountants
NIVRA: Nederlands Instituut Van Registeraccountants

PwC: Price Waterhouse Coopers

RJ: Raad voor de Jaarverslaggeving

SBF: Samenwerkende Brancheorganisaties Filantropie

WNT: Wet Normering Topinkomens

Begrippenlijst

Algemene ICT-controles: de algemene beheersingsmaatregelen die de beschikbaarheid en betrouwbaarheid van geautomatiseerde gegevensverwerking waarborgen. Dit is dus breder dan applicatiecontroles.

Applicatiecontroles: beheersingsmaatregelen binnen een applicatie die gericht zijn op betrouwbare input, verwerking en output van gegevens in een geautomatiseerd systeem.

Auditrapportage: een rapport met de bevindingen en conclusies over de interne beheersing.

Bedrijfsmodel: geeft richting op welke wijze waarde wordt gecreëerd. Het is blauwdruk van de organisatie en de relatie die de organisatie onderhoudt met haar omgeving.

Bedrijfsproces: een samenwerking van mensen (en middelen) binnen een organisatie om een product of dienst te leveren aan een klant. Afhankelijk of de klant intern of extern is, wordt er gesproken over ondersteunende en primaire processen.

(interne) Beheersing: de term beheersing is niet hetzelfde als interne controle. Beheersing heeft drie elementen die 'controle' niet heeft: voorkomen, detecteren en vooruitkijken. Bij 'controle' wordt alleen de werkelijkheid met een norm vergeleken.

Beheersbaarheidsprincipe: managers moeten alleen verantwoordelijk worden gesteld voor zaken die binnen hun invloed vallen.

Bestaand risicoprofiel: de bestaande, geïnventariseerde risico's plus de analyse binnen de organisatie.

Black swan: een onverwachte gebeurtenis met een grote impact die ondanks effectief risicomanagement plaatsvindt.

Bottom-up benadering: de informatie vanuit de praktijk, het personeel gaat naar het management.

Categorale risico-indeling: is gericht op een zevental risicocategorieën, te weten omgevingsrisico's, organisatierisico's, procesrisico's, projectrisico's, operationele sturingsrisico's, managementinformatierisico's en verantwoordingsrisico's.

Communicatie: het uitwisselen van informatie tussen ten minste twee partijen, hiervan is minimaal één partij de zender en minimaal één partij de ontvanger. De communicatie verloopt via een kanaal.

Configuratie-instellingen: de instellingen en parameters in het geautomatiseerde systeem die bepalend zijn hoe bedrijfsprocessen binnen het IT-systeem worden afgewikkeld en welke controlerapportages uit het IT-systeem kunnen worden gegenereerd.

Conformance-motief: het aanpassingsmotief, men houdt zich aan de wet-en-regelgeving. Het motief heeft een 'het-moet' karakter.

Confrontatiematrix: in deze matrix worden interne (sterkten en zwakten) en externe elementen (kansen en bedreigingen) tegenover elkaar gezet.

Control override: hierbij is het mogelijk, om door middel van een specifieke autorisatie, transacties te wijzigen waardoor voorgeprogrammeerde controles ten aanzien van de uitvoer van deze transactie kunnen worden ontweken.

Corporate governance: gaat over deugdelijk ondernemingsbestuur. Het bestaat uit besturen, beheersen, toezicht houden en verantwoorden.

COSO II(-raamwerk): geeft een definitie van risicomanagement, aanwijzingen voor de manier waarop risicomanagement kan worden gestructureerd en gemeenschappelijke uitgangspunten voor risicomanagement.

DESTEP-analyse: een model van externe factoren die de bedrijfsvoering kunnen bedreigen. De analyse wordt hier breder getrokken dan bij het vijfkrachtenmodel van Porter. De factoren die onderscheiden worden zijn: demografisch, economisch, sociaal-cultureel, technologisch, ecologisch en politiek.

Desired level of risk: de gewenste verhouding tussen de hoeveelheid risico en omzet.

Discretionary kostencentrum: de output van deze organisatorische eenheid kan niet worden gemeten in geldwaarde. De manager wordt niet alleen beoordeeld op basis van het budget, maar ook op basis van de geleverde prestaties.

Dynamische risico's: hiervan is sprake als er kansen zijn op zowel winst als verlies, het dynamisch risico worden ook wel aangeduid als ondernemersrisico. Ze treden vooral op bij het ondernemen of het doen van investeringen en zijn in het algemeen niet verzekerbaar.

Eenheid van bevel: iedere werknemer heeft slecht één baas.

Enterprise Risk Management: is gericht op de beheersing van alle risico's in een organisatie, het zogenoemde organisatiebrede risicomanagement.

European Risk Management Standard: een door de FERMA in 2002 ontwikkelde blauwdruk voor de inrichting van een risicomanagementproces.

Events: gebeurtenissen die het behalen van de gestelde doelen negatief of positief kunnen beïnvloeden.

Exoneratie(beding): een beperking van de aansprakelijkheid, opgenomen in de leveringsvoorwaarden.

Extern risico: een risico dat zijn bron heeft buiten de onderneming.

Factoring: het uitbesteden van de debiteurenadministratie (inclusief facturering en incassering) aan een (gespecialiseerde) instelling.

Federation of European Risk Management Associations: een koepelorganisatie van de in Europese landen gevestigde risicomanagementorganisaties.

Functiescheiding: de scheiding van taken en verantwoordelijkheden tussen personen op basis van arbeidsverdeling. Het doel is om tegengestelde belangen tussen functionarissen en afdelingen te creëren.

Functionele risico-indeling: risico's worden gestructureerd naar vakgebied. Voorbeelden van relevante vakgebieden zijn: financiën, politiek, technologie, wet- en regelgeving, communicatie, verantwoording, markt en organisatie en personeel.

Gebruikerscontroles: handmatige beheersingsmaatregelen die verankerd zijn in de administratieve organisatie en functiescheidingen, zoals procedures, werkinstructies en richtlijnen.

Guide 73-2009 Risk Management Vocabulary: een gemeenschappelijke 'taal' voor het voeren van risicomanagement, bedoeld om eenheid te verkrijgen in de gebruikte definities en terminologie bij risicomanagement.

Harde beheersingsmaatregelen: dit zijn de tastbare maatregelen, ook wel hard controls genoemd. Voorbeelden zijn procedures en richtlijnen.

Inherent risico (brutorisico): het risico voordat de beheersingsmaatregelen genomen zijn.

Integraal risicomanagement: het management van alle verschillende risicogebieden in onderlinge samenhang wordt in de gehele organisatie toegepast.

Interface controles: beheersingsmaatregelen ter waarborging van een juiste, tijdige en volledige gegevensoverdracht tussen applicaties onderling.

Intern risico: een risico dat voortkomt uit de onderneming zelf.

ISO 31000: de nieuwe norm voor risicomanagement. Het biedt aan de ene kant een algemeen kader voor organisatie die risicomanagement in de meest brede zin in de praktijk willen brengen, aan de andere kant dient het als 'paraplu' voor allerlei sector- en onderwerp specifieke ISO-normen op het gebied van risicomanagement.

ISO 9100: een internationale norm voor kwaliteitsmanagementsystemen. De herziene versie met onder andere veranderingen op het gebied van het identificeren en behandelen van risico's is eind 2015 gepubliceerd.

Ketenrisicomanagement: risicomanagement is volledig geïntegreerd in de samenwerking met ketenpartners.

Kwaliteitsmanagement: het geheel van besturingsactiviteiten gericht op het systematisch en gestructureerd meten, verbeteren, herontwerpen en borgen van de kwaliteit van systemen en processen binnen de organisatie.

Leasing: het huren (of verhuren) van bepaalde productiemiddelen voor een bepaalde tijd. Hierbij worden twee vormen onderscheiden: operational en financial. Bij financial lease draagt de eigenaar (in bezit) de risico's, terwijl dat bij operational lease niet zo is.

Masterdatabeveiliging: betreft de toegang en het beheer van stamgegevens binnen het IT-systeem.

Operationeel risico: het risico van verlies als gevolg van inadequate of falende interne processen, mensen en systemen als gevolg van externe gebeurtenissen.

Outsourcing: het uitbesteden van bepaalde (activiteiten), die ook door de organisatie zelf gedaan kunnen worden, aan een externe (gespecialiseerde) uitvoerder.

Particularisme: het stellen van een bijzonder belang boven het algemene belang.

Paternalisme: de neiging om alles van bovenaf, als een (autoritaire) vader, te regelen en te beslissen.

Peer-to-peer benadering: mensen in de organisatie moeten informatie met elkaar delen, als men kijkt in een organisatie, gaat de informatie 'heen en weer'.

Performance-motief: het motief om iets (risicomanagement) uit te voeren uit resultaatgerichte motieven. Men verwacht dat hier op termijn voordeel mee behaald kan worden.

Persoonlijk ontwikkelingsplan: een afspraak tussen een personeelslid en werkgever over de persoonlijke ontwikkeling van het personeelslid in relatie met de competenties en de organisatiedoelstellingen.

Planning-en-controlcyclus: de cyclus waarin strategische plannen worden opgezet en uitgevoerd.

Procesgerelateerde beheersingsmaatregelen: dit zijn maatregelen waar een directe relatie is met transacties of stromen binnen een proces.

Randvoorwaardelijke beheersingsmaatregelen: bij deze maatregelen is er geen directe relatie tussen de maatregelen en de transacties of stromen binnen het proces.

Resilience Risk Management: de organisatie accepteert risico's en is daarbij veerkrachtig genoeg om de gevolgen van de geaccepteerde risico's op te vangen en zo snel mogelijk terug te keren naar de herstelde en veilige bedrijfsvoering.

Restrisico (nettorisico): het risico dat 'overblijft' na de genomen beheersingsmaatregelen.

Resultaatgebieden: vormen een verdere uitwerking van strategische doelstellingen naar de kernfuncties van de organisatie(-eenheid) en worden uitgewerkt in de vorm van prestatie-indicatoren en voorwaarden die van belang zijn om prestaties juist te kunnen beoordelen.

Risico-acceptatiegrens (risk tolerance): welke risico's een organisatie wel of niet acceptabel vindt.

Risicomanager: degene die direct verantwoordelijk is voor de initiëring en het opstellen van de risico-inventarisatie, het uitvoeren van de risico-evaluatie en het doel van beleidsvoorstellen met betrekking tot risicoreductie en risicofinanciering.

Risicomap: een scoringsmodel waarbij aan risico's door middel van een semi-kwantitatieve score een prioriteit wordt toegekend.

Risk appetite: ook wel risicobereidheid of risicohouding genoemd. Hierbij wordt gekeken naar het bestaande risicoprofiel, de risk capacity, de risk tolerance en de desired level of risk.

Risk capacity: de hoeveelheid risico die de organisatie kan dragen zonder aantasting van de financiële positie van de organisatie.

Risk readiness: het vermogen van mensen en organisatie om onzekerheden en risico's te hanteren dat zij deze kunnen voorkomen of op een veerkrachtige manier kunnen beheersen, en dat zij dat als gedeelde overtuiging hebben verinnelijkt in risicobewustzijn en kunnen omzettten in risicobewust handelen.

Risk tolerance (risico-acceptatiegrens): de acceptabele variatie in resultaten die de organisatie bereid is te accepteren in iedere risicocategorie.

Signaleringslijsten: uitzonderingsrapportages rondom verwerkte transacties of kritische wijzigingen in de applicatie zoals masterdata of configuratie-instellingen.

Soft controls: niet-tastbare gedrag beïnvloedende factoren in een organisatie. Voorbeelden zijn leiderschap, voorbeeldgedrag en communicatiestijlen.

Staffunctie: staat in een organisatie met een divisiestructuur gegroepeerd onder de ondernemingsleiding. Als staffunctionaris rapporteert men rechtstreeks aan de ondernemingsleiding en staat men ter beschikking van alle onderdelen en afdelingen van de organisatie.

Stamgegevens: gegevens die niet vaak gewijzigd worden en die basisinformatie bevatten voor de toepassing waarop ze betrekking hebben.

Statische risico's: hierbij is uitsluitend sprake van een kans op verlies zijn in principe verzekerbaar.

States of nature: omgevingsvariabelen die buiten de macht van de onderneming liggen.

Strategisch risico: het gevaar voor kapitaalverlies en/of het voortbestaan van de organisatie als gevolg van veranderingen in de omgeving in de omgeving, zakelijk nadelige beslissingen of een onjuiste implementatie van de gekozen strategie.

SWOT-analyse: hierbij worden vier factoren onderscheiden: Strenghts, Weaknesses, Opportunities en Threats. Deze kunnen vervolgens in een matrix (confrontatiematrix) tegenover elkaar worden gezet. Het kan een hulpmiddel zijn om risico's te rangschikken.

Tone at the top: de toon van een organisatie en haar topmanagement (als voorbeeld voor de rest van de organisatie).

Top-down benadering: bij deze benadering gaat informatie vanuit het management naar het personeel. Deze benadering wordt binnen de meeste organisaties toegepast.

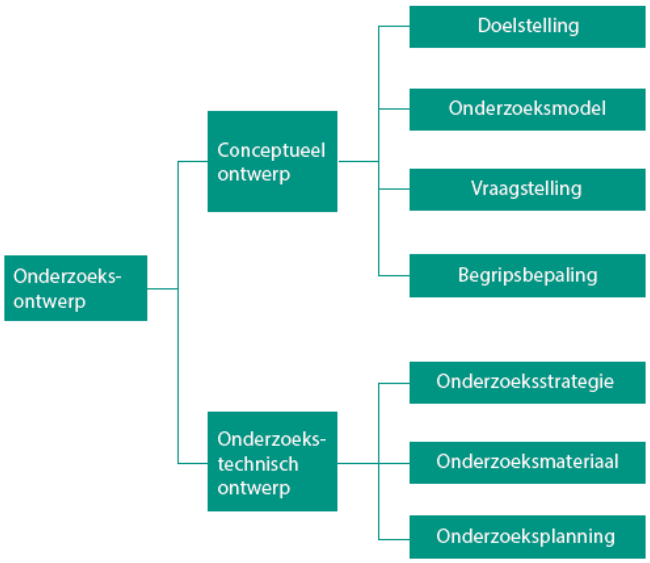
Verantwoordelijkheidscentrum: een organisatorische eenheid die wordt geleid door een manager die verantwoordelijk is voor de activiteiten daarvan.

Vijfkrachtenmodel van Porter: in dit model maakt Porter onderscheid tussen vijf factoren die de concurrentiekracht van een organisatie kunnen verstrekken of verzwakken. Deze factoren zijn: leveranciers, mogelijke toetreders, klanten en substituten en huidige concurrentie.

Vrijwaringsbeding: een bepaling in een contract waarbij partijen overeenkomen dat de ene partij de verantwoordelijkheid overneemt van de andere partij in het geval dat een bepaalde gebeurtenis tot schade leidt en die andere partij daarvoor aansprakelijk is.

1. Inleiding

In dit hoofdstuk wordt in eerste instantie de aanleiding en de afbakening van het onderwerp behandeld. Bij de uitwerking van de doelstelling, het onderzoeksmodel en de vraagstelling wordt de theorie van Piet Verschuren en Hans Doorewaard gebruikt. Piet Verschuren en Hans Doorewaard onderscheiden hierbij een conceptueel en een onderzoekstechnisch ontwerp, waarbij het conceptueel gaat over het 'wat, waarom en hoeveel er onderzocht wordt' en het technisch ontwerp over het 'hoe, waar en wanneer' gaat.[1] Het conceptueel model wordt grotendeels in dit hoofdstuk behandeld en het onderzoekstechnisch ontwerp wordt voornamelijk in hoofdstuk 2 behandeld. De aanpak van het praktijkonderzoek wordt in hoofdstuk 4 beschreven. Als laatste wordt de opbouw van het rapport weergegeven in een leeswijzer.



Figuur 1 Totaalbeeld onderzoeksontwerp (Piet Verschuren en Hans Doorewaard, 2015)

1.1 Aanleiding, afbakening en relevantie

Risicomanagement is geen nieuw begrip; in de jaren '60 werd voor het eerst gesproken over risicomanagement. Toch is de oorzaak van de huidige aandacht die er momenteel is voor risicomanagement nog niet heel oud. Enerzijds kan deze aandacht verklaard worden door diverse boekhoudschandalen, fraudegevallen en de economische crisis en anderzijds door de verandering in de publieke opinie in Nederland dat voor een belangrijk deel veroorzaakt werd door diverse financiële schandalen. Naar aanleiding van deze gebeurtenissen heeft de overheid, voornamelijk in laatste jaren tijdens en de jaren na de crisis, nieuwe wet- en regelgeving geformuleerd; deze wet- en regelgeving heeft niet alleen betrekking op financiële informatie maar ook op niet-financiële informatie.

In het licht van deze gebeurtenissen kan ook de aangepaste 'RJ 400 Jaarverslag' gezien worden. Op 26 maart 2014 is de RJ-uiting 2014-3: "ontwerp-Richtlijn 400 Jaarverslag" gepubliceerd. In deze ontwerp-richtlijn is de alinea (110) aangepast die betrekking heeft op risicomanagement. Op 1 januari 2015 is deze richtlijn in werking getreden en is van toepassing op organisaties die (verplicht zijn om) een bestuursverslag opmaken (en openbaar maken).

Voor elke organisatie wordt risicomanagement steeds belangrijker, niet alleen voor organisaties die gericht zijn op het maken van winst, maar ook voor non-profitorganisaties. Enerzijds om te voldoen aan wet-en-regelgeving (RJ 400), maar anderzijds ook om zo waarde toe te voegen aan de organisatie door er bijvoorbeeld voordeel mee te behalen.

Toch is, ondanks deze toenemende aandacht en wet- en regelgeving, uit onderzoek gebleken dat nog ruim 75% van de organisaties in de goededoelensector geen portefeuille risicomanagement in het bestuur heeft en bij bijna 50% is dit ook niet ondergebracht in een commissie.[2] Dit geeft aan dat er

[1] (Piet Verschuren en Hans Doorewaard, 2015, p. 16)
[2] (Capital Counsel, 2015, p. 6)

nog veel slagen moeten worden gemaakt met betrekking tot risicomanagement. Dit wordt mede ondersteund door de conclusie van de onderzoekers van het Tweede Nationaal Onderzoek Risicomanagement in Nederland 2014.[3]

Dit rapport bouwt voor een deel voort op het rapport van de onderzoekers van het Tweede Nationaal Onderzoek Risicomanagement in Nederland. Hierbij moet wel gezegd worden dat het rapport dat is uitgevoerd door Nyenrode Business Universiteit, Rijksuniversiteit Groningen, de Nederlandse Beroepsorganisatie van accountants (NBA) en PwC, gericht is op organisaties uit diverse sectoren. Dit in tegenstelling tot dit rapport, wat gericht is op fondsenwervende instellingen.

1.2 Probleemstelling

De aanleiding (zie vorige paragraaf) van het probleem is de recente aanpassing van RJ 400 Jaarverslag. Deze richtlijn geeft aan wat er met betrekking tot het wettelijke vereiste (art. 391 lid 1 BW2) van de beschrijving van de voornaamste risico's en onzekerheden in het jaarverslag opgenomen moet worden. Na vooronderzoek is gebleken dat de risicoparagrafen die zijn opgenomen in jaarverslagen van diverse stichtingen en verenigingen echter niet voldoen aan RJ 400. Op basis van het oriënterend onderzoek kan dit probleem echter ook in een breder context worden gezien. Uit het oriëntatieonderzoek is namelijk gebleken dat de risicoparagraaf nauw samenhangt met het risicomanagement. De risicoparagraaf kan namelijk gezien worden als een eindproduct van risicomanagement wat betreft de verantwoording. Risicomanagement is nodig om een risicoparagraaf te kunnen opnemen in het jaarverslag. Naast deze aanpassing is ook de term 'goededoelenorganisaties' aangepast. Op basis van hetzelfde onderzoek is gebleken dat dit een ruim begrip is, waar veel organisaties onder vallen. Deze term is bij de huidige probleemstelling vervangen door de term 'fondsenwervende instellingen'. Deze term wordt vanuit verslagtechnische hoek bekeken; het zijn organisaties die RJ 650 toepassen.

De huidige probleemstelling is dan ook: "Het risicomanagement bij fondsenwervende instellingen is van onvoldoende niveau."

De relatie tussen de opdrachtgever (WITh Accountants) en het probleem wordt weergeven door de aanleiding van de bovenstaande probleemstelling. WITh Accountants moet namelijk onder andere het bestuursverslag controleren. Dit wordt gedaan door te controleren of de vereiste elementen (volgens wet- en regelgeving) zijn opgenomen en of dit niet tegenstrijdig is met de jaarrekening en de opgedane kennis van de organisatie. Uit het vooronderzoek is gebleken dat de risicoparagraaf (onderdeel van bestuursverslag) niet op orde is, ook niet bij klanten van WITh Accountants. WITh Accountants moet dan in haar oordeel aangeven dat het bestuursverslag niet voldoet aan wet- en regelgeving.

Aan de ene kant doet WITh Accountants door middel van dit rapport, kennis op en anderzijds kan het advies gebruikt worden ter verbetering van de risicoparagraaf en ook voor de verbetering van risicomanagement bij klanten.

1.3 Type onderzoek

Er zijn globaal gezien twee soorten van wetenschappelijk empirisch onderzoek, een praktijkgericht onderzoek en een theoretisch-gericht onderzoek. Dit onderzoek is praktijkgericht. Bij praktijkgericht onderzoek kunnen er verschillende soorten onderzoek worden onderscheiden, wat uitgelegd kan worden aan de hand van de zogenoemde interventiecylus. Deze cyclus bestaat volgens Hans Doorewaard uit een aantal fasen: probleemanalyse, diagnose, ontwerp, verandering en evaluatie.[4]

[3] (Koninklijke Nederlandse Beroepsorganisatie van Accountants, 2014)
[4] (Hans Doorewaard, sd)

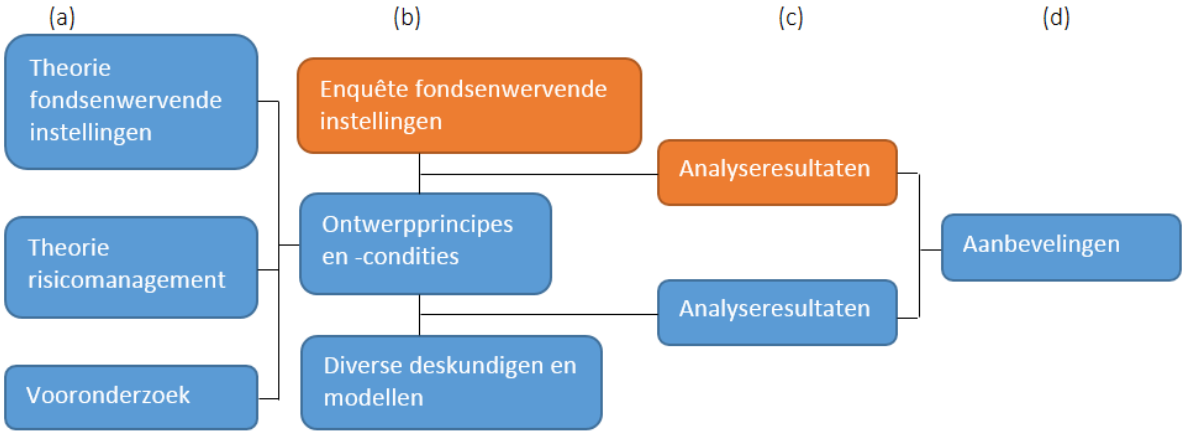
Deze cyclus geeft niet de opbouw van het rapport weer, de interventiecyclus geeft alleen de typen praktijkgerichte projecten weer. Het type praktijkgerichte project dat het beste bij dit rapport past, is ontwerpgericht; er wordt dus gezocht naar een oplossing van een probleem.

1.4 Doelstelling

Het rapport heeft tot doel om advies te geven ter verbetering van het risicomanagement bij fondsenwervende instellingen, door het niveau van risicomanagement bij fondsenwervende instellingen te onderzoeken.

1.5 Onderzoeksmodel

Zoals gezegd is het uit te voeren onderzoek is praktijkgericht en in het specifiek ontwerpgericht. Onderstaand model is daarop ook ingericht, in het midden staat: 'Ontwerpprincipes en –condities'. Dit geeft aan dat het een ontwerpgericht onderzoek betreft; de ontwerpprincipes en –condities worden onderzocht.



Figuur 2 Onderzoeksmodel (o.b.v. literatuur Piet Verschuren en Hans Doorewaard)

Een bestudering van de theorie over fondsenwervende instellingen en risicomanagement (a) afkomstig van diverse deskundigen en modellen (b) resulteert in een tweetal analyses. De bovenste analyse gaat over de resultaten van de enquête, de onderste analyse gaat over de theorie van risicomanagement (c). Bij de analyse van de theorie (Bijlage 1 Literatuuronderzoek) wordt een theoretisch model ontwikkeld (3. Theoretisch model). De vergelijking van analyseresultaten resulteert in adviezen ter verbetering van risicomanagement bij fondsenwervende instellingen (d). Tevens wordt er een implementatieplan geschreven.

De oranje gekleurde velden geven aan dat dit niet het theoretisch kader betreft, maar dat informatie verkregen wordt via de enquête en vanuit daar ook geanalyseerd wordt. Bij onderdeel c gaat het oranje gekleurde analyseresultaat over de 'ist-positie' en het blauw gekleurde analyseresultaat over de 'soll-positie'.

Het literatuuronderzoek speelt een belangrijke rol bij het uit te voeren onderzoek. Door middel van het literatuuronderzoek wordt de 'soll-positie' bepaald, wat resulteert in een model. Het advies (doel) ter verbetering van het risicomanagement zal logischerwijze zijn oorsprong hebben in het theoretisch kader. Advies kan immers geen oorsprong hebben in de enquête ('ist-positie') omdat de enquête 'alleen' het niveau van risicomanagement bij fondsenwervende instellingen onderzoekt. De enquête geeft wel richting aan het advies, op basis van de enquête kan immers bepaald worden welk advies er gegeven wordt. Immers, als uit de enquête blijkt dat een bepaald onderdeel wel voldoende scoort, is het overbodig om daar advies over te geven.

1.6 Opdracht en vraagstelling

De opdracht is: "Onderzoek van welk niveau het risicomanagement is bij fondsenwervende organisaties en geef advies ter verbetering van het risicomanagement."

Deze opdracht sluit logischerwijze aan op de doelstelling zoals beschreven in de vorige paragraaf. Als deze opdracht wordt uitgewerkt in onderzoeksvragen, moeten de volgende vragen beantwoord worden in het loop van het onderzoek.

De theorie over fondsenwervende instellingen en risicomanagement (a + b) is opgenomen in Bijlage 1 Literatuuronderzoek. Er zijn in totaal twee centrale vragen die betrekking hebben op de analyse (Figuur 2).

Centrale vraag (c):
Hoe kan het risicomanagement bij een fondsenwervende instelling ingericht worden? ('soll-positie')

Op basis van het literatuuronderzoek (a + b) wordt een (eigen) theoretisch model ontwikkeld, waarmee deze centrale vraag beantwoord wordt.

Centrale vraag (c):
Wat is het niveau van risicomanagement bij fondsenwervende instellingen? ('ist-positie')

Aan de hand van de uitgevoerde enquête en de opgestelde scoreleidraad kan deze centrale vraag worden beantwoord.

De centrale vragen zijn voor een deel afkomstig uit het vooronderzoek. Aan de hand van de probleemanalyse, wat is uitgevoerd met behulp van het visgraatdiagram, zijn een aantal onderwerpen geselecteerd die aan de orde zouden moeten komen in het rapport. Verder zijn de centrale vragen geformuleerd in relatie met het doel van dit rapport.

1.7 Opbouw

In de onderstaande tabel wordt op een overzichtelijke en schematische manier de opbouw van het rapport weergegeven.

Tabel 1 Leeswijzer

Centrale vraag	Beantwoord in
Hoe kan het risicomanagement bij een fondsenwervende instelling het beste ingericht worden?	Hoofdstuk 3 Theoretisch model risicomanagement
Wat is het niveau van risicomanagement bij fondsenwervende instellingen?	Hoofdstuk 5 Onderzoeksresultaten en analyse enquête

In het volgende hoofdstuk (hoofdstuk 2) wordt de onderzoeksopzet beschreven, dat met name ingaat op het theoretisch kader. Hoofdstuk 3 wordt geschreven op basis van het literatuuronderzoek (Bijlage 1 Literatuuronderzoek). In hoofdstuk 4 wordt de aanpak van de enquête behandeld en gaat verder in op het type onderzoek, de opzet van de enquête, de benaderde organisaties, de respons, de betrouwbaarheid en validiteit van de enquête en als laatste de scoreleidraad. In hoofdstuk 5 worden de onderzoeksresultaten weergegeven en er wordt op basis van de scoreleidraad het niveau van risicomanagement bij fondsenwervende instellingen in kaart gebracht. In hoofdstuk 6 zullen er conclusies worden getrokken (ter beantwoording van de hoofd- en deelvragen). Dit hoofdstuk zal worden gesplitst aan de hand van de centrale vragen. Als laatste (hoofdstuk 7) wordt een advies gegeven (door 'soll-positie' met 'ist-positie' te vergelijken) en een implementieplan (hoofdstuk 8) beschreven.

2. Onderzoeksopzet

Het conceptueel model is in de inleiding behandeld, in dit hoofdstuk wordt het technisch ontwerp behandeld. Zoals gezegd gaat het technisch ontwerp over het 'hoe, waar en wanneer'. Dit wordt ook terug gezien in de indeling van dit hoofdstuk, allereerst gaan de eerste twee paragrafen over het hoe, waarbij in de eerste paragraaf de aanpak aan de orde komt en in de tweede paragraaf de middelen. Gezien de geringe relevantie van het waar en wanneer, wordt dit weggelaten. Dit hoofdstuk gaat met name in op de opzet van het theoretisch kader, aan de uitwerking van het praktijkgerichte onderdeel wordt in hoofdstuk 4 extra aandacht besteed.

2.1 Onderzoeksstrategie

De eerste vier typen onderzoeksstrategieën volgens de tabel hiernaast, zijn empirisch van aard, bureauonderzoek is niet empirisch van aard. Zoals in de inleiding aangegeven is er sprake van wetenschappelijk empirisch onderzoek. Het theoretisch kader kenmerkt zich dan ook het beste door het type 'case study' en het praktijkgerichte gedeelte door het type 'survey'.

Tabel 2 Typen onderzoeksstrategieën (Ricardo Cronie, 2007)

Kenmerken van typen onderzoeksstrategie		
Type	**Kenmerken**	**Bron**
Survey	Breed overzicht Kwantitatieve verwerking Beschrijven en macht van getallen	Uit literatuur/databases Zelf verzamelen
Experiment	Zelf uitvoeren Zien is geloven, meten is weten	Veldwerk Lab werk
Case Study	Diepte analyse Kwalitatieve verwerking Beschrijven en verklaren	Interviews Literatuur en bronnen
Speciale case study: theorie	Diepte analyse Kwalitatieve verwerking Oorzaken opsporen	Interviews Literatuur en bronnen
Bureauonderzoek	Breedte of diepte Voldoende info Nieuwe conclusies	Internet Bibliotheek Archieven

Het type 'case study' kenmerkt zich door onderzoek bij slechts één onderzoekseenheid.[5] Verder worden er diverse informatiebronnen geraadpleegd door middel van documentenonderzoek. Binnen het theoretisch onderzoek wordt de case study gebruikt om een nieuwe theorie te vormen: "het ontwikkelen van een eigen model voor risicomanagement". Dit wordt later in het praktijkgerichte gedeelte getest binnen een grotere populatie (fondsenwervende instellingen). Een 'case study' is toepasselijk op praktijkgericht onderzoek waarbij aan de hand van een probleemstelling, adviezen en aanbevelingen worden gegeven.[6]

De enquête die gehouden zal worden, is een voorbeeld van het type 'survey'. Op een systematische wijze worden vragen gesteld aan fondsenwervende instellingen. Deze vragen gaan over de inrichting van risicomanagement. De enquête wordt ingevuld via het internet (online-onderzoek).

Aan de hand van dit schema en de gekozen typen blijkt ook dat het bij het literatuuronderzoek gaat om een diepte-onderzoek en dat het onderzoek zowel van kwalitatieve als kwantitatieve aard is. Het literatuuronderzoek is kwalitatief van aard, de enquête meer kwantitatief. Het literatuuronderzoek maakt immers gebruik van gegevens van kwalitatieve aard en de enquête is een onderzoek waar het niveau van risicomanagement door middel van cijfers wordt onderzocht.[7]

[5] (Foeke van der Zee, 2016)
[6] (Case-study onderzoek, 2015)
[7] (Piet Kempen & Jimme Keizer, 2016, p. 115)

2.2 Onderzoeksmateriaal

Bij het op zoek gaan naar geschikt bronnenmateriaal moet gekeken worden naar de vier dimensies die in de tabel hieronder zijn weergegeven. In dit rapport wordt het theoretisch kader gescheiden van het praktisch onderzoek (enquête). Aan de hand van deze indeling kunnen ook de bronnen ingedeeld worden.

Tabel 3 Typering bronnen (Ricardo Cronie, 2007)

Objecten	Bronnen	Type bronnen	Ontsluiting door …
Personen / groepen	Personen Media	Data bronnen	Ondervraging Observatie (waarnemen)
Situaties **Voorwerpen** **Processen**	Werkelijkheid Documenten Literatuur	Kennisbronnen: Inzichten; Theorieën	Meetinstrument Inhoudsanalyse Zoeksysteem

In het theoretisch kader worden in de eerste hoofdstukken, waar het gaat om de begripsbepaling, voorwerpen onderzocht, namelijk 'de fondsenwervende instelling' en 'risicomanagement'. Hiervoor wordt voornamelijk literatuur gebruikt van deskundigen. Dit zijn kennisbronnen waar door middel van een inhoudsanalyse en een zoeksysteem de deelvragen beantwoord worden. In het hoofdstuk over de inrichting van risicomanagement wordt een proces onderzocht, waarbij literatuur van deskundigen en modellen wordt gebruikt. Ook hier worden door middel van een inhoudsanalyse en een zoeksysteem de deelvragen beantwoord. Concreet worden boeken, websites, tijdschriften en diverse rapport als bronnen gebruikt voor het literatuuronderzoek.

In het gedeelte waar praktisch onderzoek wordt uitgevoerd, wordt de situatie onderzocht door het onderzoeken van de werkelijkheid aan de hand van een meetinstrument. Het meetinstrument is de enquête.

Aan de hand van de bronnen kan het onderzoeksmodel nader uitgewerkt worden. Bij onderdeel a staan twee onderwerpen centraal: de fondsenwervende instelling en risicomanagement. Per onderwerp zijn de gebruikte bronnen weergegeven. Hierbij worden de meest gebruikte en relevante bronnen benoemd. De bronnen die gebruikt zijn voor de theorie van fondsenwervende instellingen en risicomanagement kunnen gevonden worden in bijlage 1.

Tabel 4 Meest relevante en gebruikte bronnen per onderwerp (literatuuronderzoek)

Bronnen fondsenwervende instellingen		Bronnen risicomanagement		
Organisaties:	*Deskundigen (personen):*	*De modellen:*	*Deskundigen (personen)*	*Organisaties*
Centraal Bureau Fondsenwerving (CBF)	Prof. Dr. René Bekkers	ISO 31000	Sonja Janicijevic, Paul Claes en Rob Lengkeek	Nederlandse Beroepsorganisatie van Accountants (NBA)
Raad voor de Jaarverslaggeving (RJ)	Prof. Dr. Lucas Meijs	COSO ERM	Drs. Urjan Claassen RA RE CIA	Nyenrode Business Universiteit
Goede Doelen Nederland en IF			Jaap Zijlstra en Lizanne Vroom	Rijksuniversiteit Groningen
			Thinka Bor-Reijinga en Gert van der Kolk	PwC
			Erik van de Crommenacker, Peter Dona en Siebrand van der Ploeg	
			Roel Grit	
			Rob Uiterlinden	

Deze bronnen zijn voor een deel gevonden aan de hand van de 'Avans Catalogus', de rest is gevonden door het doornemen van literatuurlijst van de al eerder gevonden bronnen. Een groot aantal bronnen zijn experts in hun betreffende werkvelden. Op de betrouwbaarheid en validiteit wordt in de volgende paragraaf verder ingegaan.

2.3 Validiteit en betrouwbaarheid literatuuronderzoek

Validiteit gaat over de juistheid van de meting, betrouwbaarheid gaat over de herhaalbaarheid van de metingen.[8] Beide begrippen zijn van belang voor een onderzoek, hieronder zijn de validiteit en betrouwbaarheid met betrekking tot het literatuuronderzoek nader uitgewerkt.

Bij het zoeken naar literatuur is gezocht naar titels met het woord 'risicomanagement' en naar termen die verband houden met risicomanagement. In eerste instantie is gezocht via de 'Avans Catalogus', daarna zijn de bronnenlijsten van de gevonden boeken gebruikt, verder zijn boeken via de optie 'Google Boeken' opgezocht. Er zijn (wet)boeken, tijdschriften, websites, hoorcolleges en documenten van websites gebruikt, naast de al beschikbare persoonlijke kennis. Alle gebruikte bronnen zijn vermeld in de bronnenlijst. Tevens is bij gebruik van de bron, de bron inclusief paginanummer vermeld (betrouwbaarheid).

Elke bron is relevant (validiteit) omdat het direct en indirect heeft geholpen bij de beantwoording van de centrale vragen. Ook de gehanteerde methode van dit literatuuronderzoek en de gehanteerde methode van de gebruikte bronnen komt vrijwel overeen, namelijk onderzoek van literatuur en bronnen. Zoals gezegd is er gezocht naar bronnen met de titel 'risicomanagement' en titels die daarmee verband houden, dit geeft aan dat dit onderzoek en de bronnen over hetzelfde onderwerp gaan.

De theorie voor risicomanagement is niet specifiek gericht op fondsenwervende instellingen, maar de bouwstenen van risicomanagement zijn echter voor elke organisatie hetzelfde; het risicomanagementproces blijft hetzelfde (validiteit). Hoe organisaties het inrichten en de middelen die ze daarvoor gebruiken, verschilt echter wel, maar dat is niet de insteek van dit onderzoek en daaraan zal derhalve minder tot geen aandacht worden besteed.

De gebruikte bronnen zijn afkomstig van erkende instituten en personen (deskundigen). Bijvoorbeeld de Raad voor de Jaarverslaggeving, het Burgerlijk Wetboek, the Committee of Sponsoring Organizations of the Treadway Commission, de International Organization for Standardization, diverse universiteiten, de Nederlandse Beroepsorganisatie voor Accountants en diverse deskundigen die al meerdere publicaties op hun naam hebben staan. Ook is het tijdschrift 'Harvard Business Review' gebruikt. De aangehaalde bronnen in de vorm van een persoon (deskundigen) hebben veelal een titel, zoals doctorandus, doctor, registeraccountant, registercontroller, professor, certified internal auditor en register EDP-auditor. Velen hebben jarenlange ervaring in hun werkveld (betrouwbaarheid).

Verder sluiten de aangehaalde bronnen op elkaar aan en ondersteunen (op hoofdlijnen) ze elkaars theorieën (aanpak verschilt weleens), dit is ook meerdere keren aangegeven in het literatuuronderzoek (betrouwbaarheid). De bronnen zijn ook betrekkelijk actueel (validiteit), de oudste gebruikte bron komt uit 1988, wat gebruikt is voor een definitie. Het grootste gedeelte van de bronnen dateren uit 2009 en later. Het zijn vrijwel allemaal bronnen met het doel om de lezer te informeren.

[8] (Tilburg University, 2017)

3. Theoretisch model risicomanagement

Op basis van het literatuuronderzoek (Bijlage 1 Literatuuronderzoek) en eigen kennis en inzichten kan een (eigen) theoretisch model voor risicomanagement bij de fondsenwervende instelling worden ontwikkeld. Allereerst zal ter inleiding worden uitgelegd wat een fondsenwervende instelling, een risico en wat risicomanagement is (begripsbepaling), dit om een goed beeld te kunnen krijgen van het theoretisch model. Daarna wordt een risicomanagementmodel opgesteld. Voor een nadere uitleg en meer informatie wordt verwezen naar bijlage 1.

3.1 De fondsenwervende instelling

Vaak wordt onder de non-profitsector en de goededoelensector hetzelfde verstaan en de meeste mensen weten niet wat een fondsenwervende instelling is. Met de non-profit sector wordt echter iets anders bedoeld dan met de goededoelensector. De non-profit sector is een groter geheel waarvan de goededoelensector een onderdeel is. Van de goededoelensector zijn fondsenwervende organisaties vervolgens weer een onderdeel. Er kan onderscheid gemaakt worden tussen deze sectoren en organisaties op basis van wet- en regelgeving, maar ook door andere factoren, zoals de rechtsvorm, doelstellingen, de beschikking over een ANBI-status en het vrijgesteld zijn van belastingen.

Uiteindelijk kan gezegd worden dat een fondsenwervende organisatie, een particuliere organisatie is, die gericht is op het behalen van een maatschappelijke doelstelling en die voor het realiseren daarvan niet alleen een beroep doet op de maatschappij, maar ook op de overheid en bedrijven (Bijlage 1.1.2 Definitie van een fondsenwervende instelling). Verder kan vanuit verslagtechnische hoek gezegd worden dat een fondsenwervende instelling RJ 650 toepast.

3.2 Risico en risicomanagement

Om een helder begrip te krijgen van risico en risicomanagement worden deze begrippen uitgelegd. Tevens worden de indelingen van risico en de redenen voor het doen aan risicomanagement kort behandeld.

Een risico is een (mogelijke) gebeurtenis met een bepaald effect, die zowel negatief als positief kan zijn, in een bepaalde situatie en een specifieke periode (Bijlage 1.2.1 Definitie van risico). Hierbij wordt een risico gekoppeld aan de doelstellingen van een organisatie.

RJ 400 onderscheidt verschillende soorten risico's, namelijk strategische, operationele, financiële, verslaggevings- en wet- en regelgevingsrisico's. Deze soorten risico's sluiten gedeeltelijk aan bij het ERM Model (Bijlage 2.1 COSO ERM-model). Deze soorten risico's kunnen gekoppeld worden aan de organisatiedoelstellingen. Door risicomanagement kan een bepaalde mate van zekerheid verkregen worden over het bereiken van de doelstellingen. De indeling van risico's helpt ook bij het identificeren van risico's; het geeft structuur in de zoektocht naar risico's.

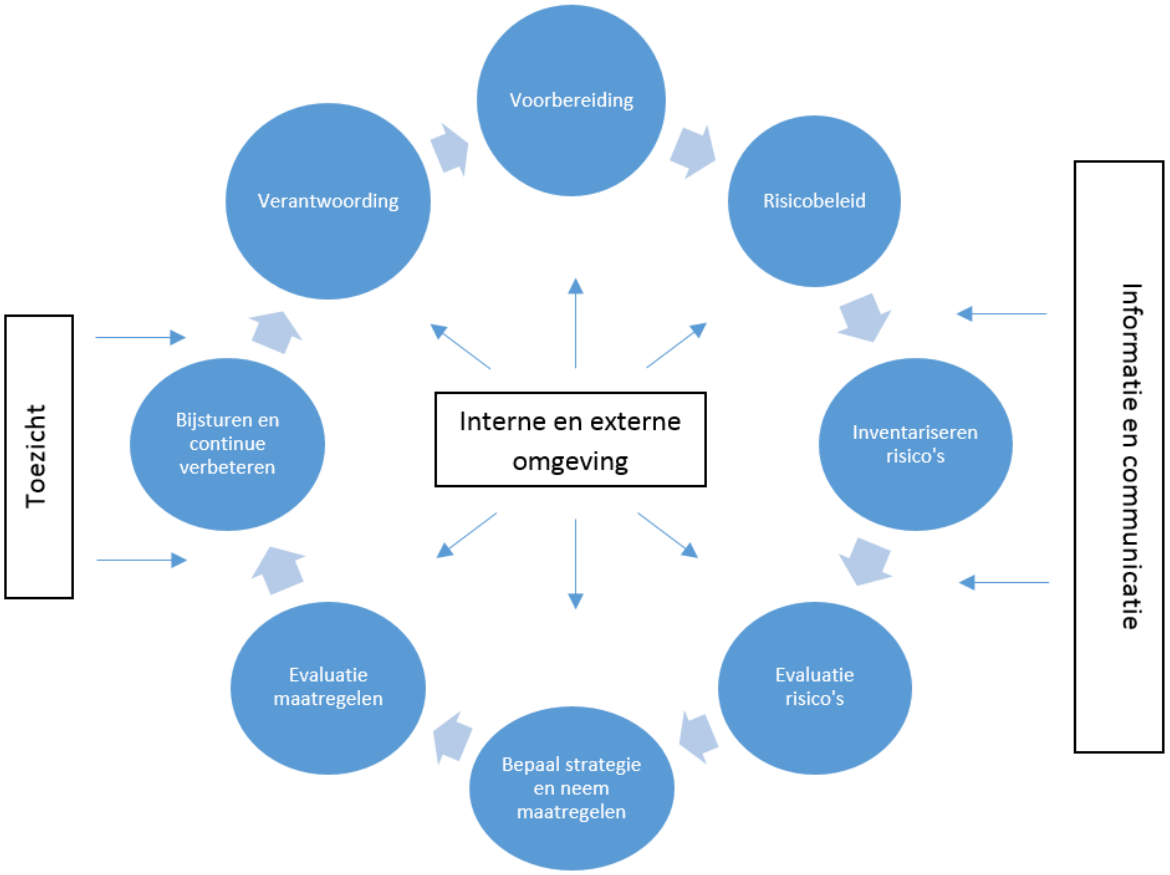
Risicomanagement is een dynamisch proces dat integraal toegepast wordt om risico's te beheersen en zo de doelstellingen te realiseren (Bijlage 1.2.3 Definitie van risicomanagement). Dit betekent enerzijds dat er voortdurend terugkoppeling plaatsvindt en dat de stappen binnen de cyclus niet op zichzelf staan en niet star van aard zijn, anderzijds betekent het dat risicomanagement in onderlinge samenhang in en door de gehele organisatie toegepast moet worden.

Risicomanagement wordt enerzijds toegepast om te voldoen aan wet en regelgeving (conformance-motief) en anderzijds om er voordeel mee te behalen (performance-motief).

3.3 De inrichting van risicomanagement

De eerste stap van de cyclus is de voorbereiding. De tweede stap is het ontwikkelen van het risicobeleid. De volgende stappen, van inventarisatie van risico's tot de verantwoording zijn onderdeel van het risicoproces.

Aan de zijkanten in het onderstaande figuur zijn de randvoorwaarden weergegeven, dit zijn de benodigdheden om het risicomanagementproces goed te laten functioneren.



Figuur 3 Cyclus risicomanagement

Voorbereiding

Voordat er een risicovisie en een risicobeleid ontwikkeld kan worden is het aan te bevelen om inzicht te krijgen in de omgeving van de organisatie en in de organisatie zelf.

Op basis van deze interne en externe oriëntatie kan dan de risicovisie ontwikkeld worden. Deze visie geeft het toekomstbeeld aan en in het bijzonder welke rol risicomanagement hierin speelt.

Een derde onderdeel dat onder de voorbereiding kan worden geschaard, is het formuleren van de risicomanagementdoelstellingen. Deze moeten geformuleerd worden in relatie met de organisatiedoelstellingen. Door deze in lijn met de doelstellingen van de organisatie te ontwikkelen, kan de risicostrategie en –beleid worden ontwikkeld, waardoor waardecreatie kan worden ondersteund (Bijlage 1.3.1 Voorbereiding).

Het laatste onderdeel is de ontwikkeling van de risicostrategie, deze beschrijft welke risico's en hoeveel risico de organisatie wenst te nemen (Bijlage 1.3.1 Voorbereiding). De risicohouding speelt hierin een belangrijke rol.

Risicobeleid

Het risicobeleid is een concrete uitwerking van de risicovisie. De onderdelen van risicobeleid zijn: de voorwaarden voor (effectief) risicomanagement, de organisatie van risicomanagement, het terrein van risicomanagement en de soorten risico's, de uitgangspunten van risicomanagement en de elementen van risicomanagement.

Uit literatuuronderzoek (Bijlage 1 Literatuuronderzoek) is gebleken dat met name cultuur en –structuuraspecten belangrijk zijn voor een succesvolle uitvoering van risicomanagement (Bijlage 1.3.2 Risicobeleid). Bij het structuuraspect van risicomanagement is van belang dat de verantwoordelijkheden zijn belegd op strategisch, tactisch en operationeel niveau; positionering van risicomanagement is een randvoorwaarde voor het creëren van draagvlak. Wat betreft het cultuuraspect is het belangrijk dat het risicobewustzijn betreffende verschillende risicogebieden actief gedeeld wordt op strategisch, tactisch en operationeel niveau; het stimuleert het organisatiebrede risicobewustzijn. In dit kader speelt ook het begrip risk readiness een rol, wat bestaat uit het risicobewustzijn en risicobewust handelen.

Wat betreft de organisatie van risicomanagement, er moet iemand verantwoordelijk zijn voor risicomanagement, bijvoorbeeld een CRO. Risicomanagement is echter ook een bezigheid voor de gehele organisatie; iedereen draagt verantwoordelijkheid voor de uitvoering van hun taken met betrekking tot risicomanagement (Bijlage 5 De taken, benodigde bewustzijn en kennis per verdedigingslinie). Het is tevens verstandig op prestatiemanagement te verbinden aan risicomanagement, dit moet echter niet te ver worden doorgevoerd, anders kan dit zich tegen een organisatie keren (Bijlage 1.3.2 Risicobeleid).

Afhankelijk van de organisatie kan risicomanagement een groot gebied bestrijken. Zo kunnen risico's op verschillende niveaus, bedrijfsonderdelen en externe factoren worden onderscheiden. Aan de hand van een bepaalde indeling kan men zich ook focussen op een bepaald aantal onderdelen (Bijlage 1.3.2 Risicobeleid). Zo kan risicomanagement op verschillende niveaus toegepast (Bijlage 2.2 INK model) worden:

- De gehele organisatie;
- Proces; en
- Activiteit.

Ook kunnen risico's per niveau worden onderscheiden. De relatie tussen risico en een niveau is tevens een indicatie voor de zwaarte van het risico. Een risico op een laag niveau zal de realisatie van de/een doelstelling(en) minder bedreigen dan een risico op een hoger niveau. Door niveaus te onderscheiden kan structuur worden aangebracht in risicomanagement.

Zoals gezegd moet risicomanagement samenhangen met de strategie en doelstellingen. De missie, visie, strategie en doelstellingen vormen het uitgangspunt voor risicomanagement (Bijlage 1.3.2 Risicobeleid). Er kunnen echter ook uitgangspunten of principes met betrekking tot risicomanagement op zichzelf worden onderscheiden (Bijlage 2.3 ISO 31000-richtlijn). Organisaties kunnen zelf ook principes opstellen, een aantal principes zijn echter altijd van belang bij risicomanagement (principes zijn afkomstig van ISO 31000 en bijlage 12):

1. Een integrale toepassing;
2. Geïntegreerd in processen en/of de planning & controlcyclus;
3. Systematisch, gestructureerd en tijdig (inclusief vastlegging)
4. Gerelateerd aan de doelstellingen;
5. Dynamisch, iteratief en reagerend op veranderingen.

De elementen van risicomanagement zijn hoofdzakelijk de stappen die gevolgd moeten worden bij risicomanagement, deze worden afzonderlijk hierna behandeld.

Risico-identificatie

De eerste stap van het risicoproces is de risico-inventarisatie, samen met de risico-evaluatie en –beheersing is dit de kern van het risicoproces.

Identificatie gebeurt in twee fasen, in de eerste fase probeert men zo veel mogelijk risico's te inventariseren. In de tweede fase worden risico's die nader onderzoek vergen, onderzocht. Het proces van inventarisatie van risico's op zichzelf gebeurt in drie stappen (Bijlage 1.3.3 Risicomanagementproces):

1. Het identificeren van gebeurtenissen;
2. Het toewijzen van oorzaken aan risico's; en
3. Het meten van risico's.

Bij het toewijzen van oorzaken aan risico's is het van belang om te bepalen of men invloed kan uitoefenen op deze oorzaken. Dit is namelijk mede bepalend voor de soort maatregelen die worden genomen.

Bij het identificeren is het belangrijk om een aanpak te hanteren die aansluit bij de structuur van de organisatie. Daarnaast is het onderzoeken van schade historie en het bijhouden van situaties die bijna tot schade hebben geleid zinvol om risico's te kunnen identificeren, ook kan de opgedane informatie bij de eerste stap (voorbereiding – inzicht verkrijgen in de interne en externe omgeving van de organisatie) hierbij gebruikt worden.

Het eindresultaat van de risico-inventarisatie is een risicolijst (Tabel 13). In deze lijst is het aan te bevelen dat degene voor wie het risico geldt, wordt benoemd. Hierdoor neemt de kans toe dat diegene ook zelf verantwoordelijkheid neemt voor dat risico en de mensen binnen de organisatie meer risicobewust worden.

Risicobeoordeling

Het is belangrijk om de stappen risico-inventarisatie en risicobeoordeling gescheiden te houden. Als dit niet gebeurt, is het mogelijk dat bepaalde risico's over het hoofd worden gezien.

Bij het beoordelen van risico's staan een aantal onderdelen een rol: kans, gevolg en de relatie met de doelstellingen. Ook spelen psychologische aspecten (risicoperceptie) een belangrijke rol.

Bij het bepalen van de zwaarte van het risico is van belang om rekening te houden met waar het risico plaatsvindt en in welke mate het risico de doelstellingen bedreigt. Risico's die zich afspelen in een (klein) onderdeel van de organisatie zijn over het algemeen minder ernstig als risico's die zich voordoen voor de gehele organisatie.

Bij het bepalen van de ernst van risico speelt de mens een belangrijke rol. Deskundigheid en persoonlijkheid spelen een belangrijke rol. Ervaring zorgt ervoor dat situaties sneller en beter herkend (kunnen) worden en ook beter beoordeeld kunnen worden. Ook de persoonlijkheid speelt een rol, over het algemeen vinden mensen het lastig om risico's in te schatten; mensen zijn vaak (te) optimistisch ingesteld. Het is daarom van belang om te kijken wie verantwoordelijk is/zijn voor het inschatten van risico's.

De risicoanalyse kan op twee manieren worden uitgevoerd: kwantitatief of kwalitatief. Bij de kwantitatieve methode wordt de zwaarte van het risico weergegeven door getallen en/of bedragen. Bij de kwalitatieve methode wordt de ernst van het risico beschreven door middel van woorden. De keuze tussen deze methoden hangt af van de aard van het risico, het doel van de analyse en de aard en voorkeur van de gebruikers van risico-informatie. Er zijn verschillende technieken die bij de risicobeoordeling gebruikt kunnen worden (Bijlage 3 Technieken risicobeoordeling).

Het eindresultaat van de risicobeoordeling (inclusief risico-inventarisatie) is het risicoprofiel (Tabel 15 en Tabel 16). Een methode om het risicoprofiel (grafisch) te presenteren is de risicomap (Figuur 50), hierbij kan ook rekening worden gehouden met de risicohouding.

Risicobeheersing

Er zijn verschillende manieren van risicobeheersing (Bijlage 1.3.3 Risicomanagementproces):

- Risico's vermijden;
- Risico's verminderen (beheersen en voorkomen);
- Risico's overdragen;
- Risico's accepteren.

Deze strategieën worden globaal gezien bij verschillende situaties toegepast. De eerste strategie wordt toegepast bij risico's met een hoge kans en impact. Risico's verminderen en risico's overdragen gebeurt wanneer één component (kans/gevolg) laag is en de andere hoog. Het verschil tussen risico's verminderen en risico's overdragen is dat men bij risico-overdracht het risico overdraagt aan een derde en bij het verminderen van risico's dat men zelf het risico vermindert. Risico's worden geaccepteerd wanneer zowel de kans als het gevolg laag is. Risico's worden echter ook geaccepteerd wanneer de andere strategieën niet mogelijk zijn, het is daarom van belang dat men veerkracht creëert om zo goed mogelijk met risico's om te kunnen gaan.

Bij het kiezen van een beheersmaatregel (Bijlage 7 Soorten beheersingsmaatregelen op verschillende niveaus) moet rekening gehouden worden met de ernst van het risico, maar ook met de economische afweging; een maatregel moet effectief en efficiënt zijn. Daarnaast is het belangrijk dat de risicohouding en de capaciteit in overweging worden genomen. Verder is het van belang dat een organisatie risk ready is en het vermogen heeft om adequaat op risico's te reageren, wanneer deze zich toch voordoen.

Het is belangrijk om te beseffen dat zowel de kans als de impact van een ongewenste gebeurtenis nooit helemaal terug te brengen is naar 'nul'. Het te ver doorvoeren van maatregelen en het doorvoeren van één bepaalde soort maatregelen kan zich bovendien tegen de organisatie keren.

Evaluatie en bijsturing

Voordat risicomaatregen geëvalueerd worden is het van belang om vast te stellen dat beheersingsmaatregelen operationeel zijn en (naar behoren) functioneren. Het heeft anders geen zin om de maatregel te evalueren.

Om de beheersingsmaatregel te evalueren moet de impact van de beheersingsmaatregel gemeten worden, daarna moet deze impact vergeleken worden met een norm of referentiepunt en wanneer de meting niet voldoet aan de norm, moet er bijgestuurd worden (Bijlage 1.3.3 Risicomanagementproces). Een goed voorbeeld van zo'n norm zijn de doelstellingen van een organisatie, deze doelstellingen dienen dan meetbaar te worden gemaakt door middel van prestatie-indicatoren. Evaluatie kan zowel gebeuren door de interne auditfunctie (of financiële afdeling) of door het tactisch en strategisch management.

De evaluatie van beheersingsmaatregelen kan afzonderlijk of voortdurend plaatsvinden. Bij afzonderlijke evaluaties is het van belang om een testmoment aan de evaluatie te koppelen, net als bij de risico-inventarisatie en –beoordeling. Dit testmoment is afhankelijk van de grootte van de organisatie en de snelheid van de veranderingen binnen en buiten de organisatie.

Naast het evalueren van het risicomanagementproces (beheersingsmaatregelen) kan het risicomanagement als functie ook geëvalueerd worden, dit kan gebeuren in opzet en werking.

Continu verbeteren
Om het risicomanagement in een organisatie te verbeteren is het van belang om ambities te formuleren. Tevens moet er inzicht worden verkregen in het huidige niveau van risicomanagement (Bijlage 6 Verschillende niveaus van risicomanagement). Door de ambities te vergelijken met het huidige niveau, kunnen er verbeteringen door worden gevoerd. Voor de ambities kunnen bijvoorbeeld de principes van zeer betrouwbare organisaties worden aangehouden (Bijlage 1.3.3 Risicomanagementproces). Bij continu verbeteren speelt het begrip leren een belangrijke rol; zowel het leren van zaken als het leren van fouten en het afleren van ongewenste zaken.

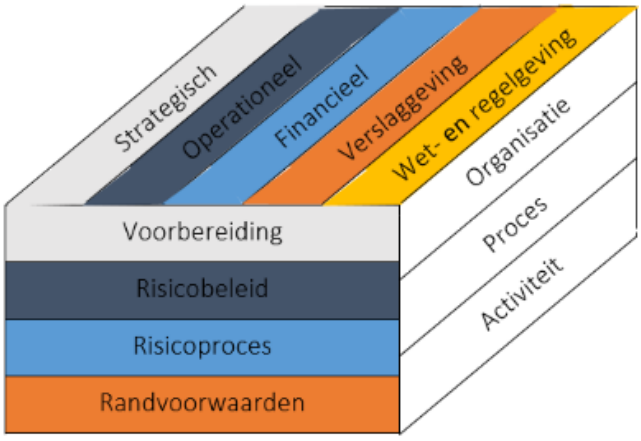
Verantwoording
Bij de verantwoording denkt men al snel aan het jaarverslag. Vanuit de wet- en regelgeving (o.a. Bijlage 10 Wet- en regelgeving met betrekking tot verenigingen en stichtingen) worden verschillende eisen gesteld aan de verantwoording (met betrekking tot het jaarverslag). De per 1 januari 2015 in werking getreden RJ 400 Jaarverslag, gaat specifiek in op de verantwoording met betrekking tot risico's (Bijlage 1.3.3 Risicomanagementproces).

Informatie
Om in de informatiebehoeften te voorzien, moet informatie verzameld worden, opgeslagen, verwerkt en beschikbaar gesteld worden. Deze informatie moet zowel efficiënt als effectief zijn om in de informatiebehoefte van de organisatie te kunnen voorzien (Bijlage 1.3.4 Randvoorwaarde). Informatie dient op alle niveaus binnen een organisatie beschikbaar te zijn om het risicomanagementproces goed uit te kunnen voeren, door middel van communicatie kan deze informatie doorgegeven worden in de stappen van de cyclus (Figuur 57**Fout! Verwijzingsbron niet gevonden.**).

Communicatie
Zonder het uitwisselen van informatie, in welke richting dan ook, komt het risicomanagement niet van de grond en kunnen de stappen van het risicomanagementproces niet doorlopen worden (Figuur 57). Bij communicatie is het van belang dat er niet alleen over inhoud en procedures wordt gecommuniceerd, maar ook over interactie en gevoel (Bijlage 1.3.4 Randvoorwaarde). Dit komt de sfeer en de cultuur binnen een organisatie ten goede, wat ook weer impact heeft op het risicomanagement.

Toezicht
Toezicht kan zowel intern als extern gebeuren. Bij intern toezicht is het van belang dat een basis voor toezicht wordt vastgesteld, net als het ontwerpen en uitvoeren van toezicht procedures en het beoordelen rapporteren van resultaten. Daarnaast is het aan te bevelen dat er extern toezicht geregeld is (CBF en accountants), er is namelijk gebleken dat dit een positieve werking heeft op risicomanagement (Bijlage 1.3.4 Randvoorwaarden).

Samenvattend kan het theoretisch model (in lijn met het COSO ERM-model) in een kubus (blok) samengevat worden. Bovenop worden de soorten doelstellingen weergegeven, die gekoppeld kunnen worden aan de risico-indeling volgens RJ 400. Rechts worden de niveaus onderscheiden en op de voorkant staan de onderdelen van de cyclus weergegeven.



Figuur 4 Framework model risicomanagement

4. Aanpak enquête

Als verdere uitwerking van hoofdstuk 2 wordt in dit hoofdstuk de opzet van de enquête gedetailleerder beschreven. Tevens worden gemaakte keuzes verantwoord en onderbouwd. Allereerst wordt ingegaan op het type onderzoek, daarna op de populatie en de respons. Tevens wordt in aansluiting op de validiteit en betrouwbaarheid van het literatuuronderzoek, zoals deze behandeld is in hoofdstuk 2, de validiteit en betrouwbaarheid van de enquête besproken. Als laatste wordt een scoreleidraad opgesteld voor het meten van de resultaten van de enquête.

4.1 Type onderzoek

Zoals gezegd is de enquête een type van survey onderzoek, binnen dit type zijn er ook weer verschillende typen te onderscheiden. Het gaat in dit geval om een internetenquête. De voordelen van zo'n enquête zijn dat het goedkoop is en er veel mogelijkheden zijn die traditionele enquêtes niet hebben. Er zijn echter ook nadelen:

- Onderdekking: organisaties uit de populatie kunnen niet in de steekproef worden geselecteerd. Zo worden organisaties die geen internetadres of e-mailadres hebben niet benaderd om de enquête in te vullen;
- Zelfselectie: de onderzoeker kan niet bepalen welke organisaties de enquête invullen;
- Meetfouten: de onderzoeker kan de respondenten niet helpen bij het geven van een 'juist' antwoord. De respondent kan mogelijk vragen anders interpreteren en is mogelijk niet gemotiveerd om de enquête compleet in te vullen.[9]

Door middel van de gehanteerde aanpak worden deze drie nadelen grotendeels tot geheel ondervangen. Zo moeten fondsenwervende instellingen hun jaarverslag publiceren (via internet), wat het eerste punt ondervangt. Wat ook in de volgende paragraaf onderbouwd wordt, is dat de gehele populatie benaderd is om de enquête in te vullen, gezien de representativiteit van de steekproef (RJ 650), is de impact van het nadeel van zelfselectie gering. Wat betreft het derde nadeel, er is zo veel mogelijk gewerkt met gesloten antwoorden en de vragen zijn mede gebaseerd op een eerder enquête over risicomanagement, wat is uitgevoerd door Nyenrode Business Universiteit, Rijksuniversiteit Groningen, de Nederlandse Beroepsorganisatie van accountants (NBA) en PwC.

4.2 Opzet enquête

De vragen van de enquête zijn enerzijds gebaseerd op het literatuuronderzoek en anderzijds, zoals gezegd, op de enquête van de Nyenrode Business Universiteit, Rijksuniversiteit Groningen, de Nederlandse Beroepsorganisatie van accountants (NBA) en PwC. Wat betreft de indeling van de enquête is voornamelijk het literatuuronderzoek gebruikt, tevens zijn er op basis van het literatuuronderzoek een aantal vragen toegevoegd en weggehaald. De enquête van de Nyenrode Business Universiteit, Rijksuniversiteit Groningen, de Nederlandse Beroepsorganisatie van accountants (NBA) en PwC is gebruikt ter indicatie van welke vragen relevant zijn; een groot aantal vragen zullen dan ook (deels) overeenkomen.

4.3 Populatie onderzoek

Het totaal aantal fondsenwervende instellingen is niet nauwkeurig vast te stellen. Als gekeken wordt naar de organisaties die hun cijfers publiceren bij het CBF, gaat het om ongeveer zeshonderd organisaties. Er zitten hier echter ook organisaties tussen die RJk C2 toepassen, die niet bij de populatie fondsenwervende instellingen horen. Het aantal organisaties dat opgenomen is in het register goede doelen van het CBF bedraagt ruim 1.500. Het is echter niet duidelijk of dit alleen organisaties zijn die RJ 650 toepassen. Hoogstwaarschijnlijk is dit niet het geval, zo zijn er ook nog andere richtlijnen van toepassing (RJ 640, RJk C2 en RJk C1).

[9] (Prof. dr. J.G. Bethlehem, sd)

Voor de bepaling van de populatie is bepaald dat de organisatie RJ 650 moet toepassen en minimaal € 500.000 aan baten moet hebben. Dit is enerzijds gedaan omdat met hoge waarschijnlijkheid gezegd kan worden dat organisaties met minder dan € 500.000 aan baten vrijwel niet de middelen hebben om aan risicomanagement te doen (vooronderzoek) en anderzijds is deze grens bepaald op basis van de categorieën die volgens de erkenningsregeling onderscheiden worden. Bij de erkenningsregeling is vastgesteld dat bij een minimale grootte van € 500.000 de organisatie RJ 650 moet toepassen in het jaarverslag.[10]

Het aantal geselecteerde organisaties bedraagt in totaal 326. Dit aantal is bereikt door de populatie meerdere keren uit te breiden om de absolute respons te verhogen en daarmee de betrouwbaarheid van de enquête te verhogen. Deze organisaties zijn geselecteerd vanuit het register goede doelen van het CBF en uit de goededoelengids 2016 van Goede Doelen Nederland. Een groot gedeelte van deze organisaties zou RJ 650 moeten toepassen. Na controle is echter gebleken (aan de hand van de enquête en jaarverslagen) dat er in totaal 9 organisaties zijn (van de 326) die geen RJ 650 toepassen. Het totaal aantal organisaties dat RJ 650 toepast is dus 317. Hierbij moet wel opgemerkt worden dat er nog mogelijk meer organisaties zijn die RJ 650 niet toepassen of dat er juist nog organisaties vergeten zijn. Verder zijn er nog een aantal organisaties die gefuseerd zijn en/of dezelfde merknaam hebben.

4.4 Respons

Er zijn in totaal 326 organisaties benaderd, hierbij is geen rekening gehouden met de organisaties die geen RJ 650 toepassen, omdat dit pas later is gecontroleerd. In totaal hebben 89 organisaties de enquête ingevuld (niet rekening houdend met de onbruikbare antwoorden). Als dit in percentages wordt uitgedrukt, dan is de respons uitgedrukt in het totaal aantal benaderde organisaties, 27%. De respons uitgedrukt in het aantal organisaties dat RJ 650 toepast, is 28%.

4.5 Validiteit en betrouwbaarheid enquête

De opzet van de enquête is gebaseerd op de behandelde onderwerpen in het literatuuronderzoek en de enquête van het onderzoek van het Tweede Nationaal Onderzoek Risicomanagement in Nederland dat uitgevoerd is door Nyenrode Business Universiteit, Rijksuniversiteit Groningen, de Nederlandse Beroepsorganisatie van accountants (NBA) en PwC (validiteit). Daarnaast zijn zo veel mogelijk gesloten antwoorden opgenomen in de enquête.

In eerste instantie is gevraagd naar het e-mailadres van de financieel manager/controller. Vanuit de organisatie zelf werden dan de contactgegevens doorgestuurd van degene die belast was met risicomanagement. Een aantal organisatie hadden het e-mailadres van degene die belast was met financiën op internet staan, deze zijn ook benaderd. Daarnaast is ter controle in de enquête een vraag opgenomen wat de functie is van degene die de enquête invult (validiteit).

De enquête is specifiek gericht op organisaties die RJ 650 toepassen, ter controle is de vraag of organisaties RJ 650 toepassen derhalve ook opgenomen in de enquête. Wat betreft de representativiteit van enquête. Elke organisatie van de populatie is benaderd en had derhalve dezelfde kans om benaderd te worden. Het verschil tussen de totale populatie en het aantal organisaties dat de enquête ingevuld heeft is dus de non-respons. Hier zit ook gelijk het probleem van de betrouwbaarheid. Bij een onderzoekspopulatie van 317 organisaties en een verwachte spreiding van 50%, is de foutenmarge 9,18%.[11] Dit percentage is gebaseerd op 84 organisaties die RJ 650 toepassen. Hierbij is nog geen rekening gehouden met de werkelijke spreiding van de antwoorden en het aantal bruikbare antwoorden.

[10] (Goede Doelen Nederland en IF, 2015, p. 7 t/m 22)
[11] (Steekproefcalculator, 2013)

4.6 Scoreleidraad

Per onderdeel zijn een aantal punten toegekend, deze toekenning is gebeurd op basis van een aantal principes (Bijlage 12 De gebruikte principes voor de scoreleidraad). De weging en verdeling is bepaald op basis van deze principes, het literatuuronderzoek en de enquête Nyenrode Business Universiteit, Rijksuniversiteit Groningen, de Nederlandse Beroepsorganisatie van accountants (NBA) en PwC. Hiermee kent deze scoreleidraad subjectieve elementen, iemand anders kan andere keuzes maken die ook te verdedigen zijn.

De voorbereiding is globaal 10% van het aantal punten, het risicobeleid ongeveer 30%, het risicoproces ongeveer 40% en de randvoorwaarden ongeveer 20%. In totaal zijn er 100 punten te 'verdienen'. Aangezien het de kern vormt is daaraan derhalve de grootste weging meegegeven. Aan de voorbereiding wordt de minste weging weergegeven. Aan het risicobeleid is een hogere weging toegekend, omdat uit onderzoek is gebleken dat structuur- en cultuuraspecten van groot belang zijn voor het welslagen van risicomanagement. Aan de randvoorwaarden is meer weging toegekend als aan de voorbereiding, maar minder dan aan het risicobeleid, omdat de randvoorwaarden (toezicht, informatie en communicatie) altijd wel aanwezig zullen zijn binnen een organisatie, omdat ze ook benodigd zijn voor andere zaken.

Aan de periodiciteit is een afnemend belang toegekend naar mate de periodiciteit toeneemt, ook aan de hulpmiddelen is weinig weging toegekend. Daarnaast zijn aan diverse opsommingen maxima toegekend. Verder zijn er een aantal vragen niet meegenomen, zoals de functie van de invuller.

De weging per onderdeel is als volgt:

- Voorbereiding: maximaal 8 punten (vraag 10, 11 en 16);
- Risicobeleid: maximaal 29 punten (vraag 8, 12, 14, 15 en 17 t/m 23). Dit onderdeel gaat met name over de structuur- en cultuuraspecten:
    - Structuur: maximaal 13 punten (vraag 12, 14, 15 en 17 t/m 21);
    - Cultuur: maximaal 16 punten (vraag 8, 22 en 23);
- Risicoproces: maximaal 43 punten (vraag 24 t/m 39 en vraag 43 en 44). Dit proces valt weer onder te verdelen in:
    - Risico-identificatie en –evaluatie: maximaal 14 punten (vraag 24 t/m 27);
    - Risicobeheersing: maximaal 9 punten (vraag 23, 28 t/m 30);
    - Evaluatie en bijsturing: maximaal 8 punten (vraag 31 t/m 34);
    - Continu verbeteren: maximaal 6 punten (vraag 35 t/m 39);
    - Verantwoording: maximaal 6 punten (vraag 43 en 44);
- Randvoorwaarden: maximaal 20 punten (vraag 3, 4, 6, 7, 20, 38 40 t/m 42). Dit valt weer te verdelen in:
    - Informatie en communicatie: maximaal 12 punten (vraag 20, 38 en vraag 40 t/m 42); en
    - Toezicht: maximaal 8 punten (vraag 3, 4, 6 en 7).

Zie bijlage 11 voor een specificatie van de verdeling van het aantal punten per vraag.

Er zijn 69 organisaties die de enquête helemaal ingevuld hebben. Van deze 69 organisaties hebben 64 organisaties zichzelf een cijfer gegeven. Voor het analyseren van de scores van de fondsenwervende instellingen zijn deze 64 organisaties gebruikt. Het verschil wordt grotendeels veroorzaakt door organisaties die niet aan risicomanagement doen, 3 organisaties die niet aan risicomanagement doen, hebben zichzelf geen cijfer gegeven. Voor de verwerking van de resultaten per vraag is het aantal antwoorden aangehouden dat bij die vraag is ingevuld.

De resultaten zijn uiteindelijk met behulp van Microsoft Excel verwerkt. Het programma SPSS is wel overwogen, maar daar is niet voor gekozen. Dit gezien de beschikbare tijd; om de functies van SPSS juist en volledig te kunnen gebruiken, is tijd nodig.

5. Onderzoeksresultaten en analyse enquête

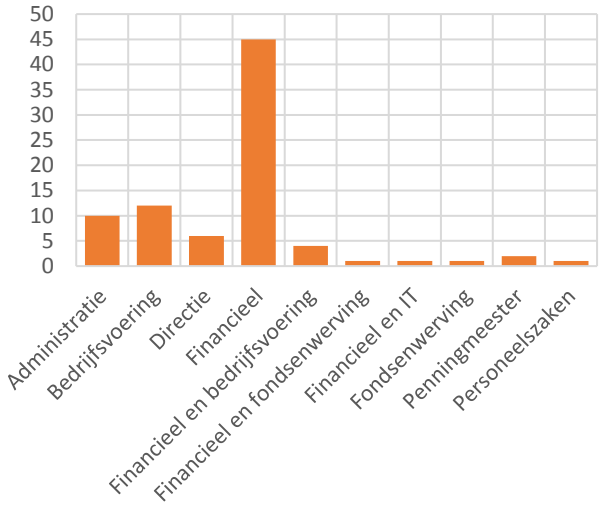
In de eerste paragraaf zullen de onderzoeksresultaten per vraag worden behandeld. In de tweede paragraaf zal er geprobeerd worden om relaties tussen vragen te onderzoeken. In de derde paragraaf zullen de behaalde scores besproken worden en als laatste wordt een vergelijking tussen de klanten van WITh en niet-klanten gemaakt.

5.1 Onderzoeksresultaten

In het totaal hebben 89 organisaties de enquête (gedeeltelijk) ingevuld. Hiervan waren er 84 die RJ 650 toepasten. Aangezien de scope van dit onderzoek beperkt is tot fondsenwervende instellingen, zijn alleen deze organisaties meegenomen in onderstaande grafieken. Hierbij dient vermeld te worden dat onderstaande figuren gebaseerd zijn op het totaal aantal gegeven antwoorden per vraag. Er is een figuur weergegeven wanneer de mogelijke opties meer dan 3 bedroegen.

Vraag 1. Wat is uw functie?

Deze vraag is in totaal door 83 mensen ingevuld. Aan de hand van de antwoorden zijn er 10 categorieën aangemaakt. Hiernaast is de verdeling per onderscheiden categorie weergegeven.



Figuur 5 Functie van degene die de enquête invult

Vraag 2. Wat was de hoogte van de baten in 2015 en 2016?

Deze vraag is door 83 organisaties ingevuld. De baten van 1 organisatie zijn niet meegenomen. De totale baten van 2015 van alle benaderde organisaties (zie vorig hoofdstuk) is € 3,9 miljard. Als alle baten van 2015 van de organisaties (82 organisaties) die de deze vraag (geldig) hebben ingevuld, worden opgesteld, komt er een bedrag van ongeveer € 1,2 miljard uit. Dit is dus ruim 31%, dit is meer dan het aantal organisaties (82) ten opzichte van het totale aantal (326) organisaties, dit is namelijk ruim 25%. De gemiddelde hoogte (€ 15 miljoen) van de baten van de organisaties die deelgenomen hebben aan deze enquête ligt dus hoger dan de gemiddelde hoogte (€ 12 miljoen) van de baten van de organisaties van de gehele populatie.

Vraag 3. Is er sprake van een toezichthoudend orgaan? (RvC, bestuur, RvT)

Bij vraag 3 zijn er in totaal 84 antwoorden gegeven, waarvan 81 (96,43%) organisaties de vraag hebben beantwoord met ‘ja’ en 3 (3,57%) organisaties met ‘nee’.

Vraag 4. Is er binnen het toezichthoudend orgaan sprake van een Audit Commissie?

Er zijn hier 49 (59,76%) bevestigende antwoorden gegeven en 33 (40,24%) ontkennende antwoorden, dit brengt het totaal aantal antwoorden op 82. Van de 3 organisaties die de vorige vraag met ‘nee’ beantwoord hebben, is er één organisatie geweest die deze vraag met ‘ja’ beantwoord heeft. Deze organisatie is niet meegenomen in het bepalen van de scores.

Vraag 5. Wordt in het jaarverslag RJ 650 Fondsenwervende instellingen toegepast?

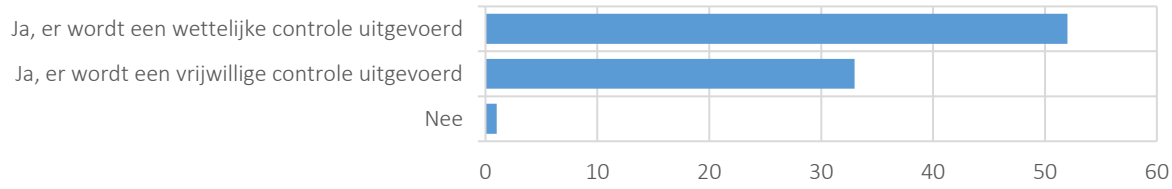
Dit is de vraag waarop is gefilterd binnen de enquête. Toch wordt deze vraag even kort toegelicht, in totaal hebben 88 organisaties deze vraag beantwoord. 1 organisatie had de enquête al ingevuld, voordat deze vraag is toegevoegd aan de enquête, deze organisatie past RJ 650 toe. Er passen 84 organisaties (94,38%) RJ 650 toe en 5 (5,62%) organisaties niet.

6. Is de organisatie aangesloten bij de erkenningsregeling?

Er wordt nu weer verder gegaan met de selectie van 84 organisaties die RJ 650 toepassen. Er zijn in totaal 84 antwoorden gegeven, waarvan 76 (90,48%) 'ja' en 8 (9,52%) 'nee'.

7. Wordt de jaarrekening door een accountant gecontroleerd?

Er zijn in totaal 83 antwoorden gegeven, het verschil van 1 met de 84 organisaties betreft een organisatie die wel heeft deelgenomen aan de enquête, maar nog niet klaar is. Van de 83 organisaties is er één organisatie waarvan de jaarrekening niet gecontroleerd wordt, bij 33 organisaties wordt een vrijwillige controle uitgevoerd en 52 organisaties geven aan dat er een wettelijke controle wordt uitgevoerd. De opties voor het samenstellen van een jaarrekening en de beoordeling ervan, waren ook weergegeven. Geen enkele organisatie heeft deze echter aangekruist.

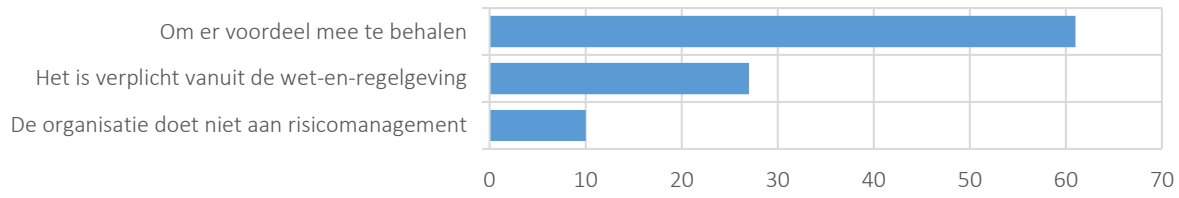


Figuur 6 Controle van de jaarrekening

Dit betekent dat bij 3 organisaties zowel een vrijwillige als een wettelijke controle wordt uitgevoerd. Op de scores heeft dit geen invloed gehad, omdat er aan zowel de uitvoering van een vrijwillige controle als de uitvoering van een wettelijke controle 3 punten is toegekend, met een maximum van in totaal 3 punten. Aan de hand van de baten is gecontroleerd welke van de opties van toepassing is, bij alle drie de organisaties was de hoogte van de baten lager dan € 8,8 miljoen. Bij deze drie organisaties is dus sprake van een vrijwillige controle. Het is tevens vreemd dat bij 50 organisaties een wettelijke controle wordt uitgevoerd, een wettelijke controle is namelijk alleen van toepassing wanneer een stichting of een vereniging een onderneming in stand houdt en die minimaal twee jaar op rij voldoet aan twee van de drie criteria. Uit eerder onderzoek van het CBF is bovendien gebleken (Bijlage 10 Wet- en regelgeving met betrekking tot verenigingen en stichtingen) dat slechts een tiental organisaties een onderneming in stand houden. De gegeven antwoorden met betrekking tot de uitvoering van een wettelijke controle lijken daarom voor een groot deel onjuist. Zoals gezegd maakt dit voor de scores niet uit.

8. Waarom doet de organisatie aan risicomanagement?

Er zijn in totaal 82 antwoorden gegeven, 10 organisaties doen niet aan risicomanagement, 27 organisaties doen het omdat het verplicht is en 61 organisaties doen het om er voordeel mee te behalen. Van de 27 organisaties zijn er 16 organisaties die het enerzijds doen vanwege de wet- en regelgeving, maar anderzijds ook om er voordeel meet te behalen. Dit betekent dat er 9 organisaties zijn die het alleen doen vanwege de wet- en regelgeving en 45 organisaties doen het alleen maar om er voordeel mee te behalen. Van de 10 organisaties die volgens zichzelf aan niet aan risicomanagement doen, vult toch nog een aantal een aantal vragen in, het is dus de vraag of het aantal organisaties (10), die helemaal niet doen aan risicomanagement, wel een volledig beeld geeft van de werkelijkheid.



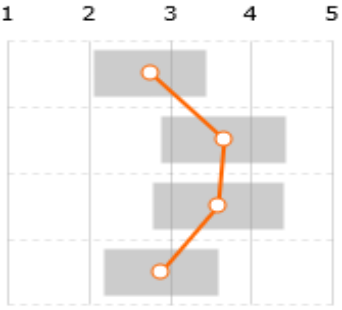
Figuur 7 Redenen voor risicomanagement

Vraag 9. In welke mate verwacht u er voordeel mee te behalen?

In totaal zijn er 69 antwoorden gegeven. Van de 61 organisaties die aangegeven hebben er voordeel mee te behalen, hebben 57 organisaties deze vraag ingevuld. Van de 9 organisaties die aangegeven hebben, niet aan risicomanagement te doen, hebben 4 organisaties vraag 9 ingevuld. Dit betekent dat 8 van de 9 organisaties die alleen aan risicomanagement doen omdat het verplicht is vanwege de wet- en regelgeving, verwachten er toch voordeel mee te behalen. Het cijfer '1' geeft aan dat er naar verwachting zeer weinig voordeel mee behaald wordt en '5' geeft aan dat er naar verwachting zeer veel voordeel mee behaald zal worden. Er waren vier opties:

1. Stabielere resultaten (financieel);
2. Het beperken van de impact van risico's;
3. Het verminderen van de kans op risico's; en
4. Het verbeteren van het resultaat.

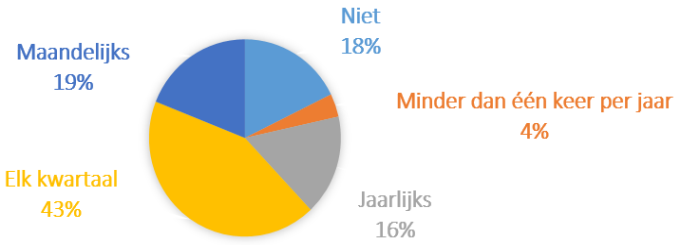
De oranje lijn geeft het gemiddelde aan en de grijze vlakken de standaardafwijking.



Figuur 8 Verwacht voordeel met betrekking tot risicomanagement

Vraag 10. Worden er binnen de organisatie managementrapportages uitgebracht waarin de veranderingen binnen en buiten de organisatie aan bod komen?

Deze vraag is in totaal door 79 organisaties ingevuld en is onderdeel van de eerste stap 'voorbereiding' volgens de cyclus van risicomanagement. Voor de verdeling van de antwoorden van de 79 organisaties over de verschillende opties, zie de figuur rechts. 'Wekelijks' was ook nog een optie, maar deze optie heeft geen antwoorden gekregen.



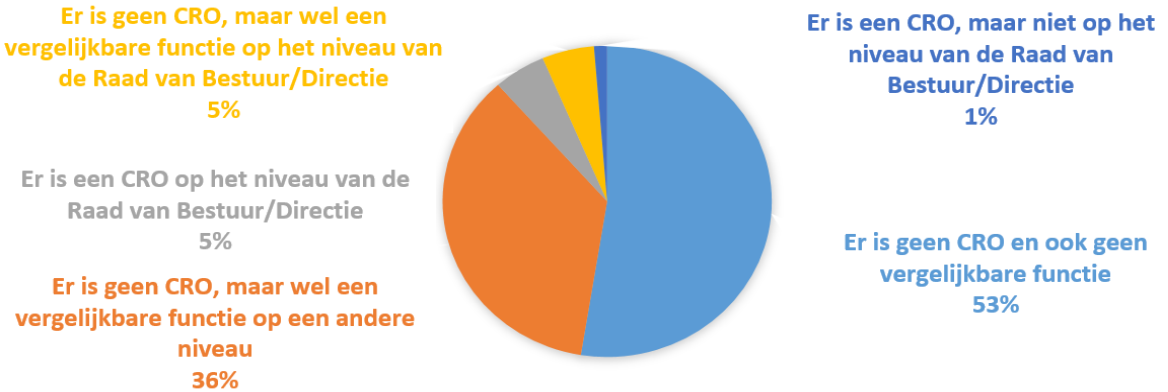
Figuur 9 Periodiciteit managementrapportages

Vraag 11. Gebruikt de organisatie de opgedane informatie van de managementrapportages voor risicomanagement? Denk bijvoorbeeld aan de risico-inventarisatie.

Er hebben 69 organisaties deze vraag ingevuld. 51 (73,91%) organisaties hebben 'ja' ingevuld en 18 (26,09%) 'nee'. Als gekeken wordt naar het aantal organisaties dat bij de vorige vraag niet 'Niet' hebben ingevuld, zijn er dat 65. Het verschil tussen 69 en 65 wordt veroorzaakt doordat 4 organisaties die bij vraag 11, 'Niet' hebben ingevuld, bij de vraag ook het antwoord 'nee' hebben gegeven.

Vraag 12. Is er sprake van een CRO (Chief Risk Officer) binnen de organisatie (of een vergelijkbare functionaris die eindverantwoordelijk is voor risicomanagement)?

Er zijn in totaal 78 antwoorden gegeven, waarvan het overgrote deel van de antwoorden 'geen CRO' betrof. Zie voor de exacte verdeling, de figuur hieronder.



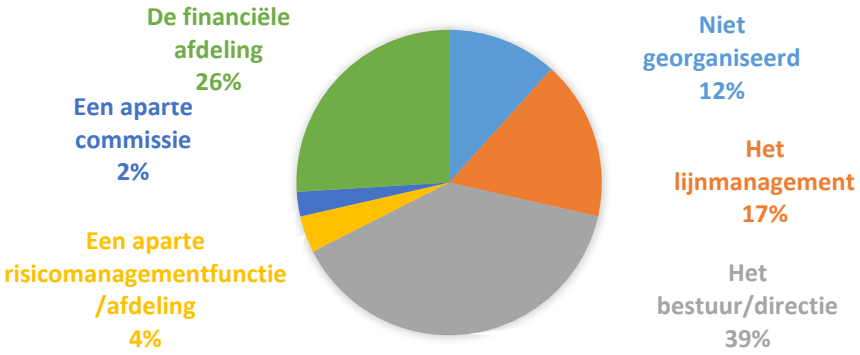
Figuur 10 Eindverantwoordelijke voor risicomanagement

Vraag 13. Heeft de CRO of de vergelijkbare functie een uitvoerende of een adviserende taak?

Er zijn in totaal 39 antwoorden gegeven. 30 (76,92%) organisaties geven aan dat de CRO of de vergelijkbare functie zowel een uitvoerende als een adviserende taak hebben, 4 (10,26%) geven aan dat deze rol alleen adviserend is en bij 5 (12,82%) organisaties is deze rol alleen uitvoerend.
Als gekeken wordt naar de vorige vraag dan zijn er 37 organisaties die een CRO of een vergelijkbare functie hebben. Het verschil (2) wordt veroorzaakt doordat er twee organisaties zijn die bij vraag 12 aangegeven hebben dat er geen CRO en geen vergelijkbare functie is, maar bij deze vraag hebben aangegeven dat de CRO of de vergelijkbare functie zowel een adviserende als een uitvoerende taak hebben. Deze vraag is niet meegenomen in de scores en heeft derhalve geen invloed op de scores.

Vraag 14. Wie coördineert de activiteiten met betrekking tot risicomanagement?

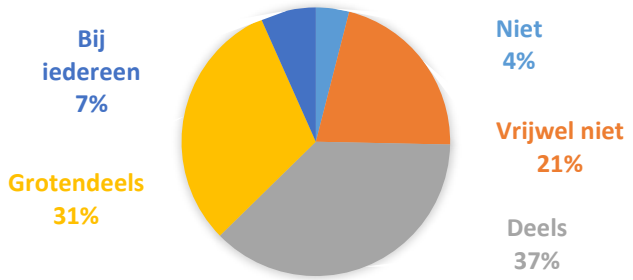
Er zijn in totaal 77 antwoorden gegeven, het grootste gedeelte gaf de antwoorden 'Het bestuur/directie' of 'De financiële afdeling', de andere opties en verdeling zijn hieronder weergegeven.



Figuur 11 Coördinatie risicomanagement

Vraag 15. Zijn de verantwoordelijkheden, taken en bevoegdheden met betrekking tot risicomanagement binnen de organisatie bekend?

Er zijn in totaal 75 antwoorden gegeven, het grootste gedeelte zit tussen deels en grotendeels. De afname in antwoorden wordt (tot nu toe) voornamelijk veroorzaakt door organisaties die de enquête niet helemaal hebben ingevuld.



Figuur 12 Bekendheid verantwoordelijkheden, taken en bevoegdheden

Vraag 16. Heeft de organisatie risicomanagementdoelstellingen opgesteld?

72 organisaties hebben deze vraag beantwoord. 33 (45,83%) organisaties geven aan dat ze geen risicomanagementdoelstellingen hebben opgesteld. De rest doet dit wel, hiervan zijn er 24 (33,33%) organisaties die ze koppelen aan de organisatiedoelstellingen, de overige 15 (20,83%) doet dit niet. De daling in de antwoorden ten opzichte van de vorige vraag wordt grotendeels (2) veroorzaakt doordat organisaties die eerder aangegeven hebben, niet aan risicomanagement te doen, minder antwoorden (gaan) geven.

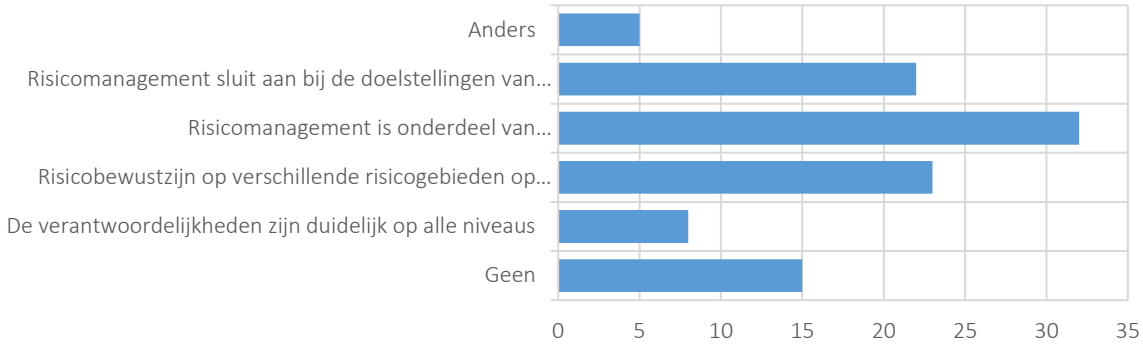
Vraag 17. Welke voorwaarden heeft de organisatie gesteld voor (effectief) risicomanagement?

Er zijn in totaal 70 antwoorden gegeven, in deze vraag is een mogelijkheid voor een open antwoord toegevoegd. Vijf organisaties hebben van deze optie gebruik gemaakt, de gegeven antwoorden zijn:

- Update Quality Management System;

- Periodieke toetsing;
- Onderdeel van besluitvorming op directie niveau niet op alle niveaus;
- Procedures in algemene zin opgesteld om risico's te voorkomen; en
- Kleine organisatie; risico's die gesignaleerd worden bespreekt men onderling.

Het grootste gedeelte van de organisatie heeft echter gekozen voor de voorwaarde: 'Risicomanagement is onderdeel van (besluitvormings)processen'.



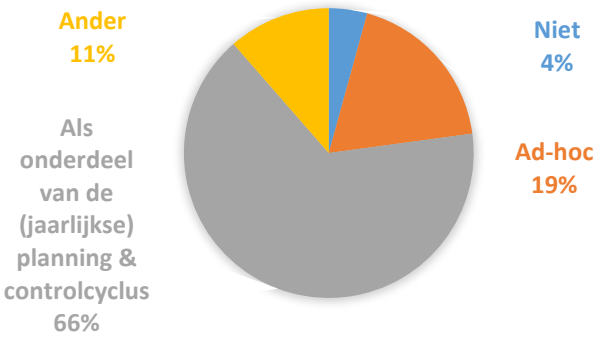
Figuur 13 Voorwaarden voor (effectief) risicomanagement

Vraag 18. Hoe voert de organisatie het risicomanagementproces uit?

Er zijn in totaal 70 antwoorden gegeven, net als in deze vraag is er een mogelijkheid voor een open antwoord toegevoegd. Er zijn in totaal 8 open antwoorden gegeven:

- ISO9001;
- Staat op agenda voor de volgende jaarrekening (over 2017);
- Nu nog ad hoc, na een dit jaar op te stellen risico-analyse als onderdeel van de planning en controlcyclus;
- In relatie met beslissingen;
- Proces wordt nu gestructureerd;
- Voornamelijk onderdeel van Meerjaren beleidsplan;
- Door de procedures te volgen en de procedures jaarlijks te monitoren; en
- Bij het beoordelen van een aanvraag voor een bijdrage of een lening.

Bij de tweede en de vijfde antwoord, zijn de antwoorden gecorrigeerd in de scores, omdat dit niet over het 'nu' gaat, maar over de toekomst. Verder heeft vrijwel elk antwoord het karakter van ad-hoc.
Zoals hiernaast in de figuur weergegeven, geeft het grootste gedeelte aan, dat het onderdeel is van de (jaarlijkse) planning & controlcyclus.

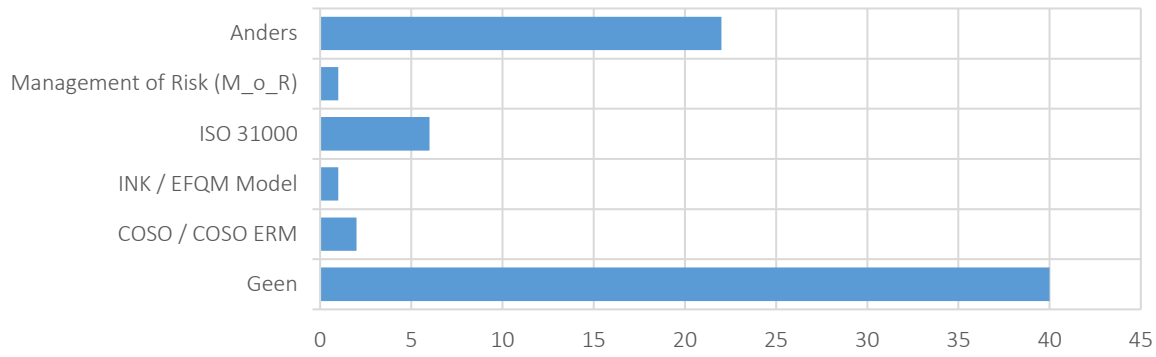


Figuur 14 Manier van uitvoering van risicomanagement

Vraag 19. Welk model gebruikt de organisatie voor risicomanagement?

In totaal zijn er bij deze vraag 72 antwoorden. Bij de vorige vraag zijn 70 antwoorden gegeven. Het verschil in aantal ingevulde antwoorden met de vorige vraag wordt veroorzaakt doordat één organisatie, die niet aan risicomanagement doet, de vorige vraag niet ingevuld heeft, maar deze vraag wel, deze organisatie heeft overigens het antwoord 'Geen' gekozen. De andere organisatie die de vorige vraag niet heeft ingevuld, heeft bij deze vraag het (gesloten) antwoord 'Anders' gegeven. Naast

de opties die hieronder zijn weergegeven, was er ook nog de optie INTOSAI, geen enkele organisatie heeft deze echter aangevinkt.



Figuur 15 Gebruik van modellen van risicomanagement

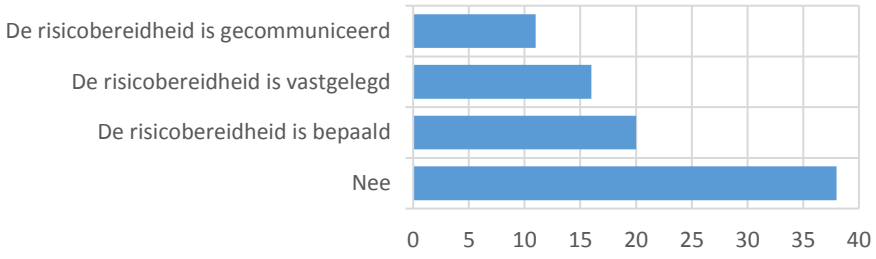
Rond (± 1 dag) 20 maart is er naar aanleiding van het relatief hoge aantal 'Anders' antwoorden, besloten om van het antwoord 'Anders' een open antwoord te maken. De acht open antwoorden die na deze datum gegeven zijn, zijn:

- Eigen intern model;
- Maandrapportage;
- Eigen model;
- Gericht op vereisten erkenningsregeling GDN;
- Grant Thornton-methode voor MKB;
- ISO 9001: 2015;
- Eigen; en
- Eigen inschatting.

Op basis van de gegeven antwoorden is het aannemelijk om te concluderen dat een groot deel van de overige antwoorden (14) ook betrekking heeft op een 'eigen model' of 'eigen inschatting'.

Vraag 20. Is binnen de organisatie de risicobereidheid bepaald, vastgelegd en gecommuniceerd?

In totaal hebben 69 organisaties een antwoord gegeven, er waren echter meerdere antwoorden mogelijk. Zo hebben van de 20 organisatie die aangegeven hebben dat de risicobereidheid is bepaald, 8 organisaties aangegeven dat de risicobereidheid is vastgelegd en 5 dat ook de risicobereidheid is gecommuniceerd. Het aantal antwoorden per optie is hiernaast weergegeven.



Figuur 16 Risicobereidheid

Vraag 21. Wordt beloning en waardering gekoppeld aan de uitvoering van risicomanagement?

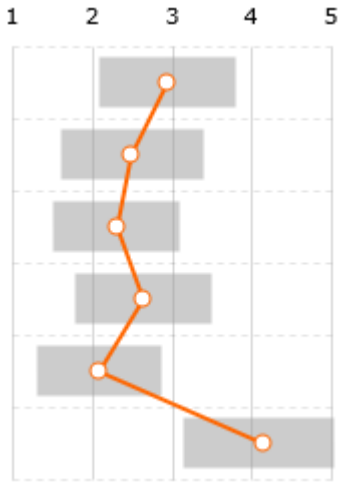
Er zijn in totaal 72 antwoorden gegeven, drie organisaties die de vorige vraag niet hebben beantwoord, hebben deze vraag wel beantwoord. Het verschil is niet direct te achterhalen, dit zijn mogelijk organisaties die het antwoord op de vorige vraag niet wisten. Het grootste gedeelte (95,83%) geeft aan dat er geen relatie is tussen de beloning en waardering en de uitvoering van risicomanagement. 3 (4,17%) organisaties geven aan dat er een indirecte (formele) relatie bestaat en geen enkele organisatie geeft aan dat er een directe (formele) relatie bestaat tussen de beloning en waardering en de uitvoering van risicomanagement.

Vraag 22. In welke mate zijn de volgende stellingen over risicomanagement van toepassing binnen de organisatie?

In totaal zijn er 68 antwoorden gegeven, dit komt doordat een aantal organisaties die aangegeven hebben niet aan risicomanagement doen, deze vraag niet ingevuld hebben. Bij deze vraag werden 6 stellingen aan de organisatie voorgelegd:

- Risicomanagement leidt tot toevoeging van waarde aan de organisatie;
- Personeelsleden mogen fouten maken, zolang ze er maar van leren;
- Het bestuur/directie geeft het goede voorbeeld;
- Overtredingen van interne regels worden serieus genomen;
- Medewerkers kunnen vrij communiceren over risico's richting leidinggevenden; en
- De beloningsstructuur zorgt voor effectief risicomanagement.

De antwoorden varieerden van 'Zeer veel van toepassing' (1) tot 'Zeer weinig van toepassing'(5). De oranje lijn geeft het gemiddelde weer en de grijze vlakken de standaardafwijking.



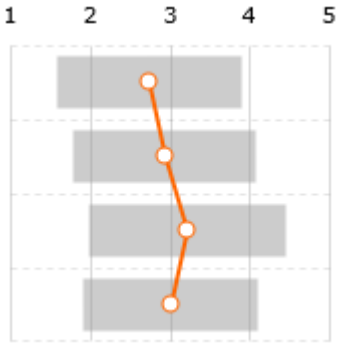
Figuur 17 Risicocultuur

Vraag 23. In welke mate zijn de volgende stellingen van toepassing binnen de organisatie?

Ook deze vraag werd door 68 organisaties ingevuld en ook bij deze vraag werden er een aantal stellingen voorgelegd, in dit geval waren het er 4:

- Iedereen binnen de organisatie is zich bewust van de noodzaak tot risicomanagement;
- Iedereen binnen de organisatie is bekend met de (belangrijkste) risico's
- Iedereen binnen de organisatie voert de genomen maatregelen uit; en
- Iedereen binnen de organisatie is er zich bewust dat elk moment er zich risico's kunnen voordoen.

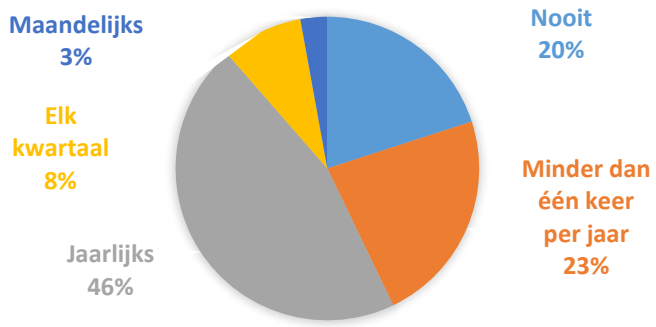
De antwoorden variëren van 'Vrijwel niemand' (1) tot 'Vrijwel iedereen' (5).



Figuur 18 Risicobewustzijn

Vraag 24. Hoe vaak wordt binnen de organisatie een (bedrijfsbrede) risico-inventarisatie en risico-evaluatie uitgevoerd?

Deze vraag is door 70 organisaties ingevuld; het is de opmaat van het onderdeel risico-identificatie en –evaluatie. Bijna de helft geeft aan dat ze jaarlijks een (bedrijfsbrede) risico-inventarisatie en risico-evaluatie uitvoeren. Toch is het aandeel van organisaties die nooit een risico-inventarisatie en risico-evaluatie uitvoeren, toch nog hoog, namelijk 20%.

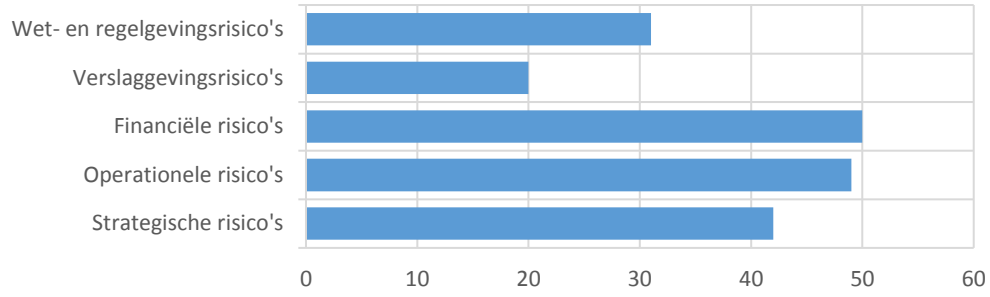


Figuur 19 Periodiciteit (bedrijfsbrede) risico-inventarisatie en -beoordeling

Vraag 25. Wat voor soort risico's brengt de organisatie hierbij in kaart?

In totaal hebben 56 organisaties ingevuld. Het verschil met de vorige vraag zit in het aantal organisatie die bij de vorige vraag 'Nooit' hebben ingevuld, dat waren er 14. Als gekeken wordt naar wat voor soort risico's het meeste in kaart worden gebracht, zijn dit operationele en financiële risico's.

Verslaggevingsrisico's worden het minst in kaart gebracht, zie voor de exacte verdeling de figuur hieronder. Gemiddeld gezien brengen organisaties meer dan 3 soorten risico's in kaart.



Figuur 20 Inventarisatie soorten risico's

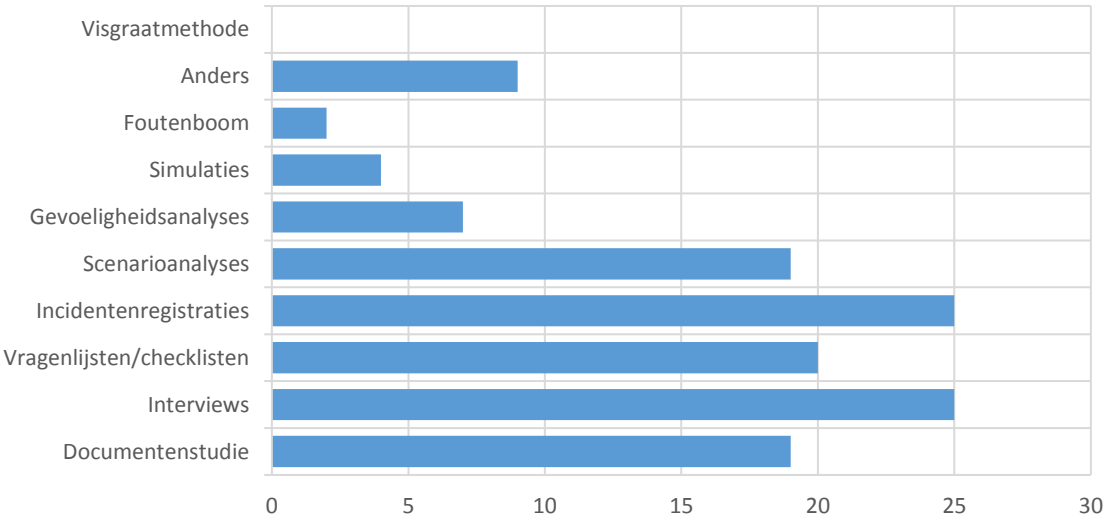
Vraag 26. Van welke hulpmiddelen maakt de organisatie gebruik bij risico-inventarisatie en risico-evaluatie?

Van de 56 organisaties die een (bedrijfsbrede) risico-inventarisatie en risico-evaluatie uitvoeren, hebben 53 organisaties deze vraag ingevuld. Gemiddeld geven organisaties aan meer dan 2 hulpmiddelen te gebruiken. 3 organisaties die bij vraag 24 niet het antwoord 'Nooit' hebben ingevuld, hebben deze vraag niet beantwoord. De antwoorden van deze organisaties zijn vanwege mogelijke verschillen van interpretatie bij vraag 24 wel meegeteld.

Gevoeligheidsanalyses, simulaties en de foutenboom worden als hulpmiddelen het minst gebruikt en de visgraatmethode wordt helemaal niet gebruikt, de overige hulpmiddelen worden vaker gebruikt. Bij deze vraag is de mogelijkheid tot een open antwoord gegeven. Er zijn in totaal 9 open antwoorden gegeven:

- Eigen zorgmodel dat uiteraard is gebaseerd op een gebruikelijke risico- inventarisatie;
- Eigen rapportages structuur;
- Eigen inzichten en ervaring;
- Maken van inschattingen van risico's;
- Inventarisatie wordt nu gestructureerd;
- Overleg met Management Team: wat zijn de 10 belangrijkste risico's?
- Process analysis / workshops / group discussions;
- Dagelijks overleg van werkzaamheden in een klein team, wekelijks teamoverleg en wekelijks stafoverleg.

Het vijfde antwoord is niet meegenomen in de scores.



Figuur 21 Hulpmiddelen bij risico-inventarisatie en risico-evaluatie

Vraag 27. Voert de organisatie de risico-evaluatie tegelijk uit met de risico-inventarisatie of worden deze apart uitgevoerd?

Deze vraag zijn door dezelfde organisaties ingevuld als bij vraag 24, er zijn dus 56 antwoorden. 25 (44,64%) organisaties zegt hierbij geen vaste volgorde aan te houden. 18 (32,14%) organisaties geven aan dat ze het tegelijkertijd uitvoeren en 13 (23,21%) organisaties voeren eerst de inventarisatie en dan pas de evaluatie uit.

Vraag 28. Welke strategie voert de organisatie uit bij wat voor soort risico?

Deze vraag sluit het gedeelte van de risico-identificatie en –evaluatie af en begint de risicobeheersing. Deze vraag is in totaal door 59 organisaties ingevuld. Bij deze vraag worden vier soorten risico's tegenover de mogelijke reacties gezet (zie tabel hieronder).

Tabel 5 Koppeling tussen strategie en soorten risico's

	Het vermijden van risico	Het verminderen van de kans op risico	Het beperken van de impact van risico	Het overdragen van risico	Het accepteren van risico	Geen	Totaal
Risico met hoge kans en hoge impact	25 (42,37%)	33 (55,93%)	25 (42,73%)	5 (8,47%)	4 (6,78%)	4 (6,78%)	96
Risico met hoge kans en lage impact	4 (6,78%)	33 (55,93%)	11 (18,64%)	6 (10,17%)	13 (22,03%)	8 (13,56%)	75
Risico met lage kans en hoge impact	12 (20,34%)	14 (23,73%)	35 (59,32%)	12 (20,34%)	9 (15,25%)	4 (6,78%)	86
Risico met lage kans en lage impact	3 (5,08%)	11 (18,64%)	8 (13,56%)	5 (8,47%)	33 (55,93%)	11 (18,64%)	71
Totaal	44	91	79	28	59	27	328

Gemiddeld gezien heeft elke organisatie per situatie meer dan één strategie toegepast, waarbij het verminderen van de kans op risico het meeste wordt toegepast, daarna het beperken van de impact van risico en het accepteren van risico. De weergegeven percentages zijn de getallen in de desbetreffende cel uitgedrukt in het aantal organisaties die deze vraag heeft ingevuld.

Vraag 29. Voert de organisatie voordat een maatregel genomen wordt, een kosten-batenanalyse uit?

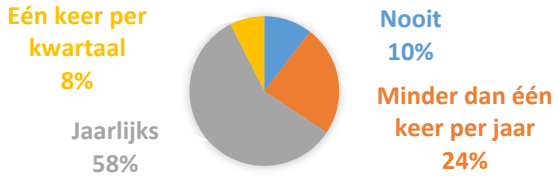
In totaal zijn er 67 antwoorden gegeven. Dit zijn er 8 meer dan de vorige vraag. Dit komt enerzijds door organisaties die eerder aangegeven hebben niet aan risicomanagement te doen en daarom niet alle vragen invullen. Anderzijds zijn het organisaties die wel begonnen zijn, maar nog niet klaar zijn met het invullen van de enquête, verder is het mogelijk dat een aantal organisaties de vorige 3 vragen niet hebben ingevuld, vanwege te weinig kennis of het niet begrijpen van de vraag.
Als gekeken wordt naar de gegeven antwoorden bij deze vraag, geven 45 (67,16%) organisaties aan dat ze eerst een kosten-batenanalyse uitvoeren, 22 (32,84%) organisaties doet dit niet.

Vraag 30. Wordt bij het accepteren van risico's, rekening gehouden met de capaciteit om risico te kunnen dragen?

Ook dit is weer een ja-nee vraag, die door dezelfde organisaties zijn ingevuld als bij de vorige vraag. 55 (82,09%) organisaties hebben hier 'ja' ingevuld en 12 (17,91%) organisaties hebben hier 'nee' ingevuld.

Vraag 31. Hoe vaak worden de genomen beheersingsmaatregelen geëvalueerd?

Ook deze vraag is door 67 organisaties ingevuld. Het grootste gedeelte geeft aan de genomen beheersingsmaatregelen jaarlijks te evalueren.



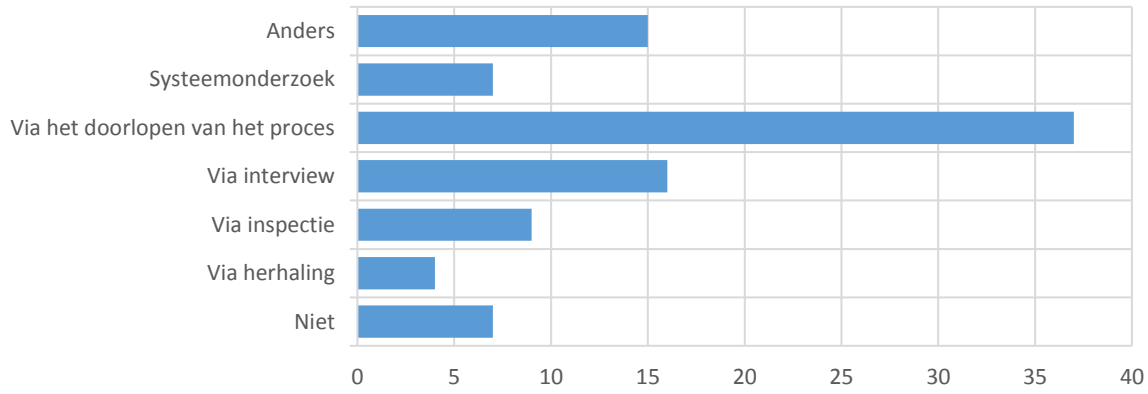
Figuur 22 Periodiciteit evaluatie beheersingsmaatregelen

Vraag 32. Hoe evalueert de organisatie de uitvoering van de genomen maatregelen?

Deze vraag is door 62 organisaties ingevuld, van 7 organisaties die bij de vorige vraag 'Niet' hebben 2 organisaties deze vraag ook ingevuld, dit verklaart het verschil tussen de aantal gegeven antwoorden tussen deze en de vorige vraag. Bij deze vraag zijn er in totaal 15 open antwoorden gegeven:

- Halfjaarlijkse interne controle toetsing;
- Peer review, "oog van de meester maakt paard vet";
- Nadenken of er verbeteringen nodig zijn;
- Aan de hand van het resultaat;
- Simulatie (veiligheidsrisico);
- Gesprek financiële commissie;
- Bespreking met bestuur;
- Proces wordt nu gestructureerd;
- Bespreking met Management Team;
- Internal audits;
- Via overleg met accountant;
- Dagelijks samenwerken;
- Doorlopend;
- Ad hoc; en
- Internal audit; management rapportage.

Als gekeken wordt naar deze open antwoorden, valt op dat een deel niet zo zeer een hulpmiddel aangeeft, maar meer de manier waarop. Toch is besloten deze antwoorden wel mee te nemen in de scores omdat het aangeeft dat ze iets doen/gebruiken voor de evaluatie. Bij het antwoord 'Proces wordt nu gestructureerd' is echter besloten om deze niet mee te laten tellen in de scores.



Figuur 23 Hulpmiddelen bij de evaluatie van beheersingsmaatregelen

Er zijn toch nog 7 organisaties geweest die hier 'Niet' hebben ingevuld, zoals gezegd zijn er 2 organisatie die bij de vorige vraag ook 'Nooit' hebben ingevuld, verder is er één organisatie geweest die naast 'Niet' ook nog andere antwoorden heeft gegeven. Er zijn dus 4 organisaties die hier het antwoord 'Niet' hebben gegeven en bij de vorige vraag niet 'Nooit'. Na controle bleken dit organisaties te zijn die het antwoord 'Minder dan één keer per jaar' hebben gegeven. Er is besloten om de 4 antwoorden van vraag 31 toch mee te tellen, omdat ze niet hebben gekozen voor het antwoord

'Nooit', bovendien hebben ze de volgende twee vragen ook ingevuld. Bij vraag 32 zijn er geen punten toegekend voor de antwoorden.

Gemiddeld gezien geven organisaties aan (meer dan) 1 hulpmiddel te gebruiken.

Vraag 33. Maakt de organisatie hierbij gebruik van prestatie-indicatoren?

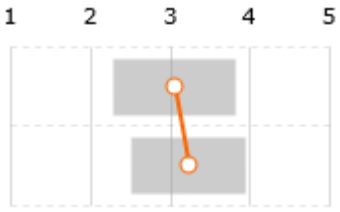
Deze vraag is ingevuld door 62 organisaties. Er zijn 2 organisaties die bij de vorige 2 vragen respectievelijk 'Niet' en 'Nooit' hebben ingevuld, deze vraag met 'ja' hebben beantwoord. Deze antwoorden zijn gecorrigeerd in de scores. In totaal hebben 23 (37,10%) organisatie deze vraag met 'ja' beantwoord en 39 (62,90%) organisaties met 'nee'.

Vraag 34. Krijgt de organisatie feedback van de (externe) accountant over risico's en risicomanagement?

In totaal zijn er 66 antwoorden gegeven. Hiervan is het overgrote deel 'ja'. Om precies te zijn hebben 60 (91,91%) organisaties een bevestigend antwoord gegeven en 6 (9,09%) organisaties een ontkennend antwoord.

Vraag 35. In welke mate volgt de organisatie de verbeterpunten op die naar voren kwamen uit de evaluatie?

Deze vraag is het begin van het onderdeel 'continu verbeteren'. In totaal zijn er 63 antwoorden gegeven. De factoren snelheid en kwaliteit (eerst snelheid dan kwaliteit) werden hierbij beoordeeld. Over deze factoren kon men een oordeel geven, dit varieerde van onvoldoende (1) tot uitstekend (5).



Figuur 24 Opvolging verbeterpunten

Vraag 36. Formuleert de organisatie ambities met betrekking tot risicomanagement?

Deze vraag is in totaal door 66 organisaties ingevuld. 23 (34,85%) organisaties geven aan ambities te formuleren. De rest (65,15%) geeft aan dit niet te doen.

Vraag 37. Vergelijkt de organisatie haar prestaties op het gebied van risicomanagement met andere organisaties?

In totaal zijn er 65 antwoorden gegeven. 14 (21,54%) organisaties hebben hier het antwoord 'ja' gegeven en 51 (78,46%) organisaties het antwoord 'nee'.

Vraag 38. Worden de 'best practices' en kennis binnen de organisatie gedeeld/gecommuniceerd?

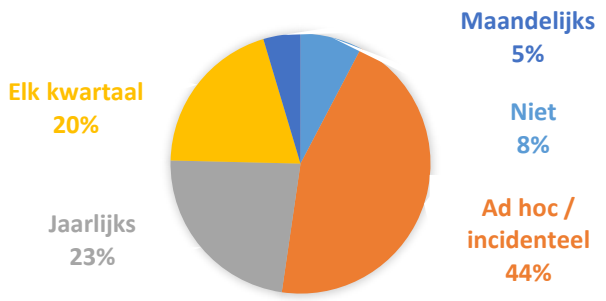
Er zijn in totaal 64 organisaties die deze vraag hebben ingevuld. 36 (56,25%) organisaties delen/communiceren 'best practices' en kennis binnen de organisatie, 28 (43,75%) organisaties doen dit niet.

Vraag 39. Biedt de organisatie personeelsleden trainingen, cursussen, opleidingen, workshops en dergelijke aan (o.a. met betrekking tot risicomanagement)?

Er zijn in totaal 65 antwoorden gegeven. 28 (43,08%) organisaties hebben een bevestigend antwoord gegeven en 37 (56,92%) een ontkennend antwoord.

Vraag 40. Hoe vaak vindt er binnen de organisatie overleg plaats over risico's en risicomanagement?

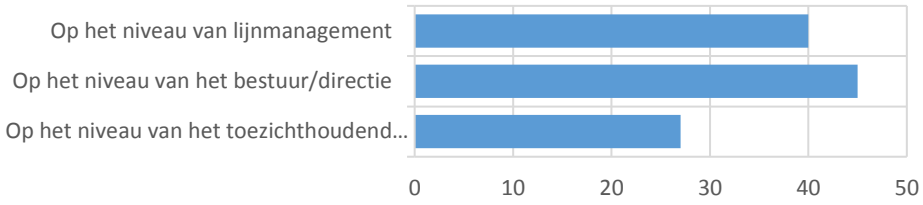
Met deze vraag wordt het onderdeel 'continu verbeteren' afgesloten en wordt het onderdeel 'informatie en communicatie' begonnen. Deze vraag is in totaal door 65 organisaties beantwoord. Het grootste gedeelte van de organisaties voert slechts incidenteel of ad-hoc overleg over risico's en risicomanagement.



Figuur 25 Periodiciteit overleg over risicomanagement

Vraag 41. Op welk niveau speelt dit overleg zich af?

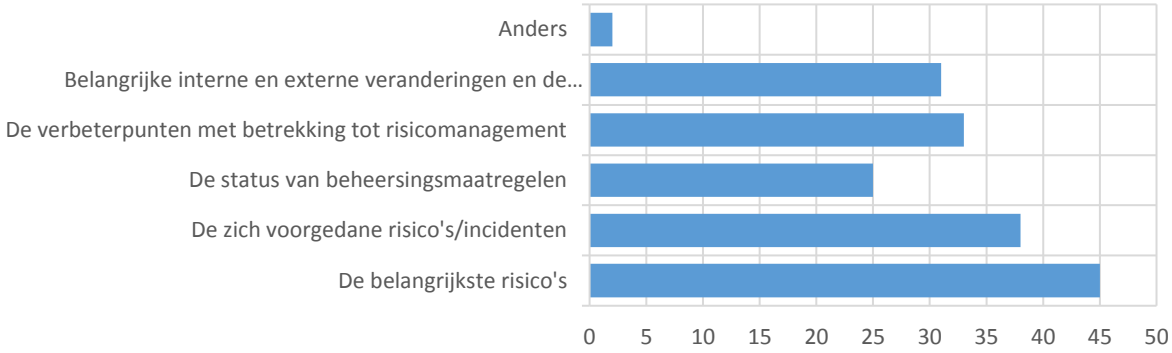
In totaal zijn er 59 antwoorden gegeven. 5 organisaties die bij het vorige antwoord 'Niet' hebben gegeven, hebben deze en de volgende vraag niet ingevuld. 1 organisatie die bij de vorige vraag 'Ad hoc/incidenteel' had ingevuld, heeft deze vraag en de volgende vraag niet beantwoord. Gemiddeld gezien voeren organisaties op (meer dan) 2 niveaus overleg.



Figuur 26 Niveaus van overleg over risicomanagement

Vraag 42. Waarover vindt overleg plaats?

Ook deze vraag is door 59 organisaties ingevuld. De focus van de organisatie ligt met name op de belangrijkste risico's en de zich voorgedane risico's en incidenten. Gemiddeld gezien overleggen organisaties over (bijna) 3 van de opties die hier beneden staan.



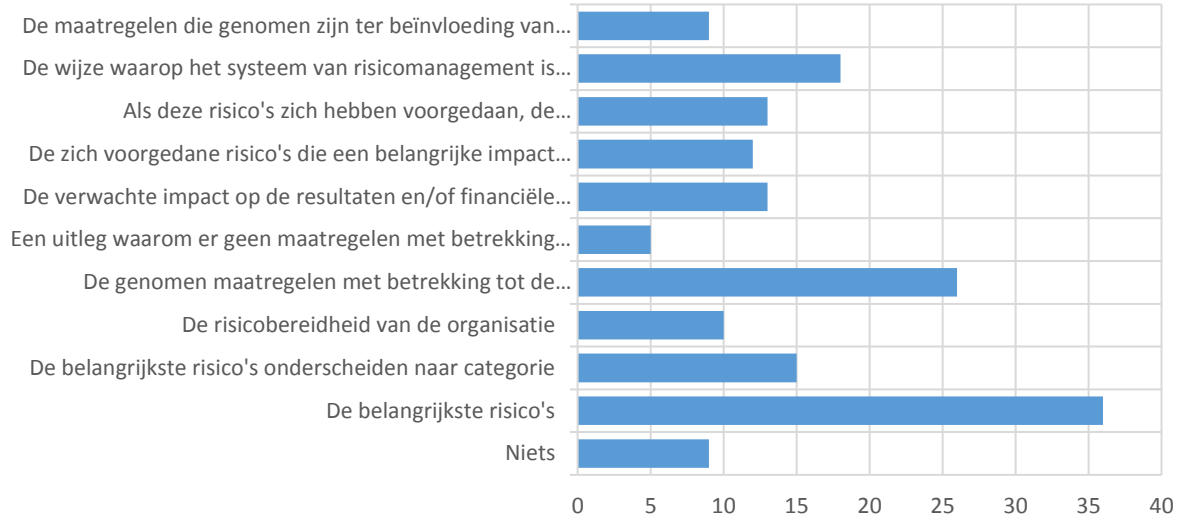
Figuur 27 Onderwerpen overleg over risicomanagement

Vraag 43. Is de organisatie op de hoogte van de aangepaste RJ 400 Jaarverslag en de gevolgen daarvan voor de verantwoording met betrekking tot risicomanagement?

Deze vraag markeert het einde van het onderdeel 'informatie en communicatie' en geeft het begin van het onderdeel 'verantwoording' aan. Er zijn in totaal 66 antwoorden gegeven, 37 (56,06%) hiervan zijn het antwoord 'ja' en 29 (43,94%) is 'nee'.

Vraag 44. Wat rapporteert de organisatie in haar jaarverslag over risico's?

Deze vraag is door 64 organisaties ingevuld. Bij deze vraag zijn er in totaal 11 opties. 8 opties zijn verplichte onderdelen volgens RJ 400, de 2 bovenste onderdelen zijn aanbevolen volgens RJ 400 en er is 1 optie voor het antwoord 'Niets'. De focus ligt met name op het vermelden van de belangrijkste risico's en de maatregelen die hiervoor genomen zijn. Het is opvallend dat optie 'De wijze waarop het risicomanagement is verankerd in de organisatie', die aanbevolen wordt door RJ 400, vaker wordt toegelicht dan een zestal verplichte opties. Gemiddeld gezien lichten organisaties maar (meer dan) 2 onderdelen toe.



Figuur 28 Verantwoorde elementen in het jaarverslag

Vraag 45. Welk cijfer geeft u het risicomanagementsysteem van de organisatie?

Deze vraag wordt uitgebreid behandeld in de analyse van de enquêteresultaten.

Vraag 46. Wat is de naam van de organisatie?

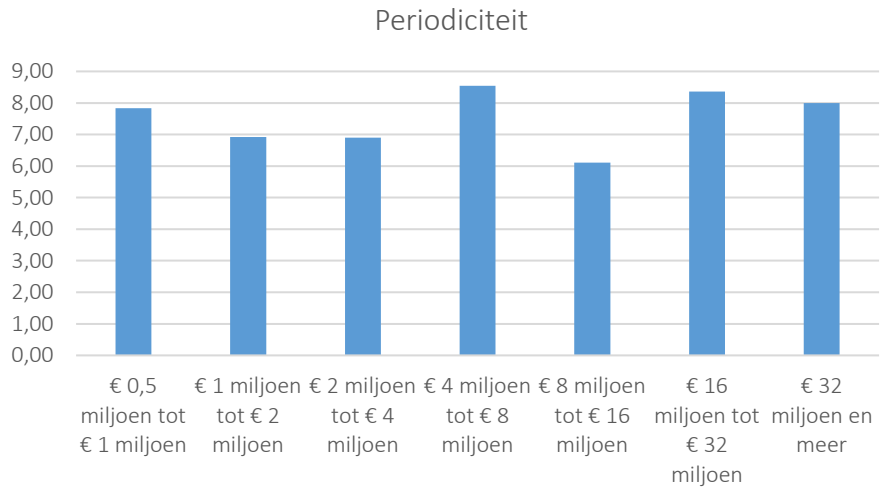
Deze vraag is niet verplicht en de organisaties die deze vraag hebben ingevuld, hebben toegestemd met de mogelijkheid dat hun naam genoemd wordt in dit rapport. In totaal zijn er 25 organisaties geweest die deze vraag hebben ingevuld: Artsen zonder Grenzen, Terre des Hommes, Stichting Woord en Daad, ICS, Jantje Beton, Stichting ZOA, Nederlandse Brandwonden Stichting, The Corts Foundations, Stichting Red een Kind, Stichting Ontmoeting, IZB, MissieNederland, Stichting VNB, ZZg, Missio, Dorcas, Stichting Kom over en Help, Mercy Ships Holland, De Hollandsche Molen, Stichting Defence for Children, stichting Kidsrights, Women on Wings, ECF, Trans World Radio en Stichting natuur- en milieufederatie Limburg.

5.2 Verbanden en relaties tussen vragen en antwoorden

Er zijn in totaal 8 antwoorden die gecorrigeerd zijn, 5 antwoorden daarvan zijn gecorrigeerd in de scores. 5 van de 8 antwoorden zijn ongeldig en 3 antwoorden zijn niet meegenomen in de scores omdat de desbetreffende antwoorden geen punten opleverden. Tevens is bij de hoogte van de baten door één organisatie een zodanig afwijkend antwoord gegeven, dat deze ook niet is meegenomen. De(ze) controle op interne validiteit is uitgevoerd in de vorige paragraaf, naast de resultaten per vraag.

5.2.1 Relatie tussen score en periodiciteit

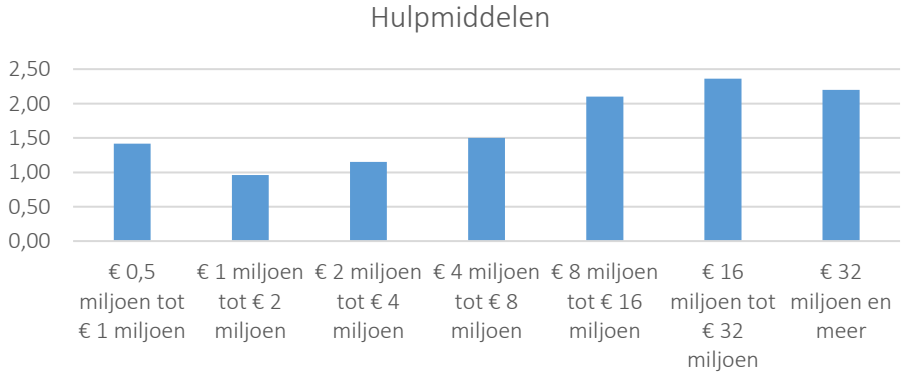
In de opzet is aangegeven dat er voor periodiciteit relatief minder punten wordt toegekend, om kleinere organisaties tegemoet te komen. Hiervoor wordt onderzocht of dit ook geldt voor de organisaties die de enquête hebben ingevuld. De vragen 10 (voorbereiding), 24 (risico-identificatie en –evaluatie), 31 (Evaluatie) en 40 (informatie en communicatie) aan over de periodiciteit van risicomanagement. Voor het inzichtelijk maken van de periodiciteit zijn 64 organisaties gebruikt die alle vier de vragen hebben ingevuld en de hoogte van de baten hebben ingevuld. Voor de verdeling van klassen naar grootte is dezelfde indeling gebruikt als bij de relatie tussen score en grootte (volgende paragraaf). In het hiernaast weergegeven figuur is het gemiddelde van het aantal punten met betrekking tot periodiciteit per klasse, onderscheiden naar grootte, met elkaar vergeleken.



Figuur 29 Behaalde punten voor periodiciteit per klasse naar grootte

5.2.2 Relatie tussen score en hulpmiddelen

In het berekenen van de scores is, in tegenstelling tot de periodiciteit, er aan hulpmiddelen geen afnemend belang toegekend. Het aantal te behalen punten is wel verlaagd en tevens is er een maximum gesteld.



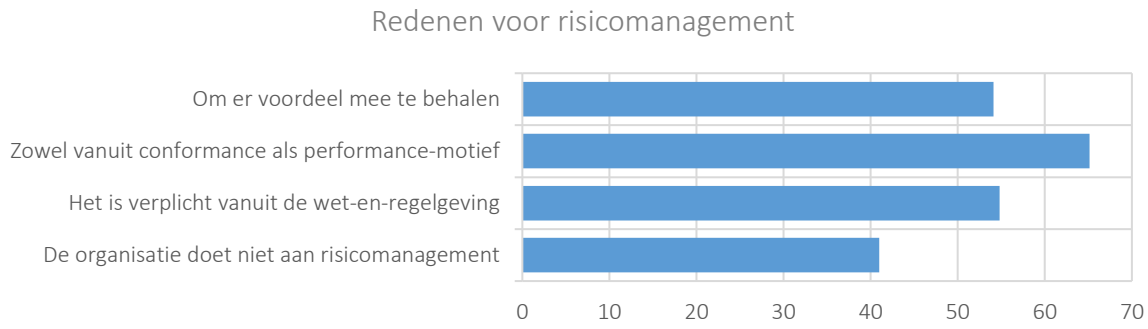
Figuur 30 Behaalde punten voor hulpmiddelen per klasse naar grootte

Voor het inzichtelijk maken van de relatie tussen de grootte van de baten en de hulpmiddelen is rekening gehouden met de antwoorden van de vragen 24 (risico-identificatie en –evaluatie) en 31 (evaluatie). Op basis van het aantal gegeven antwoorden bij vraag 24 en 31, ook het antwoord ‘Nooit’,

zijn de antwoorden van de vragen 26 (risico-identificatie en –evaluatie) en 32 (evaluatie) meegenomen. Op basis van deze selectie zijn 66 antwoorden gebruikt. De relatie wordt op dezelfde manier in kaart gebracht als bij de periodiciteit. Zowel bij deze als de vorige vraag dient wel rekening gehouden te worden met de mate van subjectiviteit van de indeling in klassen en de invloed hiervan op de verdeling van de scores.

5.2.3 Relatie tussen totale score en reden voor risicomanagement

Omdat hier in tegenstelling tot de vorige vragen, de relatie tussen de reden voor risicomanagement en de totale score wordt onderzocht, worden de antwoorden van de 64 organisaties gebruikt die de hele enquête hebben ingevuld en zichzelf ook een cijfer hebben gegeven.

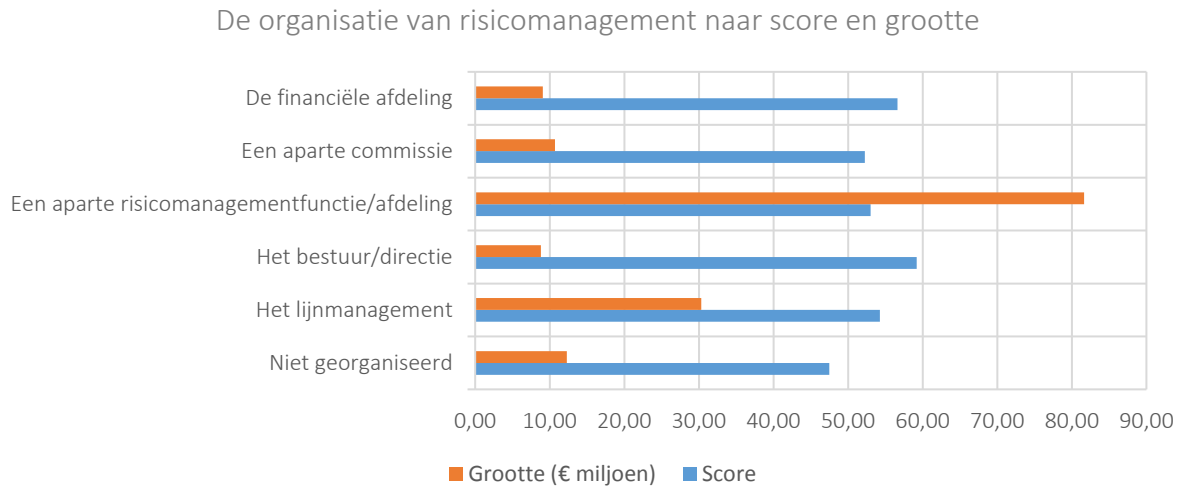


Figuur 31 De gemiddelde (totale) score per reden voor risicomanagement

Conform verwachting presteren organisaties die niet aan risicomanagement doen het minst. Het is opvallend dat de prestaties tussen de redenen 'om er voordeel mee te behalen' en 'Het is verplicht vanuit de wet- en regelgeving' niet van elkaar afwijken. Men zou verwachten dat organisaties die aan risicomanagement doen alleen vanwege om er voordeel mee te behalen, hoger scoren. Het beste scoren organisaties die zowel uit conformance-motief als performance-motief aan risicomanagement doen.

5.2.4 Relatie tussen organisatie risicomanagement, grootte en de totale score

Ook bij deze vraag worden de antwoorden van de 64 organisaties gebruikt, minus één organisatie die een afwijkend antwoord heeft gegeven bij de hoogte van de baten, dus in totaal 63 organisaties.
Bij deze resultaten is het goed te bedenken dat de opties 'Niet georganiseerd', 'Een aparte risicomanagementfunctie/afdeling' en 'Een aparte commissie' samen slechts 9 van de in totaal 63 gegeven antwoorden bedroegen. Bovendien zit er bij de optie 'Het lijnmanagement' een zeer grote organisatie bij, waardoor de gemiddelde grote van de organisaties bij de optie 'Het lijnmanagement'

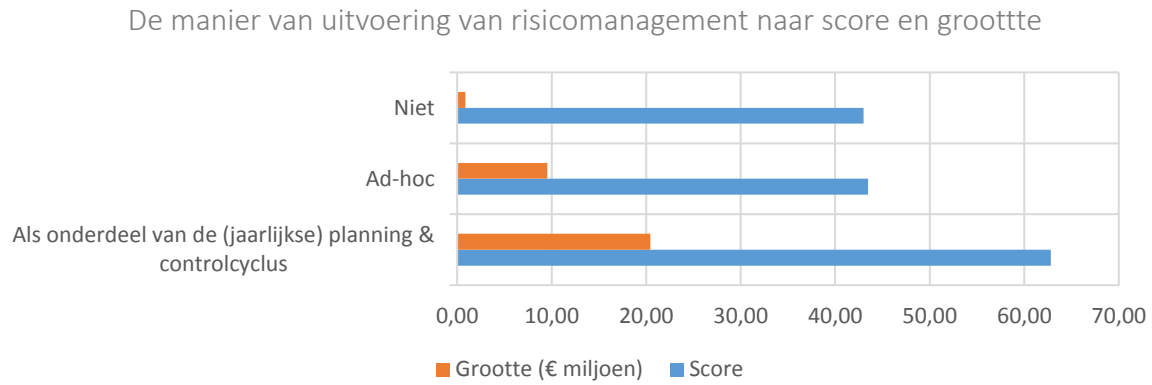


Figuur 32 De gemiddelde (totale) score bij de organisatie van risicomanagement in relatie met de grootte van de organisatie

enigszins een vertekend beeld geeft. Hetzelfde geldt voor de optie 'Niet georganiseerd', al geeft de gemiddelde grootte bij deze optie minder een vertekend beeld dan bij lijnmanagement. Bij de optie 'Een aparte commissie' is vrijwel niets zinnigs te zeggen over de gemiddelde grootte, omdat hier maar 2 antwoorden zijn gegeven.

5.2.5 Relatie tussen manier uitvoering risicomanagement, grootte en de totale score.

Bij deze vraag zijn de antwoorden gebruikt van dezelfde organisaties als bij de vorige vraag. In deze sub paragraaf wordt de relatie tussen de manier van uitvoering, de grootte van de organisatie en de score onderzocht. Bij het trekken van conclusies dient bedacht te worden dat bij de optie 'Niet' er maar 3 antwoorden zijn gegeven.



Figuur 33 De gemiddelde (totale) score bij de uitvoering van risicomanagement in relatie met de grootte van de organisatie

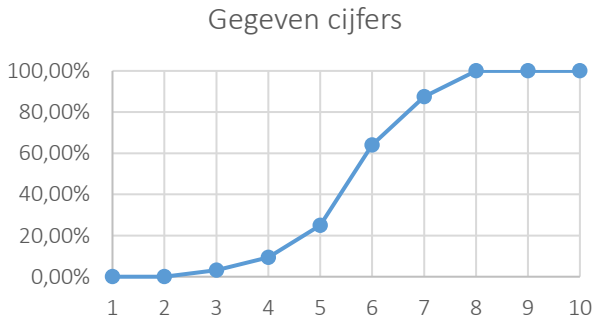
5.2.6 Relatie tussen verslaggevingsrisico en verantwoording

Allereerst wordt de relatie tussen vraag 43 en vraag 44 onderzocht, hierbij kan verwacht worden dat als men bij vraag 43 'ja' invult, men beter scoort bij vraag 44. Vraag 44 is namelijk gebaseerd op de vereisten volgens RJ 400 en als men niet op de hoogte is van RJ 400 is het moeilijker om te voldoen aan de vereisten volgens RJ 400. Voor het onderzoeken van de relatie zijn alle ingevulde antwoorden van vraag 43 gebruikt. In totaal hebben 66 organisaties gebruikt, aan de hand van deze organisaties is gekeken hoe organisaties scoorden bij vraag 44. De gemiddelde score van organisaties (37) die 'ja' hadden ingevuld, is 1,9. Het gemiddelde van organisaties (29) die 'nee' hadden ingevuld, is 1,33. Dit is significant (43%) lager.

Daarnaast wordt de relatie tussen het onderkennen van verslaggevingsrisico's en de verantwoording onderzocht, dus de relatie tussen vraag 25 (verslaggevingsrisico) en de totale score van verantwoording (vraag 43 en 44). De relatie is onderzocht aan de hand van 66 organisaties die vraag 24 ingevuld hebben. Er waren 20 organisaties die een verslaggevingsrisico onderkend hebben, de gemiddelde score op het onderdeel verantwoording van deze organisaties is 2,64. De 46 andere organisaties scoorden gemiddeld een 2,03.
Dit is 30% lager.

5.3 Scores

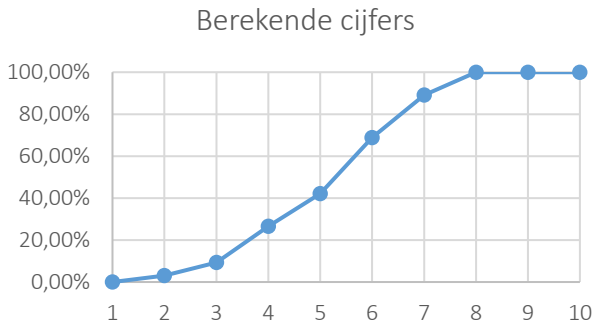
Voor het berekenen van de scores per organisatie zijn de 64 gegeven cijfers vergeleken met de 64 berekende cijfers. Het gemiddelde van de gegeven cijfers is 6,11 met een standaardafwijking van 1,19. Het aantal voldoendes ($\geq$ 6) bedraagt 75%.



Figuur 34 De verdeling van de gegeven cijfers

De berekende cijfers zijn afgerond op gehele cijfers om de vergelijkbaarheid met de gegeven cijfers te verhogen. Het gemiddelde van de berekende cijfers is 5,61 met een standaardafwijking van 1,55. De afgeronde voldoendes (≥ 6) besloegen samen 58%.

Als wordt gerekend met de niet afgeronde cijfers, bedraagt het gemiddelde van de berekende cijfers afgerond 5,60 met een standaarddeviatie van 1,52. Het aantal voldoendes (≥ 5,5) zou dan (55%) zijn.



Figuur 35 De verdeling van de berekende cijfers

Hierboven staan de verdelingen van de frequentie per cijfer van de gegeven en de berekende cijfers weergegeven. De linker as geeft het cumulatieve percentage aan, de onderste as het cijfer. Beide verdelingen zijn bij benadering normaal verdeeld. Dit is gecontroleerd aan de hand van normaal-papier.

De scores kunnen ook nader gespecificeerd worden, hierbij is de indeling zoals weergegeven in Figuur 44 en Figuur 40, aangehouden.

Als men naar onderstaande tabel kijkt is bij het aantal voldoendes gekeken naar het aantal organisaties die bij het desbetreffende onderdeel meer punten behaalden dan de helft van het maximaal aantal te behalen punten. Bij de kolom 'Gemiddelde' geeft het percentage aan wat het gemiddelde uitgedrukt ten opzichte van het maximaal aantal punten is. Bij de kolom 'Standaardafwijking' geeft het percentage de standaarduitdrukking ten opzichte van het gemiddelde weer.

Tabel 6 Aantal punten, gemiddelde, standaardafwijking en aantal voldoendes en onvoldoendes per hoofdonderdeel

Hoofdonderdeel	Max. aantal punten	Gemiddelde	Standaardafwijking	Aantal voldoende	Aantal onvoldoende
Voorbereiding	8	4,80 (60%)	2,33 (48%)	43 (67%)	21 (33%)
Risicobeleid	29	17,77 (61%)	4,71 (26%)	49 (77%)	15 (23%)
Risicoproces	43	20,55 (48%)	7,46 (36%)	29 (45%)	35 (55%)
Randvoorwaarden	20	12,86 (64%)	2,96 (23%)	51 (80%)	13 (20%)

Bij de voorbereiding hebben 8 organisaties precies 4 punten behaald, in de tabel zijn deze organisaties bij het aantal onvoldoendes opgeteld. Dit verklaart het hoge percentage onvoldoendes ten opzichte van het gemiddelde. De hoge standaardafwijking (voorbereiding) in relatie met het gemiddelde betekent er van het aantal onvoldoendes een relatief hoog percentage was dat buitengewoon laag scoorde.

De hoofdonderdelen risicobeleid, risicoproces en randvoorwaarden kunnen vervolgens ook weer verder uitgesplitst worden.

Tabel 7 Aantal punten, gemiddelde, standaardafwijking en aantal voldoendes en onvoldoendes bij het risicobeleid

Risicobeleid	Max. aantal punten	Gemiddelde	Standaardafwijking	Aantal voldoende	Aantal onvoldoende
Structuur	13	5,95 (46%)	2,25 (38%)	23 (36%)	41 (64%)
Cultuur	16	11,82 (74%)	3,17 (27%)	56 (88%)	8 (13%)

Tabel 8 Aantal punten, gemiddelde, standaardafwijking en aantal voldoendes en onvoldoendes bij het risicoproces

Risicoproces	Max. aantal punten	Gemiddelde	Standaardafwijking	Aantal voldoende	Aantal onvoldoende
Risico-identificatie en –beoordeling	14	6,02 (43%)	3,39 (56%)	27 (42%)	37 (58%)
Risicobeheersing	9	6,14 (68%)	2,36 (38%)	45 (70%)	19 (30%)
Evaluatie	8	3,59 (45%)	1,26 (35%)	18 (28%)	46 (72%)
Continu verbeteren	6	2,56 (43%)	1,51 (59%)	23 (36%)	41 (64%)
Verantwoording	6	2,25 (38%)	1,55 (69%)	18 (28%)	46 (72%)

Bij de evaluatie geeft het aantal voldoendes en onvoldoendes ten opzichte van het gemiddelde en de standaardafwijking enigszins een vertekend beeld. 8 organisaties zitten precies op de helft, die conform de richtlijn bij de onvoldoendes worden gerekend.

Tabel 9 Aantal punten, gemiddelde, standaardafwijking en aantal voldoendes en onvoldoendes bij de randvoorwaarden

Randvoorwaarden	Max. aantal punten	Gemiddelde	Standaardafwijking	Aantal voldoende	Aantal onvoldoende
Informatie en communicatie	12	5,55 (46%)	2,41 (44%)	28 (44%)	36 (56%)
Toezicht	8	7,31 (91%)	1,12 (15%)	63 (98%)	1 (2%)

Bij deze berekende cijfers zijn de scores niet afgerond, omdat per onderdeel door de organisatie geen cijfer is gegeven en derhalve er niets vergeleken kan en hoeft te worden.

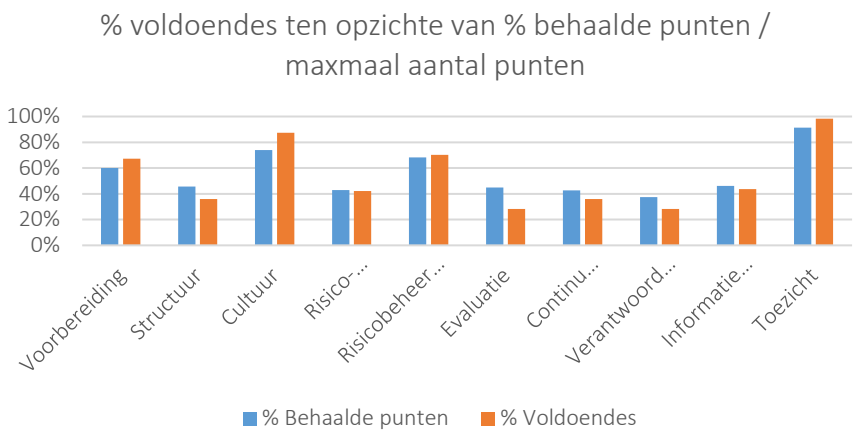
Per hoofdonderdeel is bekeken of er sprake was van een normale verdeling. Naar mate de frequentie toeneemt, wordt de frequentie steeds normaler verdeeld.[12] Aan de hand van normaal-papier en de vuistregels van de normale verdeling kan geconcludeerd worden dat op deze hoofdonderdelen de frequentie nog niet zo verdeeld is, dat er gesproken kan worden over een normale verdeling. Hiervoor zouden er meer organisaties de enquête in moeten vullen. Naast de frequentie speelt ook het aantal klassen een rol, hoe groter (nauwkeuriger) het aantal klassen, hoe 'normaler' de verdeling over het algemeen wordt. Het is echter te betwijfelen of een grotere steekproefpopulatie op sommige onderdelen de resultaten dusdanig zal beïnvloeden dat het een normale verdeling wordt. Zo zal bij de randvoorwaarden er altijd een minimum aantal punten behaald worden.

Als gekeken wordt naar organisaties die voor alle onderdelen een 'voldoende' hebben gescoord en waarbij de totale score meer dan 50 punten was, bedroeg dit aantal 4, met de stichting Woord en Daad die het beste scoorde met een totaal aantal van 83,75 punten. Andere organisaties die goed presteerden ($\geq$ 7) en de enquête niet anoniem hebben ingevuld, zijn de Nederlandse Brandwondenstichting, Women on Wings, Artsen zonder Grenzen en Stichting Red een Kind. Organisaties die minder presteerden ($\leq$ 4) en ook de enquête niet anoniem hebben ingevuld, zijn Stichting Natuur- en milieufederatie Limburg en Stichting ZOA.

Bij vraag 18 zijn twee antwoorden niet meegeteld in de scores, bij vraag 26 is er één antwoord niet meegenomen, hetzelfde geldt voor vraag 32. Bij vraag 33 zijn twee antwoorden niet meegenomen. Er zijn dus in totaal 5 antwoorden niet meegenomen. Van deze vijf antwoorden zijn er twee ongeldig en drie antwoorden waren geen antwoorden die een punt opleverden. Ten opzichte van het totaal aantal gegeven antwoorden is dit aantal verwaarloosbaar.

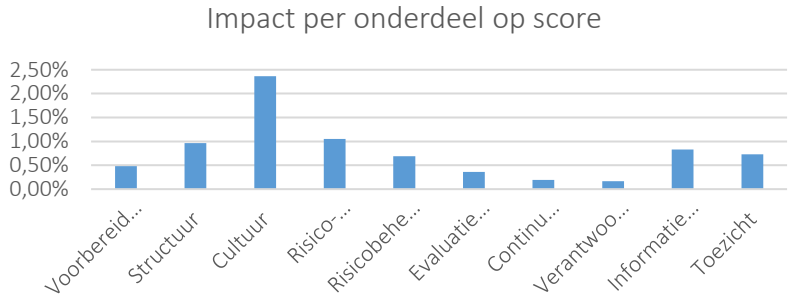
[12] (Open Universiteit, p. 2)

Hiernaast zijn de prestaties per onderdeel van de cyclus weergegeven door het aantal behaalde punten ten opzichte van het aantal maximaal te behalen punten te vergelijken met het percentage voldoendes.



Figuur 37 Percentage voldoendes t.o.v. percentage behaalde punten gedeeld door het maximaal aantal punten

De prestaties per onderdeel zijn ook nog anders uit te drukken. Per onderdeel kan ook gekeken naar de impact van het desbetreffende onderdeel op de score. Het aantal behaalde punten per onderdeel gedeeld door het totaal aantal behaalde punten, vermenigvuldigd met de weging van het desbetreffende onderdeel.

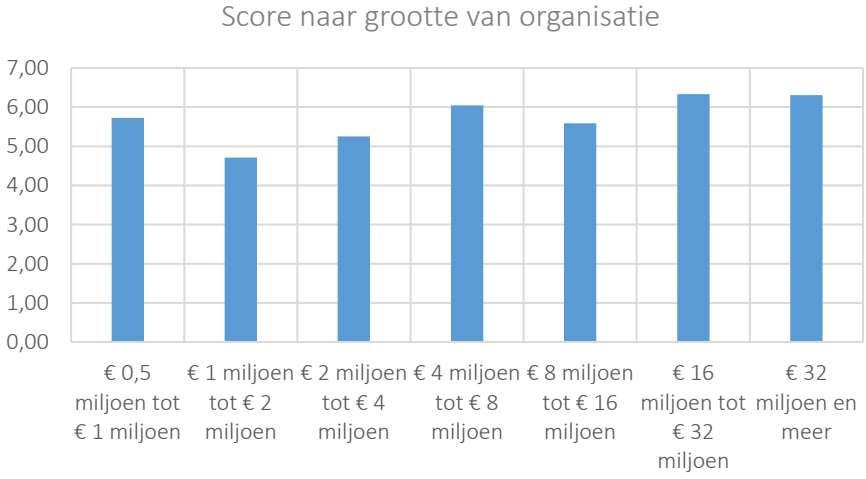


Figuur 36 De impact per onderdeel op de totale score

5.4 Relatie tussen de grootte van de organisatie en de score

De hypothese voor wat betreft de relatie tussen de grootte van de organisatie en de behaalde score is, dat minder grote organisaties minder hoog scoren dan grotere organisaties. In de scores is hiermee enigszins rekening gehouden door bij periodiciteit en hulpmiddelen relatief minder punten toe te kennen, naar mate de periodiciteit en hulpmiddelen vaker en meer werd. Voor de grootte van de organisatie wordt de hoogte van de baten als richtlijn gebruikt. Wat betreft het aantal organisaties, er wordt hetzelfde aantal organisaties aangehouden als bij de scoreberekening minus 1, deze organisatie had een zodanig afwijkend antwoord ingevuld bij de baten, dat deze niet is meegenomen. Dit zijn dus in totaal 63 organisaties.

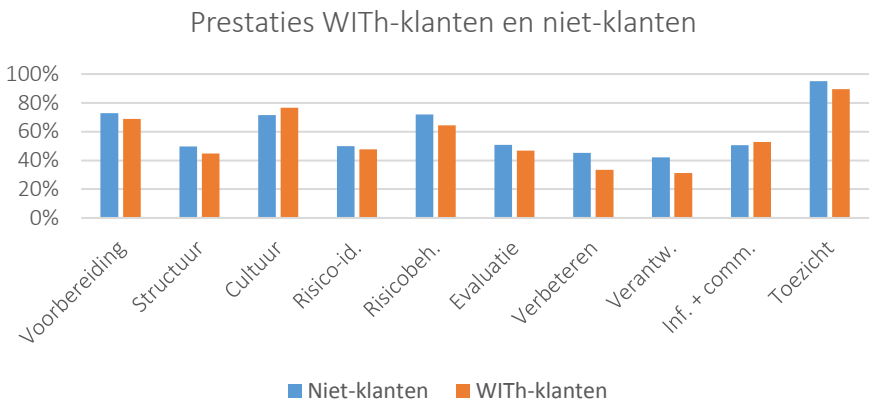
Het aantal klassen is 7 (63 / 9) waarbij een oplopend verschil per klasse is aangehouden van 2 keer het vorige verschil, verder zijn de niet-afgeronde cijfers gebruikt.



Figuur 38 De score naar grootte van de organisatie

5.5 Vergelijking WITh-klanten en niet-klanten

Als de prestaties van klanten van WITh Accountants worden vergeleken met niet-klanten moet er rekening gehouden worden met het aantal wel en niet-klanten van WITh Accountants. Er zijn in totaal 6 klanten van WITh Accountants die bij deze vergelijking meegenomen worden en 18 niet-klanten. Klanten van WITh geven zich gemiddeld een 6,33. Niet-klanten geven zich een 6,22. Op basis van de berekende cijfers is het gemiddelde cijfer voor WITh-klanten een 5,72 en voor niet-klanten een 6,01. Echter gezien het geringe aantal organisaties waarmee hier gerekend is, kan er geen conclusie worden getrokken voor gehele populatie WITh klanten en niet-klanten.



6. Conclusie

In dit onderzoek is gezocht naar de antwoorden op de vragen: ‘Hoe kan het risicomanagement bij een fondsenwervende instelling ingericht worden?’ en ‘Wat is het niveau van risicomanagement bij fondsenwervende instellingen?’ Hiervoor is zowel kwalitatief als kwantitatief onderzoek uitgevoerd. Bij het kwalitatief onderzoek is een theoretisch model ontwikkeld voor de inrichting van risicomanagement, bij het kwantitatief onderzoek is een enquête uitgevoerd om het (huidige) niveau van risicomanagement bij fondsenwervende instellingen te onderzoeken.

Globaal kan de inrichting van risicomanagement in vier onderdelen worden onderscheiden:

1. Voorbereiding;
2. Ontwikkeling risicobeleid;
3. Uitvoeren risicoproces; en
4. De randvoorwaarden.

De eerste drie onderdelen kunnen als stappen worden gezien en de randvoorwaarden zijn de benodigdheden voor de uitvoering van risicomanagement. Deze vier onderdelen bestaan zelf ook weer uit een aantal onderdelen. Zo bestaat de voorbereiding uit het inzicht verkrijgen in de interne en externe omgeving, het ontwikkelen van een risicovisie, het formuleren van risicomanagementdoelstellingen en het ontwikkelen van een risicostrategie.

Het ontwikkelen van het risicobeleid bestaat uit vijf stappen, het formuleren van voorwaarden voor (effectief) risicomanagement, het organiseren van risicomanagement binnen de organisatie, het bepalen van het terrein van risicomanagement, het bepalen van de uitgangspunten/principes van risicomanagement en het benoemen van de elementen van risicomanagement. Het ontwikkelen van een risicocultuur en de organisatie van risicomanagement zijn belangrijke aspecten voor een succesvol risicomanagement.

Het risicoproces vormt de kern van de vier onderdelen en kan beschouwd worden als een cyclus, eerst worden risico’s geïnventariseerd en daarna beoordeeld. Aan de hand van deze beoordeling worden beheersingsmaatregelen ontworpen en toegepast. Nadat deze beheersingsmaatregelen operationeel zijn, kan de werking ervan geëvalueerd worden. De laatste twee stappen zijn niet per definitie gekoppeld aan de rest van de stappen, het gaat hierbij om continu verbeteren en de verantwoording.

Het laatste onderdeel van risicomanagement zijn de randvoorwaarden, deze zijn benodigd om risicomanagement goed uit te kunnen voeren. De meest relevante randvoorwaarden met betrekking tot risicomanagement zijn informatie, communicatie en toezicht.

Uit de enquête is gebleken dat fondsenwervende instellingen het risicomanagement niet zo (gestructureerd) hebben ingericht. Door een focus op de risicobeheersing zijn verschillende onderdelen onderbelicht. De fondsenwervende instelling scoort gemiddeld een magere voldoende, organisaties die laag scoren, schatten zich te hoog in en organisaties die hoog scoren, schatten zich daarentegen iets te laag in. Wel scoort de fondsenwervende instelling goed op cultuur en toezicht.

Verder is gebleken dat er geen (significante) relatie is tussen de grootte van de organisatie en de behaalde score en dat de verschillen tussen organisaties groot zijn (hoge standaardafwijking).

Afrondend kan gezegd worden dat er nog veel slagen gemaakt kunnen worden en dat het niveau van risicomanagement deels afhankelijk is van de aandacht die er aan besteed wordt.

7. Aanbevelingen

Het advies in voornamelijk gericht op onderdelen en zaken die verbeterd kunnen worden, er wordt vrijwel niet of helemaal niet ingegaan op zaken die al 'goed' verlopen. Aan de hand van de enquête worden er eerst adviezen gegeven. Als laatste wordt het ontwikkelde model als oplossing voor het probleem behandeld.

Reden voor risicomanagement

Uit de enquête blijkt dat organisaties die zowel vanuit conformance-motief als performance-motief het beste scoren. Organisaties die ook een 'moet-karakter' ervaren van risicomanagement presteren dus beter. Vanuit diverse wet- en regelgeving wordt bijvoorbeeld verantwoording over risico's al vereist (RJ 400). Organisaties dienen zich te realiseren dat risicomanagement niet alleen (meer) een vrijwillig karakter heeft, maar dat het ook indirect verplicht is geworden.

Aandacht voor risicomanagement

Dit hangt ook samen met de aandacht die besteed wordt aan risicomanagement. Uit de enquête blijkt dat 14 van de 70 (20%) organisaties nooit een (bedrijfsbrede) risico-inventarisatie en risico-evaluatie uitvoeren, 7 van de 67 (10%) evalueren nooit de genomen beheersingsmaatregelen en 5 van de 65 organisaties (8%) hebben nooit overleg over risico's en risicomanagement. Door meer aandacht te besteden aan risicomanagement zal risicomanagement gestalte krijgen bij organisaties die nog vrijwel niet doen aan risicomanagement, de prestaties zullen hierdoor ook verbeteren.

Integratie risicomanagement

Ontwikkel een risicovisie (gebaseerd op de missie en visie) en formuleer risicodoelstellingen en leg hiermee een link met de organisatiedoelstellingen. Het risicobeleid en de –strategie kan dan bepaald worden in lijn met de strategie van de organisatie. Integreer risicomanagement in de organisatie door dit op te nemen in processen of in de planning & controlcyclus. Uit de enquête is namelijk gebleken dat integratie van risicomanagement in de planning & controlcyclus positieve invloed heeft op risicomanagement.

Risicocultuur en -bewustzijn

Blijf aandacht besteden aan de cultuur binnen de organisatie, uit de enquête is namelijk gebleken dat cultuur de grootste impact heeft gehad op de score. Zorg ervoor dat het risicobewustzijn en de –cultuur een belangrijke rol heeft binnen de organisatie. Streef naar risk readiness, wees voorbereid op onverwachte situaties en creëer veerkracht om (onverwachte en) ernstige gebeurtenissen op te vangen.

Structuur en organisatie van risicomanagement

Stel iemand of een onderdeel binnen de organisatie verantwoordelijk voor risicomanagement en zorg ervoor dat de verantwoordelijkheden, taken en bevoegdheden voor iedereen binnen de organisatie bekend zijn. Uit literatuuronderzoek is namelijk gebleken dat naast cultuuraspecten, structuuraspecten belangrijk zijn bij de uitvoering van risicomanagement.

Integratie risicomanagement en prestatiemanagement

Integreer risicomanagement en prestatiemanagement, laat de prestaties op het gebied van risicomanagement en –beheersing onderdeel zijn van beloning en/of waardering. Het zou bijvoorbeeld onderdeel kunnen uitmaken van functioneringsgesprekken. Let er wel op dat het te ver doorvoeren van risicomanagement en prestatiemanagement de cultuur binnen een organisatie weer negatief kan beïnvloeden.

De onderdelen van het risicoproces

Focus bij het risicoproces niet alleen op risicobeheersing; het proces bestaat uit meerdere onderdelen. Door het focussen op risicobeheersing, worden andere onderdelen onderbelicht, die vrijwel even belangrijk zijn. Uit de enquête is bijvoorbeeld gebleken dat op de onderdelen evaluatie, continu verbeteren en verantwoording minder wordt gescoord dan op de risico-inventarisatie en –evaluatie en de beheersing. In dit rapport is een model ontwikkeld voor risicomanagement. Dit kan een hulpmiddel zijn om meer aandacht te besteden aan andere onderdelen.

Risicobereidheid

Bepaal de risicobereidheid van de organisatie, enerzijds is het verplicht vanuit RJ 400 om dit toe te lichten in de risicoparagraaf, anderzijds is het nuttig omdat maatregelen gerelateerd kunnen worden aan de risicobereidheid. Afhankelijk van de risicobereidheid en de weging van de risico's moet bepaald worden voor welke risico's welke maatregelen genomen moeten worden.

Risico-identificatie en -beoordeling

Voer periodiek een (bedrijfsbrede) risico-inventarisatie en risico-evaluatie uit. De periodiciteit is afhankelijk van de grootte van de organisatie en de snelheid van veranderingen, zowel intern als extern. Breng bij de risico-inventarisatie zo veel mogelijk (soorten) risico's in kaart en ga bij complexere risico's dieper op de risico's zelf in. Benoem bij elk risico de oorzaak, degene voor wie het risico geldt en eventueel welke maatregelen er al genomen zijn.

Voer de risicobeoordeling gescheiden uit van de risico-inventarisatie en voer de risicobeoordeling uit na de risico-inventarisatie, dit voorkomt dat er zaken over hoofd worden gezien en dat de beoordeling up-to-date blijft. Houdt ook rekening met de relatie met de doelstellingen, risico's die de realisatie van doelstellingen bedreigen, moeten een zwaardere weging krijgen.

Laat de risico-inventarisatie en –beoordeling door meerdere mensen uitvoeren, zorg ervoor dat hierbij ook pessimisten zitten. Uit literatuuronderzoek is namelijk gebleken dat mensen risico's over het algemeen te licht inschatten. Zorg er ook voor dat deze mensen deskundig en ervaren zijn, dit verhoogt de kwaliteit van de inventarisatie en beoordeling. Laat het gebruik van hulpmiddelen, de aanpak en het doel op elkaar aansluiten. Zo kunnen bepaalde hulpmiddelen beter aansluiten op de kwalitatieve methode en andere op de kwantitatieve methode.

Strategie en risicobeheersing

Bepaal de risicoreactie aan de hand van het soort risico. Probeer risico's met een hoge kans en hoge impact te vermijden. Bij risico's met hoge kans en lage impact kan de kans op het risico verminderd worden, het risico overgedragen wordt of geaccepteerd worden door het mee te nemen in de bedrijfsvoering. Risico's met lage kans en hoge impact kunnen overgedragen (verzekerd) worden en de impact kan beperkt worden. Risico's met lage impact en lage kans kunnen geaccepteerd worden.

Houd bij het nemen van een maatregel rekening met de effectiviteit en de efficiëntie van de maatregelen; wordt hiermee het doel bereikt en wegen de kosten op tegen de opbrengsten. Zorg er voor dat er een juiste verhouding bestaat tussen hard en soft controls. Houd ook rekening met de capaciteit om risico's te kunnen dragen.

Evaluatie en bijsturing

Voordat er evaluatie kan plaatsvinden, moet worden vastgesteld dat de maatregelen operationeel zijn en naar behoren functioneren.

Stel voor de evaluatie een norm of een referentiepunt op, de doelstellingen als norm of referentiepunt verdient hierbij aanbeveling. Maak deze norm of referentiepunt vervolgens concreet door er (kritische) prestatie-indicatoren aan te koppelen. De werking van de maatregel kan dan

vergeleken worden met de norm. Aan de hand van deze vergelijking moet bepaald worden of er bijgestuurd moet worden.

Gebruik bij de evaluatie meer hulpmiddelen dan er alleen over praten, er is dan immers geen nader onderzoek geweest naar de werking van de maatregelen.

Continu verbeteren

Formuleer allereerst ambities en breng het huidige niveau van risicomanagement in kaart. Aan de hand van vergelijking tussen het huidige niveau en de ambitie kan bepaald worden waar er verbeteringen/acties genomen moeten worden.

Deel opgedane kennis en 'best practices' binnen een organisatie door (bijvoorbeeld werkgroepen op te richten die) regelmatig met elkaar overleggen en biedt als organisatie trainingen, cursussen en workshops aan om zo de kennis en het risicobewustzijn van personeelsleden te vergroten. Ook kan er tussen organisaties overleg plaatsvinden en kunnen risicomanagementsystemen van organisaties binnen dezelfde keten/sector vergeleken worden.

Verantwoording

Om de verantwoording te verbeteren is het sterk aan te bevelen dat organisaties RJ 400 doornemen. Verder dienen relevante zaken voor de verantwoording in eerdere stadia van het risicomanagement(proces) vastgelegd te worden, zodat men niet bij het opmaken van het jaarverslag voor het eerst gaat nadenken over de onderdelen die (verplicht) opgenomen moeten worden in de risicoparagraaf.

Informatie en communicatie

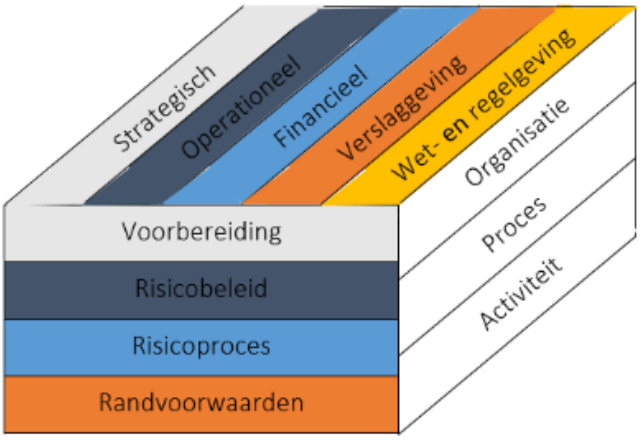
Voer in relatie met de integratie van risicomanagement in de planning & controlcyclus regelmatig overleg over risico's en risicomanagement. Beperk dit overleg niet alleen over de belangrijkste risico's en risico's die zich voorgedaan hebben, maar breid het uit tot andere onderdelen van het risicoproces, zoals evaluatie, verbetering en verantwoording.

Toezicht

Uit de enquête is gebleken dat het toezicht bij fondsenwervende instellingen op orde is. Vrijwel elke stichting heeft een toezichthoudend orgaan, wordt gecontroleerd door een onafhankelijke accountant en is aangesloten bij een brancheorganisatie. Voor organisaties die dit nog niet hebben, verdient het de aanbeveling om deze basis ook toe te gaan passen.

Model

Een groot gedeelte van deze adviezen kunnen worden ondervangen door alle stappen van het hiernaast weergegeven model toe te passen. Dit model kan namelijk structuur aan de invulling van risicomanagement geven. Het is een model dat ontwikkeld is op basis van uitgebreid literatuuronderzoek. Hierdoor is de volledigheid van het model gewaarborgd. Tevens is het bij dit model mogelijk om risicomanagement op verschillende niveaus toe te passen en om risicomanagement te integreren in de organisatie.



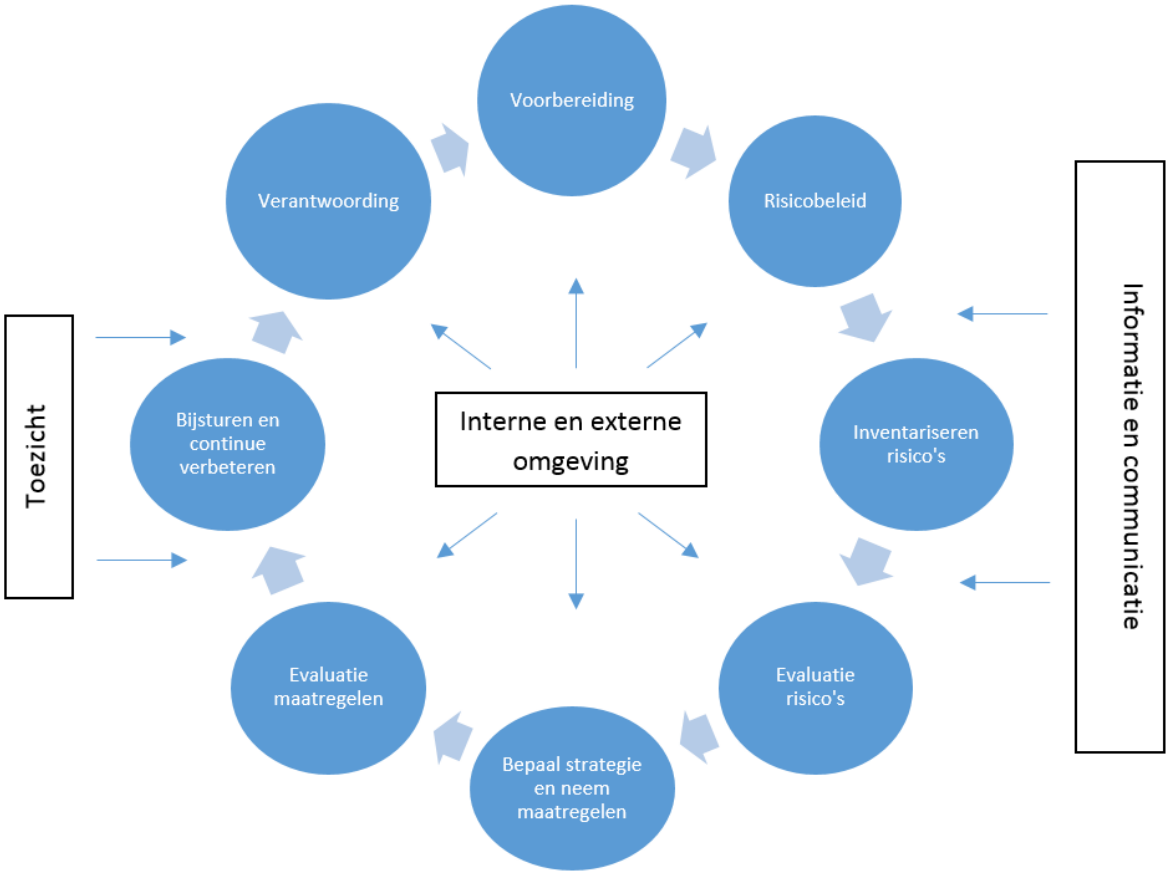
Figuur 39 Framework risicomanagementmodel

Het model bestaat uit drie dimensies:

1. De onderdelen van risicomanagement (voorkant);
2. De soorten doelstellingen (bovenkant);
3. Niveaus van risicomanagement (zijkant).

De eerste dimensie

De eerste drie onderdelen zijn stappen in het risicomanagementproces en het vierde onderdeel zijn de randvoorwaarden die benodigd zijn voor de uitvoering van (succesvol) risicomanagement. Deze voorkant worden samengevat door het onderstaande figuur.



Figuur 40 Cyclus risicomanagement

Het risicoproces en de randvoorwaarden zijn in dit figuur nader uitgewerkt. De voorbereiding en de stap 'risicobeleid' zijn niet verder uitgewerkt, omdat deze stappen niet de kern vormen van risicomanagement.

Bij de voorbereiding moet(en) er:

- Inzicht verkregen worden in de interne en externe omgeving;
- Een risicovisie ontwikkeld worden;
- Risicomanagementdoelstellingen geformuleerd worden; en
- Een risicostrategie ontwikkeld worden.

Bij het ontwikkelen van het risicobeleid moeten de volgende onderdelen aan de orde komen:

- Het formuleren van voorwaarden voor (effectief) risicomanagement;
- Het organiseren van risicomanagement binnen de organisatie;
- Het terrein van risicomanagement;
- De uitgangspunten/principes van risicomanagement; en
- De elementen van risicomanagement.

Deze cyclus is niet star van aard, risicomanagement is een dynamisch proces. Tussen elke stap dient terugkoppeling plaats te vinden. Deze cyclus dient geïntegreerd te worden in de organisatie en zo veel mogelijk aan te sluiten bij de organisatie.

Aan de zijkanten van de cyclus staan de (meest relevante) randvoorwaarden weergegeven. Om de cyclus te doorlopen is informatie nodig die door middel van communicatie worden doorgegeven. Informatie en communicatie zorgt ervoor dat de cyclus van risicomanagement doorlopen kan worden. Op elke stap afzonderlijk en op het risicomanagement als geheel moet toezicht worden gehouden, dit kan zowel intern (bestuur/RvC/RvT) als extern (accountants/externe toezichthouder).

De tweede dimensie
Op de bovenkant van het model staan de vijf soorten doelstellingen weergegeven. Door doelstellingen in te delen wordt het mogelijk om op bepaalde onderdelen van risicomanagement te concentreren. Deze doelstellingen geven aan wat de behoeften van de organisatie zijn en wat er verwacht kan worden van deze doelstellingen. Risicomanagement kan dan redelijke zekerheid verschaffen bij het bereiken van deze doelstellingen, dit is echter ook afhankelijk of de doelstellingen binnen de macht van de organisatie ligt. Zo hebben strategische doelstellingen vaak een extern karakter.

Tevens kunnen de vijf soorten doelstelling gekoppeld worden aan de indeling van risico, wat vervolgens structuur kan geven bij de inventarisatie van risico's.

De derde dimensie
Vervolgens kan dit worden toegepast op drie niveaus:

1. Organisatie;
2. Proces; en
3. Activiteit.

Door niveaus te onderscheiden is het mogelijk risicomanagement te concentreren op een bepaald niveau. Ook kunnen er risico's per niveau worden onderscheiden. De relatie tussen risico en een niveau is tevens een indicatie voor de zwaarte van het risico. Een risico op een laag niveau zal de realisatie van de/een doelstelling(en) minder bedreigen dan een risico op een hoger niveau. Door niveaus te onderscheiden kan structuur worden aangebracht in risicomanagement.

8. Implementatie

Naast dat er een model voor risicomanagement is ontwikkeld, moet het model nog wel kunnen worden geïmplementeerd in een organisatie. Hiervoor wordt allereerst een stappenplan beschreven, met daarin wie, wat en wanneer. Daarna zullen er een aantal middelen worden bespreken waarmee de implementatie ondersteund kan worden. Verder zal ingegaan worden op de verandering die de implementatie van risicomanagement teweegbrengt en waarmee rekening moet worden gehouden. Als laatste worden de randvoorwaarden voor de implementatie van risicomanagement benoemd.

Stappenplan

Drs. Urjan Claassen RA RE CIA (2009) onderscheidt een stappenplan met de volgende onderdelen:

- Een gemeenschappelijke taal;
- Het definiëren van een scope, het formuleren van een projectstructuur en het creëren van draagvlak binnen de organisatie;
- Het beoordelen van risico's en risicostrategieën;
- Inventariseren, ontwerpen en implementeren van de interne beheersing;
- Monitoring en continu verbetering.[13]

Op basis van het ontwikkelde model kunnen hier nog een aantal stappen aan toegevoegd worden, zoals de voorbereiding, de ontwikkeling van het risicobeleid, de inventarisatie van risico's en verantwoording.

Het stappenplan kan vanuit een aantal niveaus van de organisatie worden geïmplementeerd. Dit is het operationele, het tactische en het strategische niveau. Bij de implementatie van risicomanagement vanuit het operationele niveau, zal de implementatie vooral een bottom-up karakter hebben, terwijl het karakter bij de implementatie vanuit strategisch niveau, top-down zal zijn.

De keuze voor een niveau kan afhangen van het draagvlak op het desbetreffende niveau, maar ook van de aanleiding waarom een organisatie aan risicomanagement wil doen.[14]

Tabel 10 Implementatieplan

Stap	Wat	Wie	Wanneer
1.	Een gemeenschappelijke taal	Directie/bestuur	Week 1
2.	Het definiëren van een scope, het formuleren van een projectstructuur en het creëren van draagvlak	Directie/bestuur	Week 2 – week 12
3.	De randvoorwaarden van risicomanagement	Directie/bestuur en lijnmanagement	Week 4 – week 12
4.	De voorbereiding van risicomanagement	Lijnmanagement	Week 5
5.	Het ontwikkelen van risicobeleid	Lijnmanagement	Week 6
6.	Inventarisatie van risico's	Lijnmanagement	Week 7
7.	Beoordeling van risico's	Lijnmanagement	Week 7
8.	Risicobeheersing	Lijnmanagement	Week 8 – week 12
9.	Evaluatie van maatregelen	Lijnmanagement	Week 12
10.	Continu verbeteren	Lijnmanagement	Week 12
11.	Verantwoording	Directie/bestuur	Bij het opmaken van het bestuursverslag
12.	Evaluatie invoering risicomanagement	Lijnmanagement en directie/bestuur	Wanneer alle stappen tot en met 11 zijn doorlopen

Allereerst moet er een gemeenschappelijke taal ontwikkeld worden. Wat wordt er bedoeld met risico en risicomanagement en wat houden de ermee samenhangende begrippen in. Daarna wordt bepaald

[13] (Drs. Urjan Claassen RA RE CIA, 2009, p. 251 t/m 267)
[14] (Drs. U.P.W.L.M. Claassen RA RE CIA, 2013, pp. 24, 25)

waarop risicomanagement zich gaat focussen. Verder moet om risicomanagement te integreren een aantal personen worden aangewezen die verantwoordelijk zijn voor het opzetten van risicomanagement, hiervoor is draagvlak een vereiste. Het creëren van draagvlak is niet van de ene op de andere dag gebeurd, dit zal tijd kosten. Deze twee stappen worden door de directie/bestuur uitgevoerd. De eerste actie voor het opzetten van risicomanagement moet vanuit het bestuur/directie komen. Dit betekent niet dat de impuls/vraag voor risicomanagement niet bij het lijnmanagement vandaan kan komen. Het bestuur/directie moet echter wel de eerste stap zetten.
Voordat de stappen van het model worden gevolgd, is het verstandig om eerst te kijken naar de randvoorwaarden van risicomanagement. Dit zijn benodigdheden om risicomanagement goed uit te kunnen voeren. Deze randvoorwaarden (informatie, communicatie en toezicht) zullen al wel aanwezig zijn binnen een organisatie. Het is echter van belang om bij deze randvoorwaarden rekening te houden met risicomanagement. Aangezien deze randvoorwaarden zich in de gehele organisatie bevinden, moet deze stap zowel door de directie/bestuur als het lijnmanagement worden uitgevoerd.

Vervolgens kunnen de stappen van het model door het lijnmanagement worden opgezet. Belangrijk hierbij is te bedenken dat de evaluatie van maatregelen niet gelijk kan plaatsvinden. De maatregelen moeten eerst geïmplementeerd worden, voordat ze geëvalueerd worden. Ook de verantwoording hangt niet direct samen (qua opvolging) met de andere stappen. Bij het maken van het bestuursverslag moet immers het beleid met betrekking tot risico's 'pas' verantwoord te worden. Het bestuursverslag wordt geschreven door het bestuur/directie.

Als de stappen 1 tot en met 11 zijn doorlopen kan de implementatie van risicomanagement geëvalueerd worden door het lijnmanagement en de directie/bestuur. Welke stappen zijn goed doorlopen en afgehandeld en aan welke stappen moet nog extra aandacht besteed worden. Deze stap is anders dan stap 10 en 11. Bij stap 10 en 11 wordt gekeken naar de stappen van risicomanagement, bij stap 12 wordt de implementatie geëvalueerd. Qua karakter is dit eenmalig en uitgebreider dan de stappen 10 en 11.

Interventies

Om de implementatie te ondersteunen kunnen er verschillende interventies worden gebruikt. Bij de stappen waar de directie/bestuur bij is betrokken, kan gebruikt gemaakt worden van de managementinstructie. Voor het creëren van draagvlak kan met name door de directie campagne gevoerd worden, de voorgenomen verandering moet bekend gemaakt worden. Ook heeft de directie een voorbeeldfunctie wanneer het gaat om de implementatie van risicomanagement. Een laatste hulpmiddel kan zijn om externe autoriteiten in te schakelen om de noodzaak van verandering nog een uit te leggen en te onderstrepen.

Zowel het bestuur/directie als het lijnmanagement kunnen trainingen en cursussen volgen met betrekking tot risicomanagement en als dat niet helpt, kan er overlegd worden met andere soortgelijke organisaties over problemen waar men tegenaan loopt.

Verandermanagement

Bij het reorganiseren en het veranderen van een organisatie is het verstandig om rekening te houden met de volgende principes:

- Houd rekening met de omstandigheden;
- Wees geduldig;
- Speel in op de sterke kanten van de organisatie; en
- Bepaal welke (andere) systemen moeten veranderen.[15]

Andere maatregelen om de verandering bestuurbaar te krijgen en te houden zijn:

[15] (Stéphane J.G. Giro en Samina Karim, 2017, p. 130 t/m 132)

- Het meetbaar maken van de impact van de veranderingen;
- Veranderen met kleine stappen die snel worden uitgevoerd;
- Iedereen die een rol speelt bij de implementatie van risicomanagement betrekken bij de verandering;
- Motiveer mensen om risicomanagement succesvol te implementeren door motivatie belangrijker te maken dan interne regels (tijdens implementatie);
- Mensen moeten fouten bespreekpaar durven maken door er bij anderen op te wijzen en bij zichzelf aan te geven;
- Het belang van de organisatie moet voorop staan.[16]

Randvoorwaarden

Voordat risicomanagement succesvol geïmplementeerd kan worden is er meer nodig dan alleen een implementatieplan, wat kwalitatief in orde moet zijn, er zullen diverse randvoorwaarden aanwezig moeten zijn; er dient draagvlak te worden gecreëerd en er dient op een adequate manier omgegaan te worden met weerstand. Drs. Urjan Claassen RA RE CIA (2009) onderscheidt de volgende kritieke succesfactoren:

- Leiderschap:
    - Betrokkenheid topmanagement;
    - Rechtvaardiging van het project middels een heldere business case;
    - Gemeenschappelijke visie rondom het gewenste eindresultaat;
    - Realistische doelstellingen;
    - Ontwikkel een duidelijk actieplan.
- Rekenschap en betrokkenheid;
    - Betrekken belanghebbende sleutelfunctionarissen;
    - Beleggen van verantwoordelijkheid;
    - Aandacht voor mensen en soft controls;
    - Voldoende ondersteuning en projectmanagement.[17]

Het is dus belangrijk om draagvlak te creëren en adequaat om te gaan met weerstand, dit kan gebeuren door het risicobewustzijn binnen de organisatie te verhogen door medewerkers de noodzaak van risicomanagement in te laten zien. Dit kan bijvoorbeeld door het communiceren over risico's en haar gevolgen.

Uiteindelijk moet iedereen binnen de organisatie betrokken worden bij de uitvoering van risicomanagement. De directie/bestuur dient hierbij het goede voorbeeld te geven. Het doel is om te komen tot succesvol risicomanagement waarmee voldaan wordt aan wet- en regelgeving en waarmee voordeel behaald wordt.

Om risicomanagement te integreren in de organisatie moet er het een en ander veranderen. Zo moet er een risicocultuur groeien en iedereen binnen de organisatie krijgt er een taak bij; ze moeten zich bezighouden met risico's en de beheersing daarvan. Verantwoordelijkheden, taken en bevoegdheden zullen duidelijk belegd moeten worden.

Om risicomanagement in te voeren is tijd en geld nodig, de directie/bestuur moet bereid zijn om te investeren in risicomanagement.

[16] (Piet Kempen & Jimme Keizer, 2016, p. 186)
[17] (Drs. U.P.W.L.M. Claassen RA RE CIA, 2013, p. 32 t/m 34)

Nawoord

Het schrijven van dit rapport heb ik als zeer leerzaam ervaren. Risicomanagement is voor mij een vrij nieuw onderwerp, zeker omdat het een andere invalshoek betrof. In eerste instantie bekeek ik risico's en risicomanagement namelijk vanuit de hoek van de accountant. Na uitgebreid onderzoek ben ik tevreden met het resultaat en blij om deze periode af te kunnen sluiten.

Sinds de keuze voor dit onderwerp is het een en ander wel gewijzigd, zo is op basis van het vooronderzoek het probleem verschoven van de risicoparagraaf naar risicomanagement. Het was lastig om de juiste aanpak en methode te kiezen en te verantwoorden, in mijn hoofd had ik de richting wel zitten, maar de nadere uitwerking van deze richting bleek zo nu en dan lastig.

Ik denk dat ik veel geleerd heb door het uitvoeren van het onderzoek, zowel bij het kwalitatieve (literatuuronderzoek) als het kwantitatieve gedeelte (enquête). Dit waren voor mij relatief nieuwe werkterreinen, met name het verwerken van de enquêteresultaten. Ook hier liep ik tegen een aantal zaken aan, zoals de betrouwbaarheid van de enquête en de geldigheid/bruikbaarheid van de antwoorden. Net als de aanpak en de gehanteerde methode zou ik dit de volgende keer anders aanpakken.

Jaco de Vos

Hardinxveld-Giessendam, 8 juni 2017

Literatuurlijst

Annfinance. (2011, augustus 25). *Soft controls; een hype of iets om rekening mee te houden*. Opgehaald van www.wetenschap.infonu.nl: http://wetenschap.infonu.nl/economie/81078-soft-controls-een-hype-of-iets-om-rekening-mee-te-houden.html

B.J. Reijntjes. (2007, augustus 21). *Enterprise Risk Management.* Opgehaald van www.dare.uva.nl: http://dare.uva.nl/cgi/arno/show.cgi?fid=93500

Bart Sterenborg. (2003). *Fondsenwervende instellingen.* Opgehaald van www.cbf.nl: https://www.cbf.nl/Uploaded_files/Zelf/Sterenborg,%20B%20(2004)%20-%20Fondsenwervende%20Instellingen.pdf

Bosman, D. R. (2009, december 9). *www.docplayer.nl.* Opgehaald van Raamwerk of kooi? Geschiktheid van ISO als instrument voor risicomanagement bij de Provinciale overheid: http://docplayer.nl/1021428-Raamwerk-of-kooi-geschiktheid-van-iso-31000-als-instrument-voor-risicomanagement-bij-de-provinciale-overheid.html

Capital Counsel. (2015, november). *Good Governance - Een onderzoek naar Governance & risicomanagement in de goede doelensector.* Opgehaald van www.dubois.nl: http://www.dubois.nl/wp-content/uploads/2014/10/Onderzoeksrapport-Governance-goede-doelen.pdf

Case-study onderzoek. (2015, juli 12). Opgehaald van www.managementplatform.nl: http://managementplatform.nl/case-study-onderzoek/12/07/2015

CBF. (2017). *Verdeling per sector*. Opgehaald van www.cbf.nl: https://www.cbf.nl/sectorbrede-informatie/verdeling-sector/

Centraal Bureau Fondsenwerving. (2012, januari). *Doel en Taken - Centraal Bureau Fondsenwerving.* Opgehaald van www.cbf.nl: http://www.cbf.nl/Uploaded_files/Zelf/DOELENTAKENversiejanuari2012.pdf

Chris Chapman en Stephen Ward. (2003). *Project Risk Management - Process, Techniques and Insights.* The Atrium, Southern Gate, Chichester, West Sussex: John Wiley & Sons Ltd.

Commissie Goed Bestuur voor Goede Doelen. (2005, juni). *Advies van de commissie code goed bestuur voor goede doelen.* Opgehaald van www.kennisbankfilantropie.nl: http://www.kennisbankfilantropie.nl/docs/handig-voor-stichtingen/code-wijffels-goed-bestuur.pdf?sfvrsn=2

Committee of Sponsoring Organisations of the Treadway Commission. (2004, september). *Enterprise Risk Management - Integrated Framework (Executive Summary).* Opgehaald van www.coso.org: http://www.coso.org/documents/coso_erm_executivesummary.pdf

Committee of Sponsoring Organizations of the Treadway Commision. (2012, januari). *www.coso.org.* Opgehaald van Enterprise Risk Management - Understanding and Communicating Risk Appetite: http://www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (2009, januari). *Guidance on Monitoring Internal Control Systems.* Opgehaald van www.coso.org: http://www.coso.org/documents/COSO_Guidance_On_Monitoring_Intro_online1_002.pdf

Dick Hortensius en Ed Mallens. (2010). *ISO 31000: nieuw referentiekader voor risicomanagement.* Opgehaald van www.docplayer.nl: http://docplayer.nl/17834771-Iso-31000-nieuw-referentiekader-voor-risicomanagement.html

Drs. U.P.W.L.M. Claassen RA RE CIA. (2013, april). *Enterprise Risk Management Plus - Een praktische toepassing van COSO ERM.* Opgehaald van www.managementexecutive.nl: www.managementexecutive.nl/downloaden/13515/Enterprise-Risk-Management-Plus

Drs. Urjan Claassen RA RE CIA. (2009). *Handboek Risicomanagement.* Deventer: Kluwer.

Encyclo. (sd). *Definities opzoeken*. Opgehaald van www.encyclo.nl: http://www.encyclo.nl/

Eppink, Dr. D. en Keuning, Dr. D.J. (2012). *Management & Organisatie.* Groningen / Houten: Noordhoff Uitgevers.

Erik van de Crommenacker, Peter Dona, Siebrand van der Ploeg. (2015). *Verzekeren kan altijd nog - Risicomanagement en bedrijfscontinuïteitsmanagement.* Delft: Nederlands Normalisatie-Instituur.

Etienne C. Wenger en William M. Snyder. (2002). *Harvard Business Review over lerende organisaties.* Zaltbommel: Thema uitgeverij Schouten & Nelissen.

Focus op verbeteren. (2015). *Risicomanagement: een pragmatische benadering in negen stappen.* Opgehaald van www.focusopverbeteren.nl: http://www.focusopverbeteren.nl/wp-content/uploads/pdf/Risicomanagement.pdf

Foeke van der Zee. (2016). *Casestudie, casestudy of gevalsstudie*. Opgehaald van www.hulpbijonderzoek.nl: http://hulpbijonderzoek.nl/online-woordenboek/casestudie/

Fred van Hessen. (2009, december). *Het Mede Financierings Stelsel (MFS-II) in het kort.* Opgehaald van www.partin.nl: http://www.partin.nl/fileadmin/user_upload/kennis-platform/091207MedeFinancieringsStelsel.pdf

Gert Jan Schop. (2017). *INK-model*. Opgehaald van www.managementmodellensite.nl: https://managementmodellensite.nl/ink-model/#.WShaTBs5WUk

Goede Doelen Nederland en IF. (2015, december 11). *Inrichting Validatiestelsel - Normen Erkenningsregeling.* Opgehaald van www.erkenningsregeling.files.wordpress.com: https://erkenningsregeling.files.wordpress.com/2015/10/normen-erkenningsregeling-11-december-2015.pdf

Hans Doorewaard. (sd). *Typen project: praktijkgericht*. Opgehaald van www.hetontwerpenvaneenonderzoek.nl: https://www.hetontwerpenvaneenonderzoek.nl/presentaties/3/player.html

Hans van der Westen en Nienke Teunissen. (2009). *Grote-giftenwerving in 60 minuten voor non-profit bestuurders en directies.* Zutphen: Wallburgpers.

Instituut Nederlandse Kwaliteit (INK). (sd). *Fundamentele kenmerken.* Opgehaald van www.ink.nl: http://www.ink.nl/model/fundamentele-kenmerken

Intervivos B.V. (sd). *Publicatieverplichting*. Opgehaald van www.anbi.nl: https://anbi.nl/publicatieverplichting/

ISO. (2009). *ISO/Guide 73:2009(en).* Opgehaald van www.iso.org: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

Jaap Zijlstra & Lizanne Vroom. (2014). *Ik durf het risico wel aan! - Een integrale en praktisch kijk op risicomanagement.* Deventer: Vakmedianet.

Jeroen de Kort. (2014, maart). *Corporate Governance - De verhouding tussen 'hard- en soft controls' in de Nederlandse bestuurskamer.* Opgehaald van www.arno.uvt.nl: http://arno.uvt.nl/show.cgi?fid=133727

Karl E. Weick, Kathleen M. Sutcliffe. (2011). *Management van het onverwachte - wat je kunt leren van high reliability organizations.* Rotterdam: BBNC uitgeers.

Koninklijke Nederlandse Beroepsorganisatie van Accountants. (2014, oktober 29). *Tweede Nationaal Onderzoek Risicomanagement in Nederland 2014*. Opgehaald van www.nba.nl: https://www.nba.nl/Actueel/Nieuws/Nieuwsarchief/Tweede-Nationaal-Onderzoek-Risicomanagement-in-Nederland-2014/

KPMG. (2013). *COSO Internal Control - Integrated Framework (2013).* Opgehaald van www.home.kpmg.com: https://home.kpmg.com/content/dam/kpmg/pdf/2016/05/2750-New-COSO-2013-Framework-WHITEPAPER-V4.pdf

Lizanne Vroom. (2014). *Risicomanagement - vanut het Dynamisch Business Model®.* Hilversum: Educatieve Uitgeverij Nederland.

M. Paur, A. v. (2014). *De kern van de administratieve organisatie.* Groningen/Houten: Noordhoff Uitgevers.

Manon C.P. Ruijters. (2011, maart 21). *In bloei trekken... - Leren ontwikkelen van mens en organisatie.* Opgehaald van www.twynstraguddekennisbank.nl: https://www.twynstraguddekennisbank.nl/sites/default/files/pictures/2148_boekje_inauguratie_MRU_v4_lr%20(1).pdf

Mw. mr. A.M.M.M. van Zeijl, Mr. J. Keizer, Mr. J.M.K. Burger e.a. (2016). *Wetteksten Hoger Onderwijs - 2016/2017.* Groningen/Houten: Noordhoff Uitgevers.

Nassim Nicholas Taleb. (2013). *Antifragiel - Dingen die baat hebben bij wanorde.* Amsterdam: Nieuwezijds.

Nederlandse Beroepsorganisatie van Accountants (NBA), Nyenrode Business Universiteit, Rijksuniversiteit Groningen, PwC. (2014, oktober). *Hoeveel zijn we opgeschoten na de crisis? Tweede Nationaal Onderzoek Risicomanagement in Nederland 2014.* Opgehaald van www.executiveeducation.nl: http://www.executiveeducation.nl/fileadmin/user_upload/Documenten/PDF/NBA_NYENRODE_Rapport_Risicomanagement__Okt14__DEF.compressed.pdf

Nederlandse Beroepsorganisatie van Accountants. (2013, november). *Risico's managen is mensenwerk - Risicomanagement en -verslaggeving bij grote ondernemingen.* Opgehaald van www.nba.nl: https://www.nba.nl/Documents/Publicaties-downloads/ManagementLetters/pml-risicomanagement-271113.pdf

Niccolò Machiavelli. (sd). *Live by quotes*. Opgehaald van www.livebyquotes.com: https://livebyquotes.com/2014/all-courses-of-action-are-risky-so-prudence-is-not-in-avoiding-danger-but-calculating-risk-and-acting-decisively-make-mistakes-of-ambition-and-not-mistakes-of-sloth-develop-the-strength-to-d/

Nyenrode Business Universiteit. (2016). *Essayprijs 2016 - Essays naar aanleiding van de masterscriptie accountancy 2015-2016.* Opgehaald van www.nyenrode.nl: http://www.nyenrode.nl/library/Documents/essaybundel-accountancy-2016.pdf

Open Universiteit. (sd). *Populatieverdeling, verdeling van steekproefscores, en steekproevenverdeling.* Opgehaald van www.oupsy.nl: http://oupsy.nl/files/populatieverdeling,%20verdeling%20van%20steekproefscores,%20en%20steekproevenverdeling.pdf

Overheid.nl. (sd). *Publicatieplicht stichtingen*. Opgehaald van www.internetconsultatie.nl: https://www.internetconsultatie.nl/publicatieplicht_stichtingen

Payton, R. L. (1988). *www.paytonpapers.org.* Opgehaald van Philanthropy: Voluntary Action for the Public Good: http://134.68.190.22/output/pdf/book.pdf

Phil McNaull and Lorraine Loy. (2008, december). *Risk Management Policy .* Opgehaald van www1.hw.ac.uk: http://www1.hw.ac.uk/insurance/risk-management-policy.pdf

Piet Kempen & Jimme Keizer. (2016). *Competent afstuderen en stagelopen.* Groningen/Houten: Noordhoff Uitgevers.

Piet Verschuren en Hans Doorewaard. (2015, 2015). *Het ontwerpen van een onderzoek.* Amsterdam: Boom Lemma uitgevers. Opgehaald van Het ontwerpen van een onderzoek: https://www.boomhogeronderwijs.nl/documenten/9789462365070_inkijkexemplaar.pdf

Prof. dr. E.H.J. Vaassen RA, Dr. L.H.H. Bollen, Prof. dr. R.H.H. Meuwissen RA, Dr. M.P.M. Vluggen, Prof. dr. F.G.H. Hartman RC. (2012). *Basisboek Informatie & Control.* Groningen / Houten: Noordhoff.

Prof. dr. J.G. Bethlehem. (sd). *www.survey-onderzoek.nl*. Opgehaald van Voor en nadelen van online-onderzoek: http://www.survey-onderzoek.nl/online.html

Prof. dr. Kees Cools RA. (2006). *Controle is goed, vertrouwen is beter.* Assen: Van Gorcum.

Prof. dr. Lucas Meijs. (2014). *Filantropie in Nederland.* Den Haag: Stichting Maatschappij en Onderneming.

Prof. Dr. R.H.F.P. Bekkers. (2013, april 25). *www.cbf.nl.* Opgehaald van De maatschappelijke betekenis van filantropie: http://www.cbf.nl/Uploaded_files/Zelf/BekkersRDemaatschappelijkebetekenisvanfilantropieOratie25april2013.pdf

Prof. dr. René Bekkers, prof. dr. Theo Schuyt en drs. Barbara Gouwenberg. (2015, maart 31). *Geven in Nederland 2015 - Giften, Nalatenschappen, Sponsoring en Vrijwilligerswerk.* Opgehaald van www.goededoelennederland.nl: https://goededoelennederland.nl/system/files/public/Onderzoek/2015%20GIN%20samenvatting.pdf

Raad voor de Jaarverslaggeving. (2014, maart 26). *RJ-Uiting 2014-3: 'ontwerp-Richtlijn 400 Jaarverslag'.* Opgehaald van www.rjnet.nl: http://www.rjnet.nl/Documents/Uitingen%202014/RJ-Uiting%202014-3%20ontwerp-Richtlijn%20400%20Jaarverslag.pdf

Raad voor de Jaarverslaggeving. (2014, oktober 13). *RJ-Uiting 2014-7: 'ontwerp-Richtlijn 630 Commerciële stichtingen en verenigingen'.* Opgehaald van www.rjnet.nl: http://www.rjnet.nl/Documents/Uitingen%202014/RJ-Uiting%202014-7%20voor%20publicatie.pdf

Raad voor de Jaarverslaggeving. (2016). *RJ-Uiting 2016-13: 'Richtlijn 650 Fondsenwervende organisaties'.* Opgehaald van www.rjnet.nl: http://www.rjnet.nl/Global/RJ-Uiting%202016-13%20%27Richtlijn%20650%20fondsenwervende%20organisaties%27.pdf

Raad voor de Jaaverslaggeving. (2013). *Richtlijnen voor de jaarverslaggeving - voor grote en middelgrote rechtspersonen.* Deventer: Kluwer.

Ricardo Cronie. (2007, februari). *Onderzoeksmethoden - Handleiding voor studenten van de minor Regie stedelijke vernieuwing (RSV).* Opgehaald van https://communicatiekc.com/ontwerpen-van-onderzoek-volgens-verschuren-doorewaard/

Rich Milo, John G. Giakouminakis, Traci Mizoguchi, Jimmy Yu. (2013). *COSO 2013 Framework on Internal control.* Opgehaald van www.chapters.theiia.org: https://chapters.theiia.org/Orange%20County/IIA%20OC%20Presentation%20Downloads/COSO%20Placemat_Deloitte.pdf

Rob Uiterlinden RC. (2009). *'In Control', theorie en praktijk.* 's-Hertogenbosch: Tutein Nolthenius.

Roel Grit, M. G. (2009). *Zo maak je een risicoanalyse.* Groningen/Houten: Noordhoff Uitgevers.

SBF - Samenwerkende brancheorganisaties filantropie. (2015, juli 15). *SBF-code Goed Bestuur.* Opgehaald van www.goededoelennederland.nl: https://goededoelennederland.nl/system/files/public/Sector/150715%20SBF%20Code%20Goed%20Bestuur.pdf

Sonja Janicijevic, Paul Claes, Rob Lengkeek. (2016). *Risicomanagement.* Groningen/Houten: Noordhoff Uitgevers.

Steekproefcalculator. (2013). Opgehaald van www.steekproefcalculator.com: http://www.steekproefcalculator.com/steekproefcalculator.htm

Stéphane J.G. Giro en Samina Karim. (2017). *Harvard Business Review*, 130 t/m 132.

The association of Insurance and Risk Managers (airmic), The Public Risk Management Association (alarm), The institute of Risk Management (irm). (2009). *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 3100.* Opgehaald van www.theirm.org: https://www.theirm.org/media/886062/ISO3100_doc.pdf

The UWE Bristol Fund. (sd). *Risk Policy and Risk Management Procedures.* Bristol: UWE Bristol - University of the West of England.

Thinka Bor-Reijinga en Gert van der Kolk. (2014). *Alert op risico - Naar risk readiness in mensen en organisaties.* Deventer: Vakmedianet.

Thomas Hürlimann. (2011). *Risk management in a time of global uncertainty.* Opgehaald van www.hbr.org: https://hbr.org/resources/pdfs/tools/17036_HBR_Zurich_Report_final_Dec2011.pdf

Tilburg University. (2017). *Betrouwbaarheid en validiteit*. Opgehaald van www.tilburguniversity.edu: https://www.tilburguniversity.edu/nl/studenten/studie/colleges/spsshelpdesk/edesk/betrouwb.htm

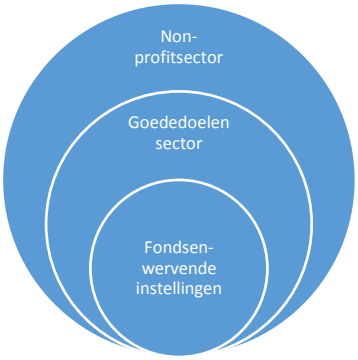
VUmc - Vrije Universiteit medisch centrum. (2004, december). *Het INK-managementmodel toegelicht.* Opgehaald van www.vumc.nl: https://www.vumc.nl/afdelingen-themas/32498/48566/INK

Bijlage 1 Literatuuronderzoek

Bijlage 1.1 Definiëring en ontwikkeling van de fondsenwervende instelling
In navolging van het onderzoeksontwerp (Figuur 1) worden de belangrijkste begrippen gedefinieerd en uitgelegd. Allereerst wordt de fondsenwervende instelling in een breder kader bekeken: de non-profitsector en de daarvan onderdeel zijnde goededoelensector. In de tweede paragraaf wordt een definitie gegeven van de fondsenwervende instelling. In de daaropvolgende paragraaf worden de ontwikkelingen en verwachtingen besproken met betrekking tot de goededoelensector. Als laatste zal er een samenvatting worden gegeven.

Bijlage 1.1.1 Afbakening van de goededoelensector

In de volksmond wordt onder de non-profitsector en de goededoelensector vaak hetzelfde verstaan. Er is echter wel onderscheid, zo behoren ziekenhuizen en onderwijsinstellingen wel tot de non-profitsector, maar niet tot de goededoelensector. De goededoelensector is echter wel weer onderdeel van de non-profitsector. Het onderscheid tussen de goededoelensector en de non-profitsector is mede gebaseerd op de verschillen in wet-en-regelgeving. Zo is 'RJ 655 Zorginstellingen' bedoeld voor ziekenhuizen en 'RJ 660 Onderwijsinstellingen' voor scholen. Binnen de goededoelensector worden 'RJ 650 Fondsenwervende instellingen', 'RJ 640 Organisaties-zonder-winststreven', 'RJk C2 Kleine fondsenwervende instellingen' en 'RJk C1 Kleine organisaties zonder winststreven' toegepast.



Figuur 41 Afbakening goededoelensector

Naast verschillen in wet-en-regelgeving kenmerkt deze sector zich doordat organisaties in deze sector een beroep (onder andere) doen op donaties en donateurs die vrijwillig een donatie geven (in tijd of geld), zonder dat er sprake is van een (evenredige) tegenprestatie.[18] Dit wordt ook wel filantropie genoemd. Payton (1988) definieert filantropie als volgt: "Voluntary action for the public good"[19]. Deze activiteiten hoeven niet in lijn te zijn met de mening van de meerderheid of die van de overheid, het karakter is dus wezenlijk anders dan dat van subsidie.[20] Schuyt (2001) sluit zich bij deze definitie aan, hij definieert filantropie als: "vrijwillige private bijdragen (in de vorm van geld, goederen en tijd) aan publieke doelen met de intentie primair het algemeen belang te bevorderen"[21].

Andere, niet unieke, kenmerken van organisaties binnen de sector zijn:
- De rechtsvorm betreft een vereniging of een stichting, kort gezegd betekent dit dat er geen winst verdeeld mag worden (art. 2:26 lid 3 en art. 2:285 lid 3 BW);[22]
- De doelstellingen hebben betrekking op gezondheid, internationale hulp, natuur en milieu en welzijn, welke weer nader onderverdeeld kunnen worden in subdoelstellingen;[23]
- Ze beschikken vaak over een ANBI-status, waardoor giften aftrekbaar zijn bij de belasting;
- In vergelijking met winstgerichte organisaties zijn ze beperkt in omvang, zo gaven 516 fondsenwervende instellingen in 2013 'maar' € 3,1 miljard uit;[24]
- Ze zijn veelal vrijgesteld van omzet- en vennootschapsbelasting.

[18] (Nyenrode Business Universiteit, 2016, p. 59)
[19] (Payton, 1988, p. 175)
[20] (Prof. dr. Lucas Meijs, 2014, p. 13)
[21] (Prof. Dr. R.H.F.P. Bekkers, 2013, p. 6)
[22] (Mw. mr. A.M.M.M. van Zeijl, Mr. J. Keizer, Mr. J.M.K. Burger e.a., 2016, pp. 384, 467)
[23] (CBF, 2017)
[24] (Prof. dr. René Bekkers, prof. dr. Theo Schuyt en drs. Barbara Gouwenberg, 2015, p. 12)

Bijlage 1.1.2 Definitie van een fondsenwervende instelling

Het CBF definieert een fondsenwervende instelling als: "een naar Nederlands recht opgerichte stichting of vereniging met volledige rechtsbevoegdheid die voor realisering van charitatieve, culturele, wetenschappelijke of andere het algemeen nut beogende doelstellingen door middel van fondsenwerving een beroep doet op de publieke offervaardigheid".[25] De oude Richtlijn 650 Fondsenwervende instellingen gaat net als het CBF uit van het beroep doen op de publieke offervaardigheid. Richtlijn 650 (2013) geeft namelijk de volgende definitie:

> *Een particuliere organisatie die qua doelstelling niet op winst is gericht en voor het realiseren van zijn doelstelling een beroep doet op de publieke offervaardigheid. De bijeengebrachte gelden en/of goederen zijn vrijwillig afgestaan, vormen geen evenredige tegenprestatie voor geleverde goederen of diensten en er kunnen geen recht voor zorg of hulp aan worden ontleend.*[26]

Het is vreemd dat de huidige richtlijn 650 spreekt over "publieke offervaardigheid", terwijl uit dezelfde richtlijn blijkt dat baten niet alleen door "publieke offervaardigheid" worden verkregen, maar ook door subsidies van overheden en ontvangsten van bedrijven. De definitie, gegeven door Richtlijn 650, lijkt daardoor niet volledig. Deze definitie is echter in de nieuwe RJ 650 aangepast waardoor deze beter bij de inhoud van de richtlijn past. De nieuwe RJ 650 (2016) definieert de fondsenwervende organisatie als:

> *Een particuliere organisatie met een maatschappelijke doelstelling die niet op winst is gericht en voor het realiseren van haar doelstelling baten verwerft uit publieke offervaardigheid en daarnaast uit andere bronnen van herkomst zoals overheidssubsidies, loterijen en baten als tegenprestatie voor de levering van producten en/of diensten.*[27]

In de nieuwe richtlijn is ook de titel veranderd, men heeft 'instelling' veranderd door 'organisatie'. Deze nieuwe richtlijn, wordt samen met de erkenningsregeling behandeld in de volgende paragraaf.[28]

Bijlage 1.1.3 Ontwikkelingen in en van de goededoelensector

Tegenwoordig is filantropie vrijwel dagelijks in het nieuws, zij het positief dan wel negatief. Dit geeft aan dat de maatschappelijke betekenis van filantropie groot is en ook toeneemt, zeker nu de overheid zich meer en meer terugtrekt. Zo heeft de overheid het medefinancieringsstelsel niet verlengd, dit stelsel was bedoeld om maatschappelijke organisaties te subsidiëren die dezelfde doelen nastreefden als de overheid.[29] Toch is de overheid nog steeds de grootste gever en zal dit ook blijven.[30] Organisaties moeten op zoek naar andere vormen van financiering en komen hierbij, onder andere, bij de maatschappij uit.

De toename van de maatschappelijke betekenis van filantropie wordt dan ook teruggezien in het bedrag dat de maatschappij doneert. Zo werd er in 1995 € 2,23 miljard gegeven, in 2013 is dit opgelopen tot € 4,36 miljard (informatie over nalatenschappen en bijdragen van vermogensfondsen is onvolledig); een stijging van 91%, het aantal giften uitgedrukt in het bbp is echter wel stabiel gebleven.[31] De groei van het aantal giften stijgt dus mee met het welvaartsniveau in Nederland.

[25] (Centraal Bureau Fondsenwerving, 2012, p. 4)
[26] (Raad voor de Jaaverslaggeving, 2013, p. 1272)
[27] (Raad voor de Jaarverslaggeving, 2016, p. 1)
[28] In het rapport wordt bij fondsenwervende instelling of organisatie geen onderscheid gemaakt tussen het woord 'instelling' of 'organisatie'
[29] (Fred van Hessen, 2009, p. 1)
[30] (Hans van der Westen en Nienke Teunissen, 2009, p. 15)
[31] (Prof. dr. René Bekkers, prof. dr. Theo Schuyt en drs. Barbara Gouwenberg, 2015, p. 15)

Richtlijn 650 Fondsenwervende organisaties

In mei 2016 is RJ 650 aangepast en gepubliceerd ('RJ-Uiting 2016-8'), op deze aanpassing kwamen diverse commentaren die uiteindelijk hebben geleid tot 'RJ-Uiting 2016-13'. RJ 650 Fondsenwervende instellingen is om een aantal redenen aangepast:

- In RJ 640 en RJ 650 waren diverse vergelijkbare bepalingen opgenomen; en
- Het SBF heeft een erkenningsregeling gepubliceerd die op 1 januari 2016 in werking is getreden. Deze regeling had tot doel om te komen tot een uniforme normering van de financiële verslaggeving van fondsenwervende instellingen.[32]

De belangrijkste wijzigingen van de nieuwe richtlijn ten opzichte van de vorige richtlijn zijn:

- De staat van baten en lasten is veranderd:
    - De baten worden ingedeeld naar herkomst (van wie of wat is het geld afkomstig);
    - De financiële baten en lasten worden weergegeven na het saldo van de baten en lasten;
    - De baten als tegenprestatie voor de levering van producten en/of diensten worden opgenomen onder de som van de geworven baten.
- Organisaties die RJ 650 toepassen moeten ook RJ 640 toepassen, dit geld echter niet voor het bestuursverslag.[33]

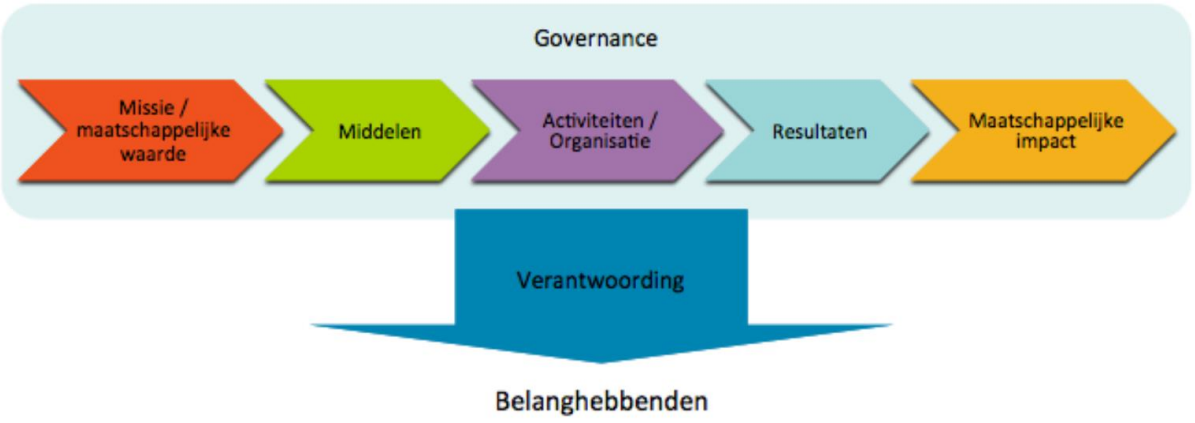
Erkenningsregeling

Op in 1 januari 2016 is de erkenningsregeling ingevoerd. Aan deze erkenningsregeling heeft vijf jaar voorbereiding ten grondslag gelegen. Zo sloten het SBF en de overheid in 2011 het convenant 'Ruimte voor Geven' en in 2014 heeft het CBF het rapport 'Toekomst Toezicht Filantropie' gepubliceerd. Ook de sector zelf heeft aan dit rapport bijgedragen.[34]

De doelen die de nieuwe erkenningsregeling wil bereiken, zijn:

- Het stimuleren van het realiseren van doelstellingen;
- Het bevorderen van de professionaliteit en kwaliteit van goededoelenorganisaties;
- Het bevorderen van het publieksvertrouwen.[35]

De erkenningsregeling komt in plaats van de bestaande keurmerken, gedragscodes en dergelijke principes. De uitgangspunten van die verschillende keurmerken en principes zijn meegenomen in het normenstelsel en gaan uit van een brede opvatting van filantropie. Het omvat de volledige



Figuur 42 Framework normenstelsel (Goede Doelen Nederland en IF, 2015)

[32] (Raad voor de Jaarverslaggeving, 2016, p. 1)
[33] (Raad voor de Jaarverslaggeving, 2016, pp. 1, 2)
[34] (Goede Doelen Nederland en IF, 2015, p. 1)
[35] (Goede Doelen Nederland en IF, 2015, p. 2)

filantropische keten: de gever, de organisatie en de begunstigde en is niet alleen gericht op de activiteiten en doelstellingen, maar ook op de maatschappelijke impact. Vanuit de sector was er sprake van een brede vorm van toezicht die naar deze factoren kijkt. De brede opvatting van filantropie in combinatie met het toezicht komt tot uiting in het framework (hierboven) voor het normenstelsel.[36]

Het toezicht sluit aan op de Code Goed Bestuur van het SBF die de volgende vier pijlers hanteert:

1. Besturen;
2. Toezicht houden;
3. Verantwoorden; en
4. Omgaan met belanghebbenden.[37]

Het framework en de vier pijlers van de Code Goed bestuur van het SBF hebben geleid tot een aantal normen waaraan een organisatie getoetst kan worden: missie/maatschappelijke waarde, middelen, activiteiten/organisatie, doelrealisatie, governance, verantwoording en belanghebbenden.[38]
Binnen het normenstelsel zijn organisaties onderverdeeld in een aantal categorieën, die gebaseerd zijn op de grootte (ontvangen baten). Naarmate de organisatie meer baten ontvangt, gelden er per categorie meer 'regels'.

[36] (Goede Doelen Nederland en IF, 2015, p. 2 t/m 5)
[37] (SBF - Samenwerkende brancheorganisaties filantropie, 2015, p. 8)
[38] (Goede Doelen Nederland en IF, 2015, p. 6)

Bijlage 1.2 Definiëring en ontwikkeling van risico en risicomanagement
In het vorige hoofdstuk hebben we gezien wat een fondsenwervende instelling is en in welk kader de fondsenwervende instelling kan worden bekeken. Net als het vorige hoofdstuk wordt in dit hoofdstuk een definiëring van een begrip (factor) behandeld; er wordt uitgelegd wat risico en risicomanagement is. Omdat deze termen vaak worden gebruikt zullen worden in het onderzoek en in het vervolg van het rapport is het belangrijk om te komen tot een goed begrip van deze termen.

Allereerst wordt uitgelegd wat de termen risico en risicomanagement inhouden. Tevens worden de redenen voor risicomanagement en de ontwikkeling van risicomanagement beschreven. Bij de ontwikkeling van risicomanagement wordt aandacht besteed aan de geschiedenis, het heden en de verwachtingen met betrekking tot risicomanagement. Als laatste wordt er een samenvatting gegeven.

Bijlage 1.2.1 Definitie van risico
Voor het inrichten van het risicomanagementproces is het belangrijk om helder te krijgen wat onder het begrip 'risico' wordt verstaan. Er zijn namelijk verschillende definities van het begrip risico die van elkaar afwijken. Hieronder worden vijf definities van risico gegeven die alle vijf van elkaar afwijken. Vervolgens worden in Tabel 11 de verschillen en overeenkomsten weergegeven.

In het algemeen denkt men bij risico alleen aan negatieve effecten, maar de volgende definities houden echter ook rekening met positieve effecten:

- De ISO 31000-richtlijn (2009) in combinatie met de Guide 73-2009 Risk Management Vocabulary, omschrijft risico als:

  > *The effect of uncertainty on objectives. In order to assist with the application of this definition, Guide 73 also states that an effect may be positive, negative or a deviation from the expected, and that risk is often described by an event, a change in circumstances or a consequence.*[39]

- COSO-II (2004) omschrijft risico als volgt:

  > *Events with a negative impact represent risks, which can prevent value creation or erode existing value. Events with positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation.*[40]

- De definitie die door Sonja Janicijevic, Paul Claes, Rob Lengkeek (2016) gegeven wordt van risico is: "Risico is de mogelijkheid dat zich een gebeurtenis voordoet in een gegeven periode en situatie, die een negatief effect heeft, waardecreatie verhindert of bestaande waardes uitholt."[41]

- Drs. Urjan Claassen RA RE CIA (2009) definieert risico als "een gebeurtenis die een negatief of positief effect heeft op het bereiken van de organisatiedoelstellingen".[42]

[39] (The association of Insurance and Risk Managers (airmic), The Public Risk Management Association (alarm), The institute of Risk Management (irm), 2009, p. 5)
[40] (Committee of Sponsoring Organisations of the Treadway Commission, 2004, p. 8)
[41] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 24)
[42] (Drs. Urjan Claassen RA RE CIA, 2009, p. 44)

- Lizanne Vroom (2014) steekt haar omschrijving van risico weer anders in: “Risico is de mogelijkheid dat positieve verwachtingen niet in vervulling gaan, onder bepaalde omstandigheden, in een bepaalde periode”.[43]

Om de verschillen inzichtelijk te maken, zijn de verschillende elementen per omschrijving hieronder opgenomen.

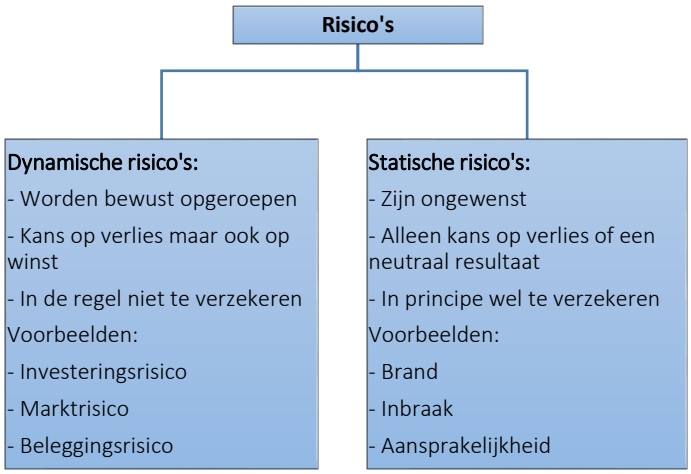
Tabel 11 Overzicht verschillen definities risico

	Onzekerheid	Negatief effect	Positief effect	Tijd	Situatie	Organisatie-doelstellingen
ISO 31000-richtlijn	✓	✓	✓		✓	✓
COSO-II		✓	✓			✓
Sonja Janicijevic, Paul Claes, Rob Lengkeek	✓	✓		✓	✓	
Drs. Urjan Claassen RA RE CIA		✓	✓			✓
Lizanne Vroom	✓	✓	✓	✓	✓	

De enige factor die bij alle vijf de omschrijvingen terugkomt, is de gebeurtenis met een negatief effect. Daarnaast wordt bij de meeste definities ook een gebeurtenis met een positief effect onderkend. Het is vreemd dat niet alle definities onzekerheid niet uitdrukkelijk noemen, ze hebben het alleen over gebeurtenissen. Risico bestaat immers volgens de risicoformule uit twee componenten: kans en gevolg (effect). Het is belangrijk hierbij te bedenken dat deze formule voornamelijk dient als denkmodel en niet als rekenmodel.

Bijlage 1.2.2 Indeling van risico

Gebeurtenissen met een negatief of positief effect vallen ook te koppelen aan de indeling van risico’s. Er kan bijvoorbeeld onderscheid gemaakt worden tussen dynamische en statische risico’s.[44] Vaak gaan deze risico’s samen, zo is het mogelijk dat men een bedrijf overneemt met het doel deze met winst te verkopen. Een risico kan echter zijn dat de waarde van de onderneming daalt door verslechterde economische omstandigheden, maar ook wanneer het pand afbrandt of de voorraad wordt gestolen. In geval van de verslechterde economische omstandigheden is er sprake van een dynamisch risico, in de andere gevallen is er sprake van een statisch risico.



Figuur 43 Onderscheid tussen dynamische risico's en statische risico's (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016)

[43] (Lizanne Vroom, 2014, p. 26)
[44] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, pp. 29, 30)

Lizanne Vroom (2014) haalt in haar boek "Risicomanagement vanuit het Dynamisch Business Model" twee indelingen aan. De eerste indeling is de indeling van risico's in strategische en operationele risico's, voor deze indeling wordt voornamelijk gekozen vanwege de verschillende verantwoordelijkheden en taken binnen de organisatie.[45] Zo kunnen strategische risico's over het algemeen gerelateerd worden aan besluiten van het topmanagement, terwijl operationele risico's veelal gerelateerd zijn aan de lagere niveaus binnen de organisatie. De tweede indeling is die van brutorisico (inherent risico) en nettorisico (restrisico), het gaat hierbij om het onderscheid van een risico voor het nemen van een beheersingsmaatregel en het risico na het nemen van een beheersingsmaatregel.[46] Het brutorisico is het risico dat bestaat voor de genomen beheersingsmaatregel, het nettorisico is het risico dat overblijft na de genomen beheersingsmaatregel.

Naast deze splitsingen kunnen risico's ook onderscheiden worden naar interne risico's en externe risico's. Een intern risico heeft zijn oorzaak binnen de organisatie, een extern risico heeft zijn oorzaak buiten de organisatie. Bij een intern risico kan gedacht worden aan fraude, bij een extern risico aan imagoschade. Externe risico's zijn veelal dynamisch en strategisch en interne risico's zijn voornamelijk van statische en operationele aard.

De indeling van risico's kan ook specifieker. Bij de bovenstaande indelingen konden risico's maar op twee manieren worden ingedeeld. Onderstaande indelingen gaan echter uit van meerdere categorieën.

Zo is er de categorale risico-indeling en de functionele risico-indeling. Een categorale risico-indeling heeft primair tot doel risicomanagement te gebruiken in de doorontwikkeling van het bedrijfsmodel en waardecreatie. De functionele risico-indeling heeft tot doel het onderhoud van risico's neer te kunnen leggen bij specialisten.[47]

De Raad voor de Jaarverslaggeving acht in richtlijn 400 alinea 110 de volgende risicocategorieën van belang:

- Strategie: de risico's van deze categorie zijn veelal van externe aard en belemmeren de realisatie van de strategie en langetermijndoelstellingen;
- Operationele activiteiten: dit zijn interne risico's die de effectiviteit en efficiëntie van processen en activiteiten beïnvloeden;
- Financiële positie: risico's die van invloed zijn op de financiële positie, deze zijn voornamelijk extern;
- Financiële verslaggeving: dit zijn veelal interne risico's, ze beïnvloeden de betrouwbaarheid van zowel interne als externe financiële verslaggeving;
- Wet- en regelgeving: dit kunnen zowel interne als externe risico's zijn, omdat ze voortvloeien uit regels van zowel buiten de organisatie (overheid e.d.) als binnen de organisatie. Deze risico's hebben invloed op de organisatie en de bedrijfsprocessen.[48]

Deze categorieën sluiten grotendeels aan bij de categorieën die in het ERM model (Bijlage 2.1 COSO ERM-model) worden onderscheiden, alleen de categorie 'financiële positie' is nieuw ten opzichte van het ERM model. In het ERM model worden deze indeling gekoppeld aan de organisatiedoelstellingen; risicomanagement is dan een hulpmiddel om zekerheid te verkrijgen over het behalen van de doelstellingen.

[45] (Lizanne Vroom, 2014, pp. 29, 30)
[46] (Lizanne Vroom, 2014, p. 31)
[47] (Drs. Urjan Claassen RA RE CIA, 2009, p. 46)
[48] (Raad voor de Jaarverslaggeving, 2014, p. 3)

Als men kijkt naar deze categorieën is het een samenvoeging van bepaalde categorieën van de functionele indeling (financieel en verantwoording) en de indeling van risico's in strategische en operationele risico's. Door samenvoeging van bepaalde indelingen kunnen er vragen ontstaan of bepaalde risico's onder de ene categorie of de andere categorie vallen.

Er zijn nog tal van andere risico-indelingen beschikbaar, de indelingen zoals die hierboven genoemd zijn, geven echter een vrij volledig beeld. Het gaat bovendien ook niet om een uitputtende lijst te geven met alle mogelijke indelingen, maar meer om een beeld te vormen van de meest relevante indelingen van risico's.

Bijlage 1.2.3 Definitie van risicomanagement

Aart, Horbeek, Jongsma en Verdonk (1990) beschrijven risicomanagement als: "de interactieve en iteratieve functie in het managementproces, die tot doel heeft de onzekerheden die de doelstellingen van een organisatie in positieve of negatieve zin kunnen beïnvloeden, op bedrijfseconomische wijze zo volledig en systematisch mogelijk te beheersen".[49]

Deze definitie legt de link tussen de doelstellingen van een organisatie en het risicomanagement. Dit komt tevens terug in de COSO-definitie van enterprise risk management (ERM).
COSO (2004) definieert het begrip 'enterprise risk management' als volgt:

> *Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*[50]

Deze definitie wordt door veel organisaties gebruikt als uitgangspunt voor de opzet van het (ondernemings)risicomanagement.

IS 31000 (2009), in combinatie met Guide 73, omschrijft risicomanagement als: "coordinated activities to direct and control an organization with regard to risk."[51] Volgens één van de principes moet risicomanagement integraal toegepast worden, in dit kader wordt dan ook gesproken over Risk Management Framework.[52] ISO 31000 definieert Risk Management Framework als volgt: "set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization."[53]

De definitie die door Sonja Janicijevic, Paul Claes, Rob Lengkeek (2016) gegeven wordt van risicomanagement is: "Risicomanagement is een combinatie van beleid, organisatie en processen opgezet en toegepast binnen de organisatie en gericht op het identificeren, beoordelen, beheersen en financieren van risico's, die de doelstellingen, mensen, middelen en immateriële belangen van de organisatie bedreigen."[54]

Lizanne Vroom (2014) definieert risicomanagement als:

[49] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 40)
[50] (Committee of Sponsoring Organisations of the Treadway Commission, 2004)
[51] (ISO, 2009)
[52] (Dick Hortensius en Ed Mallens, 2010, p. 10)
[53] (ISO, 2009)
[54] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 41)

Een systematisch en regelmatig onderzoek naar alle mogelijke risico's die de mensen, materiële en immateriële belangen en activiteiten van de organisatie bedreigen en daaraan gekoppeld een concrete aanpak om de (onacceptabele) risico's geheel of gedeeltelijk te voorkomen, om mede daardoor de bedrijfsdoelstellingen te kunnen realiseren.[55]

In onderstaande tabel zijn de verschillen en overeenkomsten tussen de vijf definities inzichtelijk gemaakt.

Tabel 12 Verschillen en overeenkomsten definities risicomanagement

	Functie en/of proces	Iteratief en/of interactief	Integrale toepassing	Risicobeheersing	Koppeling met doelstellingen
ISO 31000-richtlijn	✓		✓	✓	
COSO-II	✓		✓	✓	✓
Sonja Janicijevic, Paul Claes, Rob Lengkeek	✓			✓	✓
Aart, Horbeek, Jongsma, Verdonk	✓	✓		✓	✓
Lizanne Vroom	✓			✓	✓

Alle vijf de omschrijvingen geven aan dat risicomanagement een functie of proces is dat risico's beheerst. Vier van de vijf defenties leggen ook een koppeling met de doelstellingen en twee definities gaan uit van een integrale toepassing.

Onderzoek heeft uitgewezen dat risicomanagement binnen organisaties niet lang standhield als organisaties geen link legden tussen risicomanagement en de doelstellingen, naast het feit dat medewerkers nog niet voldoende doorgedrongen waren van de noodzaak van risicomanagement.[56] Het is daarom belangrijk dat organisaties binnen het risicomanagement een link leggen met de doelstellingen.

Bijlage 1.2.4 Redenen van risicomanagement

Nut en noodzaak voor risicomanagement ligt in een tweetal basisprincipes: het 'conformance-' en 'performance'-motief, het conformance-motief heeft betrekking op de wet- en regelgeving. [57] Zo is er regelgeving die relevant is voor risicomanagement, maar ook wetgeving waar risicomanagement direct uit voortvloeit.[58] Bij relevante wetgeving kan men denken aan het Burgerlijk Wetboek (art. 3:391 BW) en de Raad voor de Jaarverslaggeving (RJ 400). Bij wetgeving waar risicomanagment direct uit voortvloeit kan men denken aan Corporate-governanceregels en de erkenningsregeling (paragraaf Bijlage 1.1.3 Ontwikkelingen in en van de goededoelensector).

Het tweede basisprincipe heeft betrekking op het creëren van toegevoegde waarde, bij fondsenwervende organisaties zal dit betrekking hebben op het realiseren van maatschappelijke doelstellingen. [59]

Met betrekking tot het performance-motief hebben Koster en Snijders (1997)[60] vier belangrijke argumenten geformuleerd voor het belang van risicomanagement:

[55] (Lizanne Vroom, 2014, p. 31)
[56] (Erik van de Crommenacker, Peter Dona, Siebrand van der Ploeg, 2015, p. 54)
[57] (Drs. Urjan Claassen RA RE CIA, 2009, p. 17)
[58] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, pp. 15, 16)
[59] (Drs. Urjan Claassen RA RE CIA, 2009, p. 17)
[60] In het boek 'Een continue afweging van risico's tegen genoegens' (1997)

1. Risicomanagement kan organisaties inzicht geven in wat kan gebeuren;
2. Risicomanagement stelt organisaties in staat om prioriteiten toe te kennen aan onderkende risico's en daardoor gestructureerd acties te ondernemen, waardoor lukrake acties voorkomen kunnen worden;
3. Risicomanagement maakt het organisaties mogelijk om bij besluitvorming een betere financiële afweging te maken om maatregelen te treffen.
4. Risicomanagement maakt het voor organisaties mogelijk om genomen beslissingen aangaande risico's te verantwoorden.[61]

Dit sluit aan bij de vijf voordelen die organisaties zelf noemen van risicomanagement, die naast de vier hierboven genoemde voordelen, verbeterde governance, als voordeel noemen.[62]

Veel organisaties onderschatten het nut van risicomanagement en verrichten alleen de (minimale) werkzaamheden die verplicht zijn (conformance-motief). Dit terwijl uit onderzoek van Booz Allen Hamilton uit 2004 is gebleken dat 87% van het verlies aan 'maatschappelijk nut', te wijten was aan operationele en strategische blunders en dus niet aan wet-en-regelgeving.[63] Fondsenwervende instellingen hechten echter over het algemeen meer belang aan het uitvoeren van activiteiten en het afleggen van verantwoording daarover, dan aan risicomanagement en de risicoparagraaf.

[61] (Focus op verbeteren, 2015, p. 4)
[62] (Thomas Hürlimann, 2011, p. 3)
[63] (Nederlandse Beroepsorganisatie van Accountants (NBA), Nyenrode Business Universiteit, Rijksuniversiteit Groningen, PwC, 2014, p. 15)

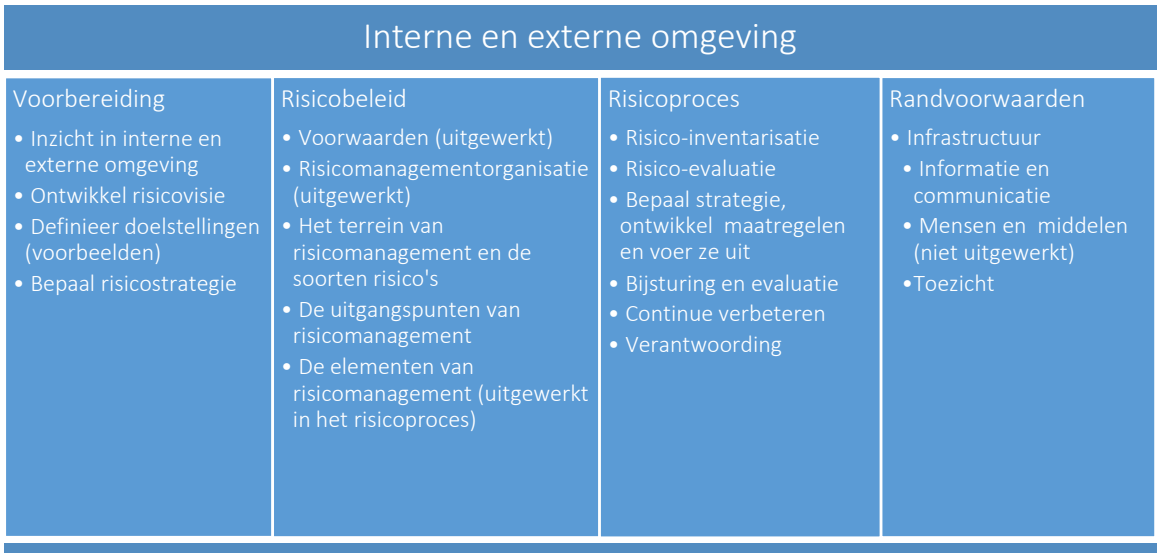
Bijlage 1.3 De bouwstenen van risicomanagement

Dit hoofdstuk gaat in op de inrichting van het risicomanagement. Het is belangrijk om te weten hoe risicomanagement wordt ingericht om zo de resultaten uit het onderzoek beter te kunnen analyseren. In dit hoofdstuk wordt niet specifiek ingegaan op het risicomanagement bij fondsenwervende instellingen. Dit is omdat de bouwstenen van het risicomanagement tussen organisaties niet (wezenlijk) verschillen.

Allereerst wordt aangegeven wat er moet gebeuren voordat er met risicomanagement wordt begonnen. Daarna wordt het risicobeleid, het risicoproces en de randvoorwaarden behandeld (figuur hieronder). Als laatste wordt er een samenvatting gegeven.

Bijlage 1.3.1 Voorbereiding

Aangezien dit hoofdstuk de kern (diepte-onderzoek) vormt van het theoretisch kader en er veel onderwerpen en stappen worden behandeld, wordt in een schema, op volgorde, de te bespreken elementen weergegeven.



Figuur 44 Leeswijzer bijlage 1.3

Inzicht in interne en externe omgeving

Voordat er begonnen wordt met het formuleren van het risicobeleid en een risicovisie is het verstandig om eerst inzicht te krijgen in de omgeving van de organisatie en in de organisatie zelf. Op basis van deze oriëntatie kunnen de missie en visie worden geformuleerd, maar ook het risicobeleid en de risicovisie. De Zwitsers Alexander Osterwalder en Yves Pigneur hebben hiervoor een inzichtelijk businessmodel ontworpen: 'Canvas', dat hiervoor gebruikt kan worden. Het geeft een overzicht van alle belangrijke bedrijfsprocessen in hun samenhang.[64] Lizanne Vroom heeft dit model doorontwikkeld tot haar eigen model (Bijlage 9 Het Dynamisch Business Model).

Risicovisie

Voordat een risicobeleid geformuleerd kan worden, moet er eerst een risicovisie gedefinieerd worden. Deze visie (gebaseerd op de missie en visie) geeft het toekomstbeeld aan en wat de rol van risicomanagement hierin is. Drs. Urjan Claassen RA RE CIA (2009) onderscheidt vier functies van de risicovisie: richting geven, inspireren, onderscheiden en (over)leven.[65] In dit kader kan ook de

[64] (Erik van de Crommenacker, Peter Dona, Siebrand van der Ploeg, 2015)
[65] (Drs. Urjan Claassen RA RE CIA, 2009, p. 70)

risicomanagementfilosofie (Figuur 57) worden onderscheiden, waarbij de kernwaarden van de organisatie ten opzichte van risico's beschreven worden.

Risicomanagementdoelstellingen

Bij het benoemen van de risicomanagementdoelen is het belangrijk dat er een link wordt gelegd met de organisatiebrede doelstellingen. Door deze als uitgangspunt te nemen, kan de risicostrategie en het risicobeleid ontwikkeld en bepaald worden in relatie met de strategie van de organisatie, waardoor waardecreatie kan worden ondersteund.[66] Dit sluit ook aan op één van de voorwaarden van effectief risicomanagement (Bijlage 1.3.2 Risicobeleid).

Jaap Zijlstra en Lizanne Vroom (2014) noemen een aantal voorbeelden van risicomanagementdoelstellingen, een selectie van deze voorbeelden is hieronder opgenomen:

- "Het bevorderen van een ononderbroken voortgang van de activiteiten van de onderneming en het zo spoedig mogelijk opheffen van ongewenste onderbrekingen als die zich toch zouden voordoen";
- "Het zorgen voor stabiliteit in de winst en 'rust in de begroting' van de onderneming door onverwachte verliezen ten gevolge van schaden te voorkomen";
- "Ervoor zorgen dat de onderneming haar ethische en maatschappelijke verantwoordelijkheid onbelemmerd door risico's kan dragen";
- "Het bevorderen van vertrouwen in de onderneming, zowel bij het eigen management (de eigen directieleden), als bij de medewerkers en derden, door het wegnemen van (statische) risico's, die inherent zijn aan de aard van de werkzaamheden binnen de organisatie"; en
- "Het opbouwen, hooghouden en beschermen van de goede naam van de onderneming".[67]

Risicostrategie

De risicostrategie beschrijft welke en hoeveel risico de organisatie (management) wenst te nemen. Deze strategie is wezenlijk anders dan de strategie die de organisatie hanteert ter beheersing van risico's, zoals beschreven in Bijlage 1.3.3 Risicomanagementproces. In dit kader kan ook de risicohouding onderscheiden worden.

Figuur 45 Overzicht factoren van risk appetite (COSO, 2012)

Bij het bepalen van de doelstellingen en de strategie om deze te bereiken, moet het management rekening houden met de risico's en de houding ten opzichte van deze risico's. Het bereiken van doelstellingen hangt namelijk af van het identificeren van risico's en het bepalen of deze risico's binnen de risk appetite van de organisatie vallen. Dit heeft weer effect op de maatregelen die een organisatie moet nemen. Risk appetite wordt dus niet ontwikkeld als een losstaande factor (figuur hierboven). Zo moet een organisatie het vermogen bepalen om risico's op te kunnen vangen in nastreving van de doelstelling. Het moet ook het bestaande risicoprofiel meenemen, niet als bepalende factor voor risk appetite, maar meer als indicatie van de risico's waarop het zich momenteel richt.[68]

[66] (Drs. Urjan Claassen RA RE CIA, 2009, pp. 71, 72)
[67] (Jaap Zijlstra & Lizanne Vroom, 2014, pp. 79, 80)
[68] (Committee of Sponsoring Organizations of the Treadway Commision, 2012, p. 3)

Bijlage 1.3.2 Risicobeleid

Het risicomanagementbeleid en de plaats van risicomanagement binnen de organisatie worden in deze paragraaf besproken. Het risicomanagementproces wordt in de daaropvolgende paragraaf behandeld.

Volgens Sonja Janicijevic, Paul Claes, Rob Lengkeek (2016) bestaat het risicomanagementbeleid meestal uit de volgende elementen:

- De risicomanagementdoelstellingen;
- De voorwaarden waaraan een effectief risicomanagement moet voldoen;
- Het beschrijft de risicomanagementorganisatie plus de rollen en verantwoordelijkheden ervan;
- Het bepaalt het terrein van risicomanagement en welke soorten risico's relevant zijn voor het management;
- Het beschrijft de uitgangspunten om risicomanagement te waarborgen;
- Het geeft de elementen weer van het risicomanagementproces.[69]

Uit deze opsomming blijkt dat de voorbereiding en het risicobeleid dicht bij elkaar liggen en ook door elkaar heen kunnen lopen. In dit rapport is ervoor gekozen om de risicomanagementdoelstellingen onder de voorbereiding te plaatsen omdat het risicobeleid een nadere en concretere uitwerking van de risicovisie en –doelstellingen is.

Voorwaarden effectief risicomanagement

Ingaande op de voorwaarden waaraan een effectief risicomanagement moet voldoen blijkt volgens Bosman (2009) dat, naast de te volgen stappen van het risicomanagementproces, met name cultuur- en structuuraspecten belangrijk zijn voor een succesvolle uitvoering van risicomanagement:

- De verantwoordelijkheden zijn belegd op strategisch, tactisch en operationeel niveau; positionering van risicomanagement is een randvoorwaarde voor het creëren van draagvlak;
- Het risicobewustzijn betreffende verschillende risicogebieden wordt actief gedeeld op strategisch, tactisch en operationeel niveau. Het stimuleert het organisatiebrede risicobewustzijn;
- Risicomanagement maakt deel uit van (besluitvormings)processen. Risicomanagement dient als een adequaat sturingsmechanisme voor het op niveau houden en verbeteren van de processen en de organisatie;
- Risicomanagement sluit aan bij de doelstellingen van de organisatie. De risico's die de doelstellingen van de organisatie bedreigen zijn het belangrijkst.[70]

Deze aspecten wordt ook genoemd door organisaties zelf, als zijnde kritisch voor het presteren van een organisatie, naast dat risico's proactief geïdentificeerd worden, beslissingen binnen de risico-tolerantie (houding) vallen en het aansturen van risico beperkende activiteiten.[71]

De risicocultuur omvat de gemeenschappelijke kernwaarden, houding en gebruiken die beschrijven hoe mensen binnen een organisatie omgaan met risicomanagement. Risicocultuur komt voor een deel voort uit de risicovisie en de risicostrategie. Belangrijk bij de risicocultuur is dat het topmanagement het goede voorbeeld geeft.[72] Een risicomanagementcultuur levert veel voordelen op binnen een organisatie, dit wordt ook benadrukt door Chapman en Ward (Bijlage 8 De gunstige effecten van evenwichtig risicomanagement in een gezonde bedrijfscultuur).

[69] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 45)
[70] (Bosman, 2009, p. 56)
[71] (Thomas Hürlimann, 2011, p. 1)
[72] (Drs. Urjan Claassen RA RE CIA, 2009, p. 58)

In een wereld waar alles op rolletjes loopt en er geen tegenslagen zijn, neemt het risicobewustzijn af. Daniel Kahneman (2012) stelt dat mensen zich minder bewust worden van risico's als die zich een lange periode niet hebben voorgedaan. Verder benadrukte hij dat mensen individueel het moeilijk hebben om risico's juist in te schatten; men denkt te licht over risico's. [73]

Figuur 46 Ontwikkeling van risk readiness (Thinka Bor-Reijinga en Gert van der Kolk, 2014)

Zelfreflectie, in combinatie met andere soft controls en het gezamenlijk beoordelen van risico's is daarom noodzakelijk om risico's te beheersen en uiteindelijk de gewenste resultaten te behalen.[74]

In een organisatie waar hard controls de overhand hebben is het van belang om deze te verbinden met soft controls (Bijlage 7 Soorten beheersingsmaatregelen op verschillende niveaus). Dit kan gebeuren door risk readiness; het dient ertoe om er bewust van te worden dat er meer is dan alleen hard controls. Samen met hard controls en soft controls leidt risk readiness tot houding en gedrag. Afhankelijk van de gewenste houding en gedrag dienen er hard controls en soft controls aanwezig te zijn.[75]

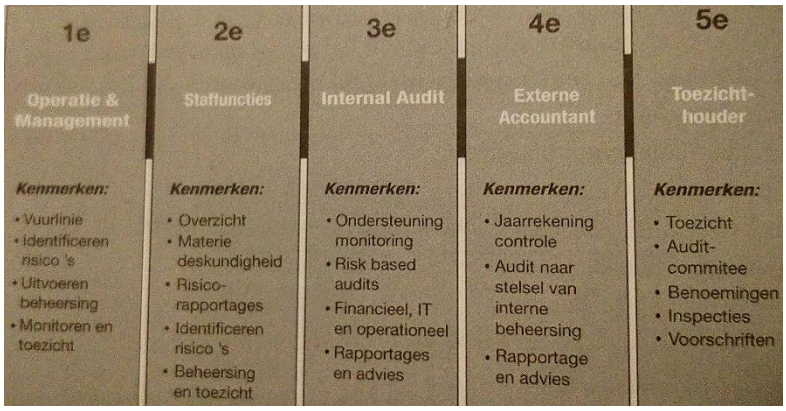
In de volgende subparagraaf wordt verder ingegaan op de structuuraspecten. Dit is zowel een onderdeel van het risicobeleid als een voorwaarde voor effectief risicomanagement die door Bosman (2009) onderscheiden wordt.

De organisatie van risicomanagement, taken en verantwoordelijkheden

Wat betreft de plaats van risicomanagement in de organisatie, moet er iemand zijn die verantwoordelijk is voor risicomanagement: de risicomanager (CRO). Uit onderzoek is gebleken dat organisaties die een CRO hebben aangesteld, hoger scoren op het gebied van risicomanagement.[76] Niet alle organisaties hebben een risicomanager, bijvoorbeeld door de beperkte omvang of doordat ze een extern adviesbureau hiervoor hebben ingehuurd. De risicomanager moet in een positie in de organisatie hebben, waaruit hij overzicht heeft over alle afdelingen. De voorkeur van de plaats van een risicomanager gaat in dit kader uit naar een staffunctie voor de risicomanager. Volgens Sonja Janicijevic et. al (2016) zijn hiervan de voordelen:

- Betere coördinatie en controle van de uitvoering van de genomen maatregelen; en
- Een centrale staffunctionaris kan een grote deskundigheid opbouwen.[77]

Uitgangspunt hierbij moet echter zijn dat men in de top van het bedrijf zelf ook de relevante

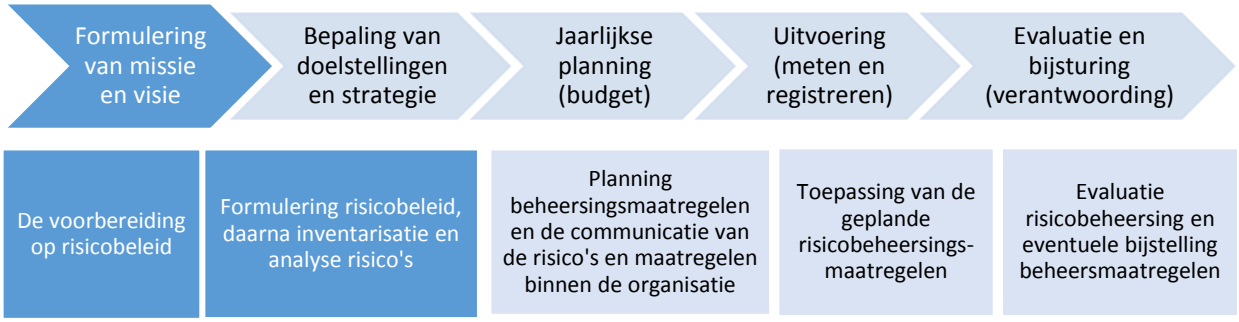


Figuur 47 Verdedigingslinies voor risicomanagement (Drs. Urjan Claassen RA RE CIA, 2009)

[73] In het boek 'Ons feilbare denken – thinking, fast and slow' (2012)
[74] (Thinka Bor-Reijinga en Gert van der Kolk, 2014, p. 10 t/m 12)
[75] (Thinka Bor-Reijinga en Gert van der Kolk, 2014, pp. 37, 38)
[76] (Nederlandse Beroepsorganisatie van Accountants (NBA), Nyenrode Business Universiteit, Rijksuniversiteit Groningen, PwC, 2014, pp. 55, 56)
[77] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, pp. 48, 49)

risico's kent, de risicomanager mag hiervoor geen substituut zijn.
Zoals eerder gezegd is risicomanagement een bezigheid voor de gehele organisatie. Iedereen draagt dus een stuk verantwoordelijkheid voor de uitvoering van hun taken met betrekking tot risicomanagement. [78] Deze verantwoordelijkheden kunnen worden onderverdeeld in vijf verdedigingslinies (Figuur 47). In bijlage 5 zijn de taken en de benodigde risicobewustzijn en kennis per verdedigingslinie uitgewerkt.

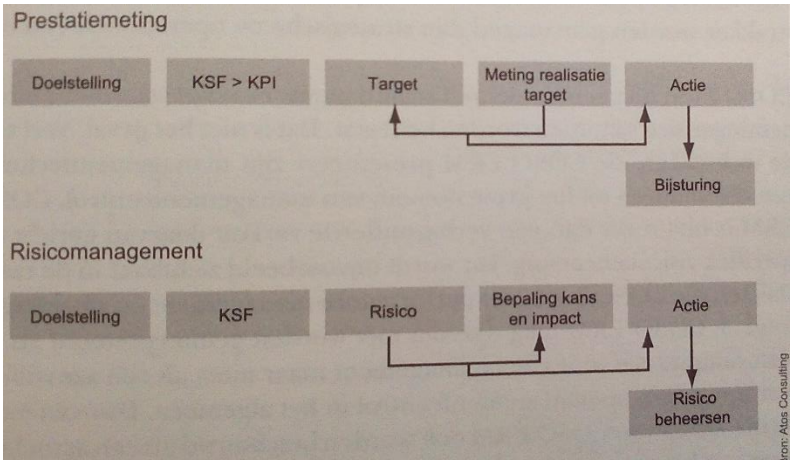
Als risicomanagement onderdeel uit gaat maken de managementdiscipline, verliest het zijn procesmatige karakter. Het is dan opgenomen in de planning-en-controlcyclus. Bij het opstellen van de planning-en-controlcyclus wordt dus gelijk rekening gehouden met de risico's.[79]



Figuur 48 Koppeling risicomanagement aan planning-en-controlcyclus (o.b.v. literatuur Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016)

Het is tevens verstandig om prestatiemanagement te koppelen aan risicomanagement. Want de buitenwereld houdt degene die verantwoordelijk is voor de resultaten, ook verantwoordelijk voor de risico's.[80]

Prestatiemeting kan op verschillende niveaus gebeuren. Allereerst moet gekeken worden hoe prestaties gemeten gaan worden en waarmee prestaties vergeleken worden. Hierbij komt ook de term 'verantwoordelijkheidscentra' om de hoek kijken.



Figuur 49 Prestatiemeting en risicomanagement (Rob Uiterlinden, 2009)

Verantwoordelijkheidscentra bij fondsenwervende instellingen zijn meestal 'discretionary' kostencentra, zo is het resultaat moeilijk te meten in geld. Vaak werken deze organisatorische eenheden met budgetten. Het is daarom van groot belang dat deze organisaties overeenstemming bereiken over de doelstellingen, niet alleen op strategisch niveau, maar ook op operationeel niveau. Men dient duidelijke en bij voorkeur kwantitatieve normen te hanteren om zo prestaties te kunnen beoordelen.[81] Prestaties kunnen gekoppeld worden aan de voortgang van het behalen van doelstellingen.

[78] (Drs. Urjan Claassen RA RE CIA, 2009, p. 77)
[79] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 52 t/m 54)
[80] (Nederlandse Beroepsorganisatie van Accountants (NBA), Nyenrode Business Universiteit, Rijksuniversiteit Groningen, PwC, 2014, p. 12)
[81] (Eppink, Dr. D. en Keuning, Dr. D.J., 2012, pp. 581, 582)

Ook beloning heeft veel raakvlakken met verantwoordelijkheidscentra en prestaties. Een manier om het risicobewustzijn en aandacht voor risicomanagement te versterken is het integreren van risicomanagement in de beloningen. De prestaties van medewerkers op het gebied van het inventariseren van risico's, beoordelen en beheersen van risico's zou dan een onderdeel moeten gaan vormen van functioneringsgesprekken.[82] De voornaamste van deze drie factoren is het beheersen van risico's (voor elke medewerker), het is namelijk niet altijd zo dat iedereen binnen de organisatie de risico's inventariseert en beoordeelt. Het is echter belangrijk om te bedenken dat het te ver doorvoeren van prestatiegericht belonen, uiteindelijk zich tegen de organisatie kan keren.

Terrein van risicomanagement en soorten risico's

Risicomanagement kan een groot gebied beslaan; risico's kunnen betrekking hebben op diverse bedrijfsonderdelen en externe factoren, afhankelijk van de aard van de activiteiten, de grootte van de organisatie en de externe omgeving. Het is daarvan van belang om een focus en/of afbakening aan te brengen; waar wordt wel en waar wordt geen (extra) aandacht aan besteed. Risico's kunnen dan ook op diverse manieren worden ingedeeld (Bijlage 1.2.2 Indeling van risico).

De uitgangspunten van risicomanagement

Risicomanagementactiviteiten staan in samenhang met de strategie en doelstellingen, risicomanagement moet dus ten gunste staan van de strategie en de doelstellingen. De visie, missie, strategie en doelstellingen van de organisatie staan centraal en vormen dan ook de uitgangspunten voor risicomanagement.[83]

Dit is echter nog wel wat anders als de uitgangspunten van risicomanagement op zichzelf. De uitgangspunten van risicomanagement houden verband met de risicovisie, -filosofie en –principes en gaan verder dan alleen de eerder genoemde punten. Dit wordt onder andere duidelijk gemaakt door het ISO 31000 model, waarin hoofdstuk 3 aandacht wordt besteed aan de principes die moeten worden toegepast (Bijlage 2.3 ISO 31000-richtlijn) en de principes volgens het COSO model van 2013 (Bijlage 12 De gebruikte principes voor de scoreleidraad).

Voorbeelden, voortschrijdend op de behandelde elementen van risicobeleid, van risicobeleid zijn de "Risk Policy and Risk Management Procedures" van de "University of the West of England"[84] en de "Risk Management Policy" van de "Heriot Watt University".[85]

De elementen van risicomanagement

Hiermee worden de verschillende stappen bedoeld in het risicomanagementproces, hierbij valt dus te denken aan de inventarisatie, evaluatie, het nemen van maatregelen, evaluatie en bijsturing, continu verbeteren en verantwoording. Deze stappen worden afzonderlijk in de volgende paragraaf behandeld.

Bijlage 1.3.3 Risicomanagementproces

In deze paragraaf worden de stappen van het risicomanagementproces behandeld. Deze stappen worden gescheiden van de randvoorwaarden, zoals toezicht, informatie en communicatie. De stappen van het risicomanagementproces zijn risico-identificatie, risicoanalyse, het nemen van beheersingsmaatregelen, de evaluatie ervan en de daarmee samenhangende eventuele bijsturing, continu verbeteren en verantwoording.

[82] (Lizanne Vroom, 2014, p. 258)
[83] (Jaap Zijlstra & Lizanne Vroom, 2014, p. 23)
[84] (The UWE Bristol Fund)
[85] (Phil McNaull and Lorraine Loy, 2008)

Risico-identificatie

Er bestaat geen vaste, waterdichte methode die kan worden gebruikt bij risico-inventarisatie. De risico-identificatie zal per bedrijf verschillen omdat elk bedrijf uniek is. Organisaties verschillen immers in aard, omvang en activiteiten.

Echter, voordat de risico-inventarisatie kan plaatsvinden, moet er een oriëntatie op de organisatie hebben plaatsgevonden. Verder moet de reikwijdte van de risico-identificatie worden bepaald. Voor deze oriëntatie kan men ook gebruik maken van de oriëntatie die al eerder is uitgevoerd bij het bepalen van de missie, visie en doelstellingen (Bijlage 1.3.1 Voorbereiding). De reikwijdte van de risico-identificatie is als het goed is vastgelegd bij de ontwikkeling van het risicobeleid (Bijlage 1.3.2 Risicobeleid).

De aanpak van het inventariseren van risico's kan op verschillende manieren:

- De eerste benadering onderzoekt de samenhang tussen mogelijke schadeoorzaken en de belangen, objecten of personen van deze mogelijke schadeoorzaken, en de schade die als gevolg van de risico's kan ontstaan;
- De ERMS van de FERMA identificeert risico's op een systematische manier aan de hand van belangrijke activiteiten in een organisatie;
- De COSO gaat uit van de zogenoemde 'objective based risk identification approach', hierbij worden risico's geïdentificeerd en gekoppeld aan de doelstellingen;
- Een andere methode is om bij elk balansonderdeel na te gaan of er sprake is van een risico.[86]

Het is belangrijk om een goed gestructureerde aanpak te hanteren die aansluit bij de structuur van de klant.[87] Hierbij moet ook de afweging worden gemaakt of de aanpak wel efficiënt en effectief is.

Als de voorbereidende stappen gevolgd zijn en de manier van aanpak bepaald is, kunnen de risico's geïdentificeerd worden.

De inventarisatie van risico's gebeurt in twee fasen. In de eerste fase probeert men een juist en volledig beeld te krijgen van alle mogelijke risico's door middel van een organisatiebrede analyse. Een veelgebruikt hulpmiddel hierbij is de algemene checklist en het Dynamisch Business Model (Bijlage 9 Het Dynamisch Business Model), andere hulpmiddelen zijn het vijfkrachtenmodel van Porter en de DESTEP-analyse voor externe risico's en de SWOT-analyse voor zowel interne als externe risico's. In de tweede fase worden risico's die lastig zijn te definiëren, nader onderzocht. Bij de inventarisatie van risico's is het aan te raden dat mensen uit verschillende niveaus en onderdelen die pessimistisch ingesteld zijn de risico-identificatie uit te laten voeren.[88] Enerzijds om zo tot een volledig mogelijke risicolijst te komen en anderzijds om het risicobewustzijn in de organisatie te verbeteren.
In de tweede fase worden de risico's die nader onderzoek nodig hebben verder onderzocht.

Het onderzoeken van de schadehistorie is van belang voor de risico-identificatie. Het analyseren en onderzoeken hiervan hoort feitelijk bij de volgende stap. Maar de schadehistorie is ook een indicatie voor de aanwezigheid van risico. Ook het bijhouden van een register met 'bijna-schaden' is van belang voor de aanwezigheid van risico. [89] Bij het vastleggen van schadehistorie kan gedacht worden aan dezelfde factoren die worden vastgelegd bij de risicolijst.

[86] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 77 t/m 80)
[87] (Jaap Zijlstra & Lizanne Vroom, 2014, p. 98)
[88] (Erik van de Crommenacker, Peter Dona, Siebrand van der Ploeg, 2015, p. 139)
[89] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 87)

Het proces van inventarisatie van risico's gebeurt in drie stappen:

1. Het identificeren: het achterhalen van gebeurtenissen die het realiseren van de doelstellingen bedreigen;
2. Het toewijzen van oorzaken aan risico's: hierbij wordt gelet op het 'waar', 'hoe', en 'wanneer' van het risico. Het achterhalen van de oorzaken is van belang voor het nemen van beheersingsmaatregelen;
3. Het meten van risico's: hierbij moeten de prestatie-indicatoren van de mogelijke gevolgen in kaart worden gebracht. Dit kan zowel kwantitatief als kwalitatief. [90]

Bij het toewijzen van oorzaken aan risico's is het van belang om te bepalen of men invloed kan uitoefenen op deze oorzaken. Dit bepaalt namelijk mede de manier waarop met deze risico's wordt gegaan. Oorzaken waarop je geen invloed hebt zijn namelijk niet te voorkomen, maar de impact kan nog wel beperkt worden of er kunnen correctieve maatregelen genomen worden.[91] Risico's kunnen ook een relatie hebben met andere risico's, bij het inventariseren moeten risico's dus in een breder verband worden bekeken, hetzelfde geldt bij het bedenken van maatregelen.[92] Verder is het van belang om de risico's te relateren aan de doelstellingen, zoals al eerder aangegeven in hoofdstuk 4.

Het eindresultaat van de risico-inventarisatie is een risicolijst (tabel hieronder). In deze lijst wordt het soort risico genoemd en de omschrijving genoemd. Verder wordt de oorzaak, degene voor wie het risico geldt (risico-eigenaar) en de eventuele beheersingsmaatregelen die al genomen zijn, benoemd.[93] Door risico-eigenaren te benoemen, neemt de kans toe dat medewerkers zelf verantwoordelijkheid nemen voor de risicobeheersing.[94]

Tabel 13 Voorbeeld risicolijst (o.b.v. literatuur Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016)

Strategische doelstellingen	**Doelstelling 1**		**Doelstelling 2**		**Doelstelling 3**	
Operationele doelstellingen	Doelstelling 1.1	Doelstelling 1.2	Doelstelling 2.1	Doelstelling 2.2	Doelstelling 3.1	Doelstelling 3.2
Politiek						
Technologie						
Juridisch						
Communicatie						
Organisatie & Personeel						
Financieel						
Uitvoering						
Markt						
Verantwoording						

De tabel hierboven geeft een mogelijke risicolijst weer, in deze lijst worden de doelstellingen gekoppeld aan de risico's. Hierbij wordt gekeken naar risico's die bij de strategische doelstellingen horen (strategische risico's) of bij de operationele doelstellingen (procesrisico's). Risico's worden in dit geval ingedeeld aan de hand van de functionele risico-indeling (zie paragraaf Bijlage 1.2.2 Indeling van risico), deze indeling is onder de operationele doelstellingen weergegeven. In de lege cellen moeten de omschrijving van het risico, de oorzaak en de risico-eigenaar plus de eventuele al genomen maatregelen worden weergegeven.

[90] (Drs. Urjan Claassen RA RE CIA, 2009, pp. 90, 91)
[91] (Erik van de Crommenacker, Peter Dona, Siebrand van der Ploeg, 2015, pp. 135, 136)
[92] (Lizanne Vroom, 2014, p. 128)
[93] (Roel Grit, 2009, p. 39 t/m 41)
[94] (Jaap Zijlstra & Lizanne Vroom, 2014, p. 99)

Risicobeoordeling

Het is belangrijk om de risico-inventarisatie en de risico-evaluatie gescheiden te houden, zo kan men met een open blik naar risicosituaties kijken. Als men namelijk bij de risico-inventarisatie al prioritering aanbrengt in risicosituaties, is het mogelijk dat bepaalde risicosituaties over het hoofd worden gezien.[95]

Bij het beoordelen van risico's staan drie componenten centraal. Twee van deze componenten worden weergegeven in de risicoformule (kans en gevolg) en de andere component is de relatie met de doelstellingen.[96] Tevens spelen psychologische aspecten (risicoperceptie) een belangrijke rol bij het beoordelen van risico's. Later in deze paragraaf wordt hier nader op ingegaan.

Als wordt ingegaan op de component 'gevolg' van de risicoformule zijn twee zaken van belang om de omvang van dit 'gevolg' te kunnen bepalen:

1. Criteria: hoe wordt de omvang van een risico gemeten?
2. Tijdsfactor: wat zijn de gevolgen van het risico op korte, middellange en lange termijn?

Om de omvang van een gevolg van een gebeurtenis goed in te kunnen schatten speelt ervaring een belangrijke rol. [97]

Als wordt ingegaan op de component 'kans' is de kwaliteit van deze beoordeling een belangrijk aspect. Voor het inschatten van de kans worden veelal statistische methoden gebruikt, maar toepassing hiervan is echter niet altijd mogelijk. Bijvoorbeeld bij risico's die zich incidenteel en zonder periodiciteit voordoen. Het is daarom verstandig om dieper in te gaan op de aard van de gebeurtenis. Net als bij het bepalen van de omvang van het gevolg is ook bij het bepalen van de kans, ervaring van groot belang.[98]

Naast de ervaring en deskundigheid die benodigd is om de kans en het gevolg in te schatten is het ook belangrijk om te bepalen wie het gevolg en de kansen inschatten. Zoals gezegd hebben mensen het individueel moeilijk om risico's in te schatten; risico's worden vaak onderschat (Bijlage 1.3.2 Risicobeleid). Het is daarom van belang om te kijken wie risico's inschatten en of er meerdere mensen risico's inschatten.

Bij het bepalen van de omvang van het risico dient ook de relatie met de doelstellingen meegenomen te worden. Als een risico de realisatie van de doelstellingen bedreigt, is dat een indicatie van het belang van het risico. Verder moet er ook rekening gehouden worden waar risico's zich voordoen. Zo kunnen risico's niet of minder van belang zijn voor de doelstellingen van een organisatie als geheel maar kunnen wel van belang zijn voor de doelstellingen van een divisie of dochteronderneming.[99]

Als gekeken wordt naar het 'hoe' van de risicoanalyse, onderscheidt Roel Grit (2009) twee methoden:

- De kwantitatieve methode:
    - Kwantitatief in risicobedragen: de omvang van de gevolgen van risico's worden onderling vergeleken door middel van geldbedragen per jaar. Deze worden dan gecombineerd met de kans, die tussen 0 en 1 ligt. Het risicobedrag wordt dan berekend door de omvang en de kans te vermenigvuldigen;
    - Kwantitatief met risicofactoren: risico's worden met elkaar vergeleken door middel van kansklassen, gevolgklassen en risicofactoren; en

[95] (Jaap Zijlstra & Lizanne Vroom, 2014, pp. 120, 121)
[96] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 126)
[97] (Drs. Urjan Claassen RA RE CIA, 2009, p. 111)
[98] (Drs. Urjan Claassen RA RE CIA, 2009, p. 112)
[99] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 126)

- De kwalitatieve methode: sommige risico's zijn lastig uit te drukken in geldbedragen. De omvang van het risico wordt dan aangeduid door elementen of scenario's ervan te beschrijven en eventueel te vergelijken met eerdere ervaringen. De kans en impact worden vaak omschreven met termen als: hoog, midden en laag.[100]

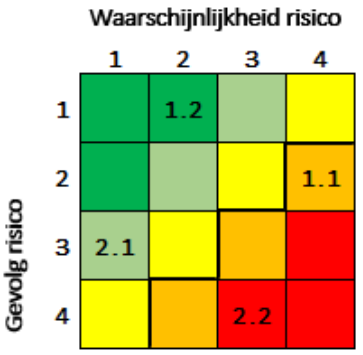
Een aantal technieken, zowel kwantitatief als kwalitatief om risico's te kunnen beoordelen, zijn opgenomen in bijlage 3.

Bij de keuze of men de kwantitatieve of de kwalitatieve benadering gebruikt, onderscheiden Sonja Janicijevic et. al (2016) een aantal factoren:

- De aard van het risico: het ene risico is makkelijker uit te drukken in bedragen dan het andere risico, denk bijvoorbeeld aan imagoschade;
- Het doel van de analyse: wil de risicomanager of het topmanagement alleen een prioritering van de risico's of vormt dit ook de basis voor het opstellen van rapportages e.d.; en
- De aard en voorkeur van gebruikers van de risico-informatie: zijn de stakeholders en de organisatie zelf geïnteresseerd in bedragen of meer in een beschrijvende manier van risico's.[101]

Een kwantitatieve benadering komt meestal betrouwbaarder over dan een kwalitatieve benadering. Uit de omschrijving van risico is echter gebleken dat de factor onzekerheid, van zowel kans als impact, een belangrijke rol speelt. Een kwantitatieve benadering is dus niet per definitie altijd betrouwbaarder.

Het eindresultaat van de inventarisatie en analyse van risico's is het risicoprofiel (Tabel 15). In het risicoprofiel is het ook mogelijk om de al genomen beheersingsmaatregelen op te nemen. Dit kan dan worden opgenomen na het inherente risico (Tabel 16). Vervolgens kan beoordeeld worden hoeveel risico er overblijft (nettorisico). Als dit gedaan wordt, vervagen wel de grenzen tussen de stappen risicoanalyse en evaluatie van maatregelen. Het risicoprofiel dient regelmatig aangepast te worden evenals bij veranderingen die van (grote) invloed zijn op de organisatie. Deze actualisatie hangt af van de grootte van de organisatie en de snelheid van de veranderingen binnen en buiten de organisatie.



Figuur 50 Risicomap

Een methode binnen het risicoprofiel voor het presenteren van de risico-analyse is de risicomap (zie figuur hiernaast). De rode kleur geeft aan dat het risico (zowel kans als gevolg) hoog is en groen dat het risico laag is. In de risicomap of –matrix kan ook de risico-acceptatiegrens worden aangegeven. De risico-acceptatiegrens hangt af van de risk appetite (Fout! Verwijzingsbron niet gevonden.). In het figuur hiernaast wordt de risico-acceptatiegrens aangegeven door de dikgedrukte zwarte lijn.

Het resultaat van waarnemen wordt ook wel perceptie genoemd. Net als bij veel andere zaken en situaties is perceptie van risico's in het risicomanagementproces zeer belangrijk. Het proces wordt immers door mensen uitgevoerd.
Voor wat betreft de inschatting van risico's onderscheidt Lizanne Vroom (2014) een aantal stellingen:

- Gevaren worden niet of verkeerd gezien;
- Bij risico's die regelmatig voorkomen, treedt het effect van gewenning op;
- De waarschijnlijkheid van het voordoen van een risico wordt onderschat;

[100] (Roel Grit, 2009, p. 53)
[101] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 126 t/m 128)

- Wanneer men zelf een negatieve gebeurtenis meemaakt, wordt de omvang hoger ingeschat, zeker wanneer men de inschatting kort na de gebeurtenis doet.[102]

Deze stellingen sluiten aan op de theorie van Daniel Kahneman (Bijlage 1.3.2 Risicobeleid), die onder andere zegt dat mensen risico's niet goed kunnen inschatten, omdat men risico's vaak onderschat.

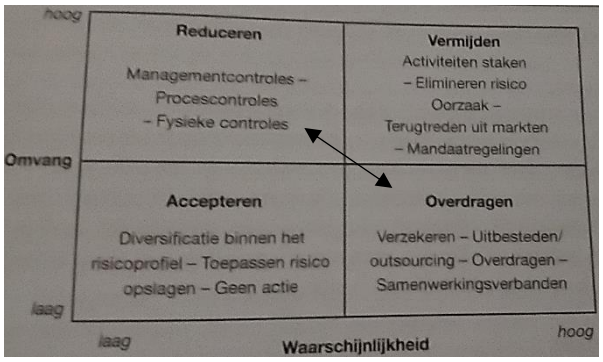
Naast risicoperceptie is ook risicoanalyse zelf onderhevig aan risico's. Grundl en Schulze (2006)[103] onderscheiden drie categorieën:

1. Er kunnen vergissingen worden gemaakt bij het inventariseren van risico's;
2. Het risico van toevalligheid van gegevens en aannames waardoor onzekerheid ontstaat over de betrouwbaarheid van het proces waarmee deze gegevens zijn gegenereerd;
3. Gegevens en aannames zijn geen garantie voor de toekomst.[104]

Risicobeheersing en financiering

Er zijn verschillende manieren (strategieën) om met risico om te gaan:

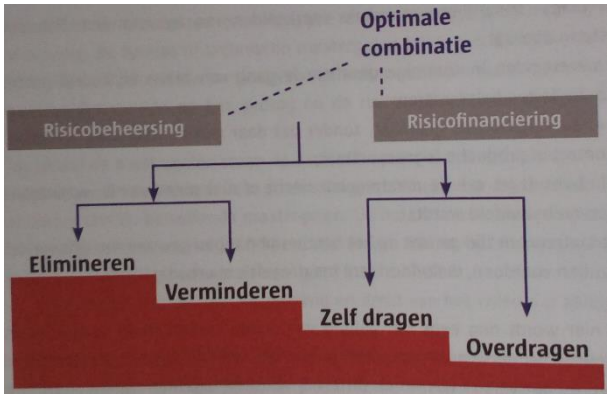
- Maatregelen om risico's te vermijden;
- Maatregelen om risico's te verminderen (beheersen/voorkomen);
- Maatregelen om risico's over te dragen; en
- Het accepteren van risico's.[105]



Figuur 51 Soorten risicostrategieën (Drs. Urjan Claassen RA RE CIA, 2009)

De strategieën worden meestal in deze volgorde opgesomd, dit betekent echter niet dat de afwegingen om risico's te vermijden of te verminderen dan wel zelf te dragen (altijd) in deze volgorde worden gemaakt.

Er kunnen ook onverwachte gebeurtenissen met grote impact plaatsvinden, die (vrijwel) niet zijn in te schatten of te voorspellen. Zo'n gebeurtenis wordt ook wel black swan genoemd, het is dan makkelijker om de impact te bepalen. In deze situaties is het van belang om veerkracht te organiseren.[106]
In dit kader worden ook correctieve maatregelen onderscheiden. Deze maatregelen worden uitgevoerd wanneer het risico zich daadwerkelijk heeft voorgedaan.



Figuur 52 Hoofdstrategieën bij het bedenken van maatregelen (Lizanne Vroom, 2014)

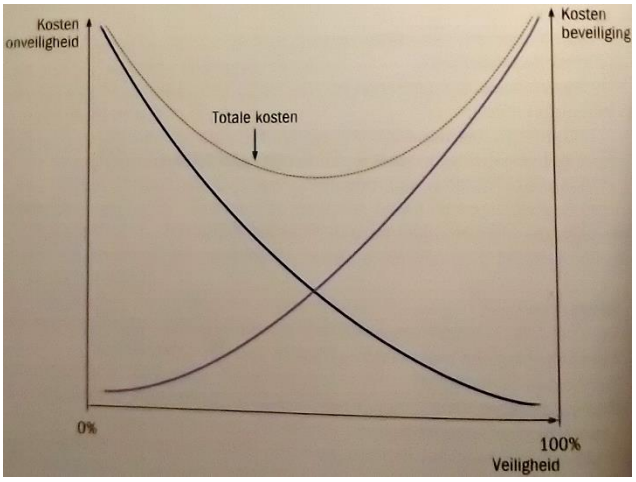
Maatregelen om risico's te vermijden komen voornamelijk voor in situaties waarbij zowel de kans als de omvang significant is. Deze risico's zijn veelal een bedreiging voor de continuïteit van de organisatie. De organisatie kan het risico niet verminderen of vindt dat te duur. Het verminderen van risico's gebeurt bij een lage kans en een hoge impact (focus op vermindering impact) en bij risico's met een hoge kans en een lage impact (focus op vermindering kans). Risico's kunnen ook overgedragen worden, dit vindt veelal plaats wanneer het

[102] (Lizanne Vroom, 2014, p. 140)
[103] In het boek 'Einführung in die Aufgabenbereiche des betrieblichen Risikomanagement' (2006)
[104] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 155)
[105] (Roel Grit, 2009, p. 65 t/m 68)
[106] (Nassim Nicholas Taleb, 2013, p. 2)

risico een hoge kans en een lage impact heeft.[107] Het overdragen van risico kan echter ook gebeuren bij risico's met een lage kans en een hoge impact (verzekeren). Risico's die zowel een kleine kans als een lage impact hebben, worden vaak geaccepteerd.

Bij risico's met een hoge waarschijnlijkheid en een kleine omvang zijn preventieve maatregelen de belangrijkste beheersingsmaatregelen. Door middel van deze maatregelen wordt de kans op het risico verminderd of zelfs uitgesloten. Het is hierbij echter wel van belang om te bedenken dat er ook gebeurtenissen zijn, waarvoor geen preventieve maatregelen getroffen kunnen worden; op deze gebeurtenissen kun je geen invloed uitoefenen (bijvoorbeeld een economische crisis). Bij risico's met een lage waarschijnlijkheid en een grote omvang zijn repressieve maatregelen het belangrijkst. Deze maatregelen zijn gericht op het verminderen van de omvang van het gevolg. In Figuur 51 staan een aantal voorbeelden van zulke maatregelen.

Bij het kiezen van een beheersingsmaatregel moet rekening gehouden worden met de zwaarte (kans en omvang) van het risico, maar ook met de economische afweging. Dit betekent dat de kosten van de maatregelen moeten opwegen tegen de (mogelijke) kostenbesparingen. De beheersingsmaatregel moet dus zowel effectief als efficiënt zijn. Een effectieve maatregel is doeltreffend; het risico wordt verminderd tot een aanvaardbaar niveau. Een efficiënte maatregel maakt op verantwoorde wijze gebruik van de (beschikbare) resources. Bij elke strategie dient een kosten-batenanalyse te worden gemaakt; wegen de kosten van de te nemen maatregel op tegen de verwachte opbrengsten. Uiteindelijk blijft de keuze voor een beheersmaatregel echter voor een groot deel gebaseerd op professionele oordeelsvorming.



Figuur 53 Relatie tussen kosten en veiligheid (Sonja Janicijevic et. al, 2016)

Bij het nemen van beheersingsmaatregelen moet het restrisico bepaald worden. Dit gebeurt nadat de beheersingsmaatregelen gedefinieerd zijn. Het risico moet door de beheersingsmaatregelen teruggebracht naar een aanvaardbaar niveau. Hierbij komt ook de risicohouding van de organisatie om de hoek kijken. Welke risico's vallen binnen de risicohouding en kunnen dus geaccepteerd worden en voor welke risico's moeten er beheersingsmaatregelen worden genomen.

Het vermijden van risico's
Het vermijden van risico's is een drastische methode om met risico's om te gaan. Lizanne Vroom (2014) onderscheidt in hoofdzaak twee manieren om risico's te vermijden:

1. Risico's worden vermeden door het afstoten van activiteiten; en
2. Risico's worden vermeden door het veranderen van de activiteiten.[108]

Bij de tweede optie kan gedacht worden verandering in de aard van de activiteiten en de verandering van de plaats van handeling. Aangezien deze risico's vaak de continuïteit van de organisatie bedreigen, is het belangrijk om altijd de kosten tegenover de baten te zetten. Welke mogelijke schade wil een organisatie vermijden en weegt dit op tegen de (mogelijk) gederfde inkomsten.[109]

[107] (Drs. Urjan Claassen RA RE CIA, 2009, p. 120)
[108] (Lizanne Vroom, 2014, p. 217)
[109] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 169 t/m 171)

Het verminderen van risico's
Het verminderen van risico's kan op twee manieren gebeuren. Enerzijds kan gedacht worden aan het verminderen van de kans op risico en anderzijds aan het beperken van het gevolg van risico.

Bij het verminderen van risico wordt door Lizanne Vroom (2014) een fysiek en een psychologisch aspect onderscheiden. Bij het fysieke aspect worden alle materiële (technische) en organisatorische maatregelen onderscheiden die gericht zijn op het voorkomen en verminderen van schade. Voorbeelden van organisatorische maatregelen zijn procedures, instructies en afspraken omtrent de activiteiten die door de medewerkers worden uitgevoerd. Bij materiële (technische) maatregelen kan men denken aan blusmiddelen, camera's etc. Wat betreft het psychologische aspect moet worden gedacht aan het risicobewustzijn van medewerkers in de organisatie; medewerkers moeten participeren in het proces van het voorkomen en verminderen van schade. Deze maatregelen zijn bijvoorbeeld voorlichting, opleiding en training, waardoor medewerkers zelf een actievere rol kunnen spelen bij de beheersing van risico's.[110]

Het is hierbij belangrijk om te beseffen dat zowel de kans als de impact van een ongewenste gebeurtenis nooit helemaal terug te brengen is naar 'nul'. Daarnaast moet er gekeken worden naar de realiteitszin van deze maatregelen, als de preventie en beheersing zo ver wordt doorgevoerd dat medewerkers zich erdoor gehinderd voelen, gaan deze maatregelen hun doel voorbij.[111]

Figuur 54 De benadering van risico afgezet tegen de prestatie van risicobeheersing (Lizanne Vroom, 2014)

Net zoals bij de juiste afstemming tussen hard en soft controls gaat het hierbij ook om de juiste afstemming tussen psychologische maatregelen en fysieke maatregelen. Organisaties hebben nogal eens de neiging om alleen te investeren in fysieke maatregelen. Maar zonder psychologische maatregelen hebben fysieke maatregelen weinig effect.[112]

Het overdragen van risico's
Lizanne Vroom (2014) onderscheidt met betrekking tot de risico-overdracht activiteiten die in drie categorieën verdeeld kunnen worden:
- Risicovolle werkzaamheden en verantwoordelijkheden worden overgedragen;
- Verantwoordelijkheden voor bepaalde activiteiten en de bijbehorende mogelijke gevolgen worden overgedragen; en
- De financiële gevolgen worden overgedragen door verzekeringen.[113]

Bij de overdracht van risicovolle werkzaamheden en verantwoordelijkheden onderscheiden Sonja Janicijevic et. al. (2016) vier vormen: outsourcing, leasing, (publiek-private) samenwerking en factoring. Bij de overdracht van verantwoordelijkheden voor bepaalde activiteiten en de bijbehorende mogelijk gevolgen onderscheiden Sonja Janicijevic et. al. (2016) twee vormen: contractuele overdracht en aanvaarding van risico's, bijvoorbeeld door leveringsvoorwaarden, het exoneratiebeding en het vrijwaringsbeding en gebruiksaanwijzingen en garantiebepalingen.[114]

[110] (Lizanne Vroom, 2014, pp. 213, 218)
[111] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 161 t/m 164)
[112] (Lizanne Vroom, 2014, p. 218)
[113] (Lizanne Vroom, 2014, p. 219)
[114] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 216)

Het accepteren van risico's
Het accepteren van risico's geeft aan dat de organisatie de risico's voor eigen rekening neemt en geen verdere actie onderneemt, dit gebeurt grotendeels bij risico's met een lage impact en een lage kans.[115] Het kan echter ook voorkomen dat een organisatie het risico moet dragen omdat een risico niet te verzekeren is. Bij de vraag wat de organisatie zelf kan dragen en wat (gedeeltelijk) verzekerd moet worden onderscheiden Sonja Janicijevic et. al. (2016) een aantal basisvragen:

- Wat is de aard van de risico's en wat zijn de verwachte gevolgen?
- Wat kan en wil de organisatie zelf dragen?
- Welke methoden om risico te dragen zijn het voordeligst?
- Op welke wijze zijn binnen de organisatie de risico's gespreid?[116]

Globaal kan men aanhouden dat schaden die zich frequent voordoen (voorspelbaar) zelf te dragen of over te dragen en zeer grote schaden, die minder vaak voorkomen, altijd te verzekeren.[117]

In aansluiting op het accepteren van risico's kan ook het organiseren van veerkracht onderscheiden worden, zoals eerder gezegd in deze paragraaf. In dit kader wordt de laatste jaren aandacht geschonken aan Resilience Risk Management. Het risicomanagement richt zich dan niet alleen op het voorkomen en beheersen van risico's, maar ook op een aanpak om risico's te voorzien en maatregelen die kenmerken van een systeem herstellen (correctieve maatregelen). [118] Denk hierbij aan de vijf principes 'high reliable organizations' (Bijlage 1.3.3 Risicomanagementproces). Risico's zijn immers nooit volledig uit te sluiten en dit is praktisch ook niet haalbaar. Het organiseren van veerkracht heeft alles te maken met risk readiness zoals beschreven in Bijlage 1.3.2 Risicobeleid, maar ook met het lerend vermogen (Bijlage 1.3.3 Risicomanagementproces); het voortdurend leren van fouten en het geleerde vervolgens ook kunnen toepassen.

In aansluiting op de theorie van de black swan spreken Weick en Sutcliffe van het managen van het onverwachte, anticipatie speelt hierbij een belangrijke rol. Volgens Weick en Sutcliffe (2011) gaat het bij veerkracht om drie capaciteiten:

1. De capaciteit om spanning te absorberen en toch te kunnen blijven functioneren ondanks het voordoen van gebeurtenissen die niet te voorkomen of te beheersen zijn;
2. De capaciteit om te herstellen en/of terug te keren vanuit een ongewenste positie naar de oorspronkelijke positie;
1. De capaciteit om te leren en groeien van eerdere ervaringen en het geleerde in het praktijk te kunnen brengen om zo veerkrachtig te kunnen handelen.[119]

Evaluatie en bijsturing

Monitoring kan in de eerste plaats gebeuren door de interne auditfunctie en de externe auditfunctie. Een andere mogelijkheid is het betrekken van het tactisch en strategisch management bij het monitoren van de effectiviteit van beheersingsmaatregelen. De auditfunctie is dan niet meer gericht op het testen van de effectiviteit van de beheersingsmaatregelen, maar op het waarborgen van de betrouwbaarheid van interne rapportages omtrent de effectiviteit van de beheersingsmaatregelen. Om tot een effectieve risicogerichte aanpak te komen is het gebruik van een risicobeheersingsmatrix aanbevolen (tabel volgende bladzijde).[120]

[115] (Drs. Urjan Claassen RA RE CIA, 2009, p. 120)
[116] (Sonja Janicijevic, Paul Claes, Rob Lengkeek, 2016, p. 276)
[117] (Lizanne Vroom, 2014, p. 220)
[118] (Lizanne Vroom, 2014, p. 221 t/m 223)
[119] (Karl E. Weick, Kathleen M. Sutcliffe, 2011, p. 76)
[120] (Drs. Urjan Claassen RA RE CIA, 2009, p. 178 t/m 180)

Tabel 14 Risicobeheersingsmatrix (Drs. Urjan Claassen RA RE CIA, 2009)

		Risico	Risico 1	Risico 2
		Soort risico	Financieel	Operationeel
		Risicoclassificatie	Hoog	Gemiddeld
Beheersingskader	**Niveau**	**Subtype**		
Beheersingsmaatregel 1	Management	Taakbeheersing	X	X
Beheersingsmaatregel 2	Proces	Handmatig		X
Beheersingsmaatregel 3	Proces	Applicatie	X	
Beheersingsmaatregel 3	Proces	Handmatig	X	X
Beheersingsmaatregel 3	Proces	Applicatie		X
Effectiviteit ontwerpbeheersing			Hoog	Laag
Classificatie restrisico			Laag	Gemiddeld

Om de werking van de beheersingsmaatregelen te meten moet een bepaalde norm of referentiepunt worden opgesteld, de voorkeur gaat hierbij uit naar de risicodoelstellingen als norm of referentiepunt.[121] Zoals gezegd is het dan van belang om bepaalde prestatie-indicatoren aan deze doelstellingen te koppelen, zodat de werking van de maatregel vergeleken kan worden met de norm. Dit sluit aan op de traditionele opvatting van 'control', wat gebaseerd is op de cybernetica: het is een proces van meten, vergelijken en bijsturen.[122] Om maatregelen te evalueren moet de impact van de beheersingsmaatregel dus gemeten worden, vergeleken worden met een norm of referentiepunt en wanneer de meting niet voldoet aan de norm, moet er bijgestuurd worden.

De evaluatie van beheersingsmaatregelen kan gebeuren door middel van zich herhalende metingen of afzonderlijke evaluaties. Repeterende metingen kunnen plaatsvinden door middel van KPI's, rapportages en dergelijke. Als de waarde van een KPI zich buiten de bandbreedte (risicotolerantie) begeeft, moet er worden ingegrepen. Afzonderlijke evaluaties worden toegepast op activiteiten waarbij er niet doorlopend gemeten kan worden en/of wanneer de effectiviteit van de beoordeling van doorlopende metingen moet worden beoordeeld.[123] Het is tevens van belang om aan een evaluatie een testmoment te koppelen, eens per jaar of vaker.[124] Het restrisico wordt nogmaals bepaald en gekeken of deze binnen de risicohouding valt.

Voordat men de assessment van de maatregelen uitvoert, moet eerst gekeken worden of de beheersingsmaatregelen wel daadwerkelijk zijn doorgevoerd; het heeft anders weinig zin om een assessment uit te voeren. Voor het assessment zelf onderscheidt Rob Uiterlinden (2009) verschillende methoden om een assessment uit te voeren:

- Herhaling: door een beheersingsmaatregel zelf uit te voeren en het resultaat te vergelijken met het eerder 'behaalde' resultaat kan er een oordeel worden gevormd omtrent de effectiviteit;
- Inspectie: de maatregel wordt gecontroleerd door documentatie te controleren, bij voorkeur uit verschillende bronnen. Een voorbeeld is de monitoring en bewaking van een KPI;
- Observatie: hiermee wordt waarneming ter plaatse bedoeld;
- Interview: door middel van gesprekken met degene die de maatregel uitvoert kan de effectiviteit worden vastgesteld;
- Proces doorlopen: door het hele proces te doorlopen wordt vastgesteld of de maatregelen correct worden uitgevoerd;

[121] (Lizanne Vroom, 2014, p. 281)
[122] (Prof. dr. E.H.J. Vaassen RA, Dr. L.H.H. Bollen, Prof. dr. R.H.H. Meuwissen RA, Dr. M.P.M. Vluggen, Prof. dr. F.G.H. Hartman RC, 2012, p. 243)
[123] (Rob Uiterlinden RC, 2009, pp. 92, 93)
[124] (Lizanne Vroom, 2014, p. 281)

- Systeemonderzoek: door informatie uit databases te analyseren, kunnen verbanden worden gelegd waardoor er kan worden vastgesteld of bepaalde maatregelen goed werken.[125]

Ook binnen dit proces is het van belang om functiescheiding aan te brengen. Zo moet er functiescheiding zijn tussen het opstellen van beheersingsmaatregelen, de uitvoering van de beheersingsmaatregelen en controle en bijsturing ervan.

Naast het evalueren van het de risicobeheersingsmaatregelen kan het risicomanagement als functie ook geëvalueerd worden. Dit kan dan gebeuren in opzet en werking, waarbij gekeken wordt naar het risicomanagement(systeem) als geheel, de processen (stappen binnen het systeem) en de inhoud (kwaliteit van risico-informatie en prestaties).[126] Dit sluit deels aan bij de uitvoering van een audit, waarbij in een interim controle de opzet, het bestaan en werking (van key controls) worden getest.

Continu verbeteren

Verbetering kan op elk onderdeel van risicomanagement gebeuren. Om het risicomanagement (of een onderdeel) te verbeteren moeten allereerst ambities worden geformuleerd. In relatie met deze ambities moet ook inzicht worden verkregen in het huidige niveau (Bijlage 6 Verschillende niveaus van risicomanagement) van risicomanagement. Door de ambities te vergelijken met het huidige niveau kan worden bepaald waar er verbeteringen kunnen (moeten) worden doorgevoerd. Nadat deze vergelijking is uitgevoerd, is het nodig dat er ook daadwerkelijk maatregelen worden genomen. Toch kan op langere termijn de aandacht verslappen. Om dit te voorkomen wordt door Drs. Urjan Claassen RA RE CIA (2009) drie hulpmiddelen onderscheiden:

1. Benchmarking: periodiek moet het risicomanagement vergeleken worden met concurrenten. Deze vergelijking kan als input dienen voor de verdere verbetering van het risicomanagement;
2. Kennisdeling: het delen van 'best practices' en kennis binnen de organisatie;
3. Opleiding en training: het opleiden van betrokkenen draagt bij aan het draagvlak en kennis van risicomanagement binnen de organisatie.[127]

Een manier om kennisdeling te stimuleren is het opzetten van communities door het management en deze te integreren in de organisatie. Deze kennisdeling leidt tevens tot nieuwe benaderingen van problemen.[128]

Het begrip leren speelt bij continu verbeteren een belangrijke rol. M. Ruijters (2011) onderscheidt vier vormen van leren:

1. Intellectueel leren: dit gebeurt vooral in het onderwijs;
2. Informeel leren: het leren door ervaringen die je overkomen;
3. Imaginair leren: leren door situaties aan te voelen en voor te stellen; en
4. Intuïtief leren: leren door op een andere manier tegen een vraagstuk aan te kijken.[129]

Werkend leren is een combinatie van deze factoren.[130] Het is tevens een belangrijke basis voor risk readiness (Bijlage 1.3.2 Risicobeleid), zowel voor het organiserend als het interventievermogen.

Weick en Sutcliffe (2011) hebben organisaties onderzocht die goed willen presteren bij catastrofale gebeurtenissen. Op basis van dit onderzoek zijn een aantal principes naar voren gekomen die worden onderscheiden bij zeer betrouwbare organisaties (high reliabele organizations):

[125] (Rob Uiterlinden RC, 2009, p. 93 t/m 98)
[126] (Lizanne Vroom, 2014, pp. 286, 287)
[127] (Drs. Urjan Claassen RA RE CIA, 2009, p. 212 t/m 217)
[128] (Etienne C. Wenger en William M. Snyder, 2002, p. 1)
[129] (Manon C.P. Ruijters, 2011, p. 25 t/m 27)
[130] (Thinka Bor-Reijinga en Gert van der Kolk, 2014, p. 58)

- Gericht op verstoringen;
- Terughoudend bij vereenvoudiging;
- Aandacht voor de uitvoering;
- Het creëren van veerkracht (Bijlage 1.3.3 Risicomanagementproces); en
- Het respecteren van expertise.[131]

In het kader van continu verbeteren kunnen organisaties streven om deze vijf principes toe te passen in hun organisatie. Ondanks dat deze principes gericht zijn op catastrofale situaties, kunnen deze principes bijvoorbeeld ook worden meegenomen bij het beoordelen van risico's en het nemen van maatregelen.[132]

Verantwoording

Als men naar de verantwoording over risicomanagement kijkt, komt men uit bij het bestuursverslag. In de huidige richtlijn 650 verwijst men naar RJ 400. In de nieuwe richtlijn 650 staat RJ 400 alinea 110 opgenomen in alinea 406 van RJ 650. Alinea 111 van RJ 400 over financiële instrumenten is opgenomen in alinea 408 van de nieuwe RJ 650. RJ 400 is dus in de nieuwe RJ 650 opgenomen en wijkt niet af van de vereisten zoals die zijn vermeld in RJ 400. Bovendien is het zo dat als men één hoofdstuk van de Raad van de Jaarverslaggeving toepast, dat alle hoofdstukken toegepast moeten worden.

RJ 400 volgt hierin het Burgerlijk Wetboek, waarin wordt aangegeven dat het bestuursverslag "tevens een beschrijving van de voornaamste risico's en onzekerheden waarmee de rechtspersoon wordt geconfronteerd"[133] (art. 3:391 BW lid 1) moet geven.

RJ 400 (2014) zegt over deze beschrijving het volgende, de rechtspersoon moet:

- bij de identificatie van de voornaamste risico's en onzekerheden de categorieën, strategie, operationele activiteiten, financiële risico's, financiële verslaggeving en wet-en-regelgeving onderscheiden;
- de risicobereidheid (op hoofdlijnen) toelichten;
- een beschrijving geven van de genomen beheersingsmaatregelen en als dit voor één of meer van de belangrijkste risico's niet is gebeurd, moet dit worden toegelicht;
- een beschrijving geven van de verwachte gevolgen op de resultaten/financiële positie als één of meerdere van deze risico's zich voordoet;
- de risico's en de gevolgen ervan die zich het afgelopen boekjaar hebben voorgedaan, benoemen en wanneer zich deze risico's hebben voorgedaan, of, en zo ja welke verbeteringen er zijn doorgevoerd;
- bij voorkeur aangeven hoe het risicomanagement(systeem) is verankerd in de organisatie en de maatregelen die de organisatie heeft genomen ter beïnvloed van de cultuur, het gedrag en de motivatie van haar medewerkers; en
- ten aanzien van het gebruik van financiële instrumenten, het beleid inzake risicobeheer (inclusief afdekking van risico's) vermelden, voor zover dat van belang is voor de beoordeling van de activa, passiva, financiële toestand en resultaat.[134]

Bijlage 1.3.4 Randvoorwaarden

Voor het goed verlopen van het risicomanagementproces is er in principe één randvoorwaarde benodigd: de infrastructuur. Infrastructuur is een containerbegrip en kan onderverdeeld worden in een aantal onderdelen. Men kan hierbij denken aan informatie, communicatie, mensen, middelen

[131] (Karl E. Weick, Kathleen M. Sutcliffe, 2011, p. 9 t/m 19)
[132] (Lizanne Vroom, 2014, p. 210)
[133] (Mw. mr. A.M.M.M. van Zeijl, Mr. J. Keizer, Mr. J.M.K. Burger e.a., 2016, p. 517)
[134] (Raad voor de Jaarverslaggeving, 2014, pp. 3, 4)

(hard- en software, procedures etc.) en toezicht. Mensen en middelen worden hier verder niet behandeld, vanwege de verscheidenheid van mensen en middelen. Het is daarom niet praktisch om nader in te gaan op de mens en middelen als onderdelen van de infrastructuur.

Informatie

Informatie is dus niet zozeer een stap in het risicomanagementproces, maar meer een randvoorwaarde om het risicomanagement in een organisatie goed te laten functioneren. Informatie dient op alle niveaus binnen een organisatie beschikbaar te zijn, zowel op operationeel, tactisch als strategisch niveau. Informatie is nodig om elke stap in het risicomanagementproces uit te kunnen voeren, door middel van communicatie (volgende paragraaf) kan informatie van de ene persoon naar de andere persoon gebracht worden binnen de stappen van het risicomanagementproces (Figuur 57).

Informatie kan zowel vanuit binnen de organisatie als buiten de organisatie komen, de belangrijkste informatie is van operationele en/of financiële aard. De planning- en controlcyclus heeft niet alleen financiële gegevens, maar ook niet-financiële gegevens nodig, vaak weergegeven door middel van KSF's en KPI's.[135] Welke informatie een organisatie nodig heeft wordt bepaald door een gebruiker binnen de organisatie zelf, deze behoefte vormt de input voor een informatiesysteem.

Vanuit deze informatiebehoefte is er infrastructuur benodigd om informatie te verzamelen, op te slaan, te verwerken en beschikbaar te stellen. Dit gebeurt door middel van een informatiesysteem, wat zowel interne als externe informatie kan verwerken. Om een (geautomatiseerd) systeem te laten werken onderscheiden Prof. Dr. Eddy Vaassen RA et. al. (2012) vijf onderdelen die benodigd zijn: hardware, software, gegevens, netwerken en mensen en procedures.[136]

Door het gebruik van informatiesystemen ontstaan zelf echter ook weer risico's, bijvoorbeeld op het gebied van informatiebeveiliging en computercriminaliteit. Het beheersen van deze risico's moet vanzelfsprekend onderdeel zijn van het risicomanagement van een organisatie.

Om het risicomanagementproces effectief uit te kunnen voeren moet informatie zowel efficiënt als effectief zijn. Effectiviteit kan zelf worden onderverdeeld in relevantie en betrouwbaarheid. Betrouwbare informatie is informatie die overeenstemt met de werkelijkheid, relevantie informatie is informatie die het besluitvormingsproces, het proces van delegatie en het afleggen van verantwoording of het functioneren van de organisatie positief beïnvloedt.[137] Betrouwbare informatie moet volledig, accuraat en juist zijn, relevante informatie moet nauwkeurig, tijdig en begrijpelijk zijn.

Communicatie

Communicatie is een randvoorwaarde voor het risicomanagementproces. Zonder het doorgeven van informatie, in welke richting dan ook, komt het risicomanagement niet van de grond en kunnen de stappen van het risicomanagementproces niet doorlopen worden. Het is hierbij belangrijk te bedenken dat het geen starre cyclus is, de uitvoering van

Figuur 55 Gewenste onderdelen van communicatie (Lizanne Vroom, 2014)

[135] (Rob Uiterlinden RC, 2009, pp. 88, 89)
[136] (Prof. dr. E.H.J. Vaassen RA, Dr. L.H.H. Bollen, Prof. dr. R.H.H. Meuwissen RA, Dr. M.P.M. Vluggen, Prof. dr. F.G.H. Hartman RC, 2012, p. 165)
[137] (Drs. Urjan Claassen RA RE CIA, 2009, pp. 192, 193)

een fase kan ook informatie nodig hebben van mensen die de volgende fase uitvoeren of zelfs over meerdere fasen heen gezien; het risicomanagementproces is een dynamisch proces (Figuur 57).

T. Bor-Reijinga en G. van der Kolk (2014) onderscheiden vier niveaus van communicatie: inhoud, procedure, interactie en gevoel. Er wordt vrijwel altijd gecommuniceerd over inhoud en procedures. Het gevaar van routine en versimpeling liggen echter hierbij op de loer. Deze gevaren spelen zich af op het niveau van interactie en gevoel, deze gevaren worden echter vrijwel nooit aan de orde gesteld. Om problemen en risico's in kaart te brengen is het belangrijk dit patroon te doorbreken.[138]

Een voorbeeld van belangrijke communicatie over het risicomanagement, is de communicatie van de risicomanagementvisie en - filosofie en een duidelijke verdeling van rollen en verantwoordelijkheden (Bijlage 1.3.2 Risicobeleid). Naast interne communicatie, bijvoorbeeld tussen werknemers, is er ook sprake van externe communicatie, bijvoorbeeld naar klanten, leveranciers, overheid en de maatschappij.[139] In dit kader spreekt Lizanne Vroom (2014) over een stakeholdersanalyse, waarbij de invloed en de houding van de stakeholders ten opzichte van de organisatie wordt onderzocht, op basis van dit onderzoek kunnen dan verschillende communicatiestrategieën voor de desbetreffende stakeholders worden ontwikkeld.[140]

Toezicht

Toezicht en evaluatie en bijsturing (Bijlage 1.3.3 Risicomanagementproces) houden veel verband met elkaar. De evaluatie en bijsturing is echter een stap in het risicomanagementproces, waarbij het meer gaat om de werkzaamheden die moeten worden uitgevoerd. Het toezicht gaat meer over het 'hoe' en de structuur van de evaluatie en bijsturing en is derhalve aangemerkt als een randvoorwaarde.

Toezicht op de werking van de interne beheersing op het operationeel en managementniveau is erop gericht om de doelstellingen te behalen. COSO ERM (2009) onderscheidt een drietal elementen voor effectief toezicht:

1. Het vaststellen van een basis voor monitoring met een:
    a. Een goede 'tone at the top';
    b. Een effectieve organisatiestructuur die verschillende rollen toewijst aan mensen met de vereiste vaardigheden, objectiviteit en gezag; en
    c. Een startpunt van een bekende, effectieve interne beheersing waaruit monitoring en evaluaties kunnen worden uitgevoerd;
2. Het ontwerpen en uitvoeren van monitoringprocedures, die gericht zijn op de importantie van informatie over de werking van key-controls die belangrijke risico's afdekken; en
3. Het beoordelen en rapporteren van resultaten, waaronder het evalueren van de ernst van de geconstateerde tekortkomingen en het rapporteren van de monitoring resultaten aan het juiste personeel en het bestuur voor tijdige acties en follow-ups, wanneer nodig.[141]

Fondsenwervende organisaties hebben veelal een bestuur als uitvoerend orgaan en een raad van toezicht of een raad van commissarissen als toezichthoudend orgaan. Het is ook mogelijk dat er een directeur is die de dagelijkse leiding op zich neemt en dat het bestuur een toezichthoudende rol vervult. Binnen het toezichthoudend orgaan kan er ook sprake zijn van een audit commissie, die zich met name richt op de financiën en onder andere op risicomanagement.
Toch is een toezichthoudend orgaan voor verenigingen en stichtingen (nog) niet verplicht; momenteel is een wetsvoorstel (Wet bestuur toezicht rechtspersonen) in behandeling die dit verplicht wil gaan maken.

[138] (Thinka Bor-Reijinga en Gert van der Kolk, 2014, p. 42 t/m 44)
[139] (Rob Uiterlinden RC, 2009, p. 90)
[140] (Lizanne Vroom, 2014, p. 318)
[141] (Committee of Sponsoring Organizations of the Treadway Commission, 2009, pp. 2, 3)

Er zijn wel (gedrags)codes beschikbaar die het toezicht voor fondsenwervende instellingen regelen. Denk bijvoorbeeld aan de Code Wijffels en de code van Goed Bestuur SBF. Ze geven echter geen uitgebreide omschrijvingen van de verantwoordelijkheden van het toezichthoudend orgaan en het bestuur. De Code Wijffels[142] als de code van Goed Bestuur SBF zeggen dat degene die de fondsenwervende instelling bestuurt, verantwoordelijk is voor het functioneren van de organisatie en een adequate beheersing van risico's. Het toezichthoudend orgaan volgt het signaleren en beheersen van risico's.[143]

Bij toezicht kan niet alleen interne governance (toezichthoudend orgaan) worden onderscheiden, maar ook externe governance, bijvoorbeeld de accountants. De accountant speelt een rol bij het risicomanagement van hun klanten: via de controle van de jaarrekening (inclusief risicoanalyse), het uitvoeren van de aanwezigheid- en consistentietoets op het jaarverslag (en het gebruiken van controle-informatie) en eventueel via de managementletter.[144]
Uit onderzoek is gebleken dat externe governance, een positieve werking heeft op het risicomanagement bij hun klanten.[145]

[142] (Commissie Goed Bestuur voor Goede Doelen, 2005, p. 15)
[143] (SBF - Samenwerkende brancheorganisaties filantropie, 2015, pp. 11, 12)
[144] (Nederlandse Beroepsorganisatie van Accountants, 2013, p. 7)
[145] (Nederlandse Beroepsorganisatie van Accountants (NBA), Nyenrode Business Universiteit, Rijksuniversiteit Groningen, PwC, 2014)

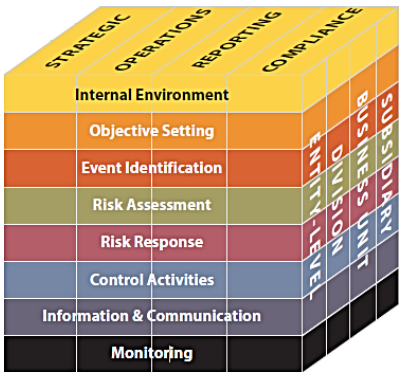
Bijlage 2 Risicomanagementmodellen

Volgens het onderzoek 'Hoeveel zijn we opgeschoten na de crisis?' uitgevoerd door de NBA, Nyenrode Business Universiteit, de rijksuniversiteit Groningen en PWC, gebruikt in 2014 ongeveer 51% van de non-profitsector nog geen standaard voor het inrichten van risicomanagement en interne beheersing. Hoewel er geen garantie bestaat dat gebruik van een standaard noodzakelijk is, is een model wel behulpzaam als referentie. Bij organisaties die wel een model gebruiken is volgens hetzelfde rapport COSO het meest gebruikte model, gevolgd door het INK/EFQM model en de ISO 31000-richtlijn. Deze modellen worden daarom hieronder behandeld.

Bijlage 2.1 COSO ERM-model

COSO (2004) stelt dat ERM gericht is op het realiseren van organisatiedoelstellingen. De organisatiedoelstellingen worden verdeeld in vier soorten:

1. Strategisch: de doelen op strategisch niveau die zijn afgestemd op die missie;
2. Operationeel: het effectief en efficiënt gebruik van de hulpmiddelen;
3. Rapportage: de betrouwbaarheid van de rapportage;
4. Toezicht: naleving van de relevante wetten en regels.



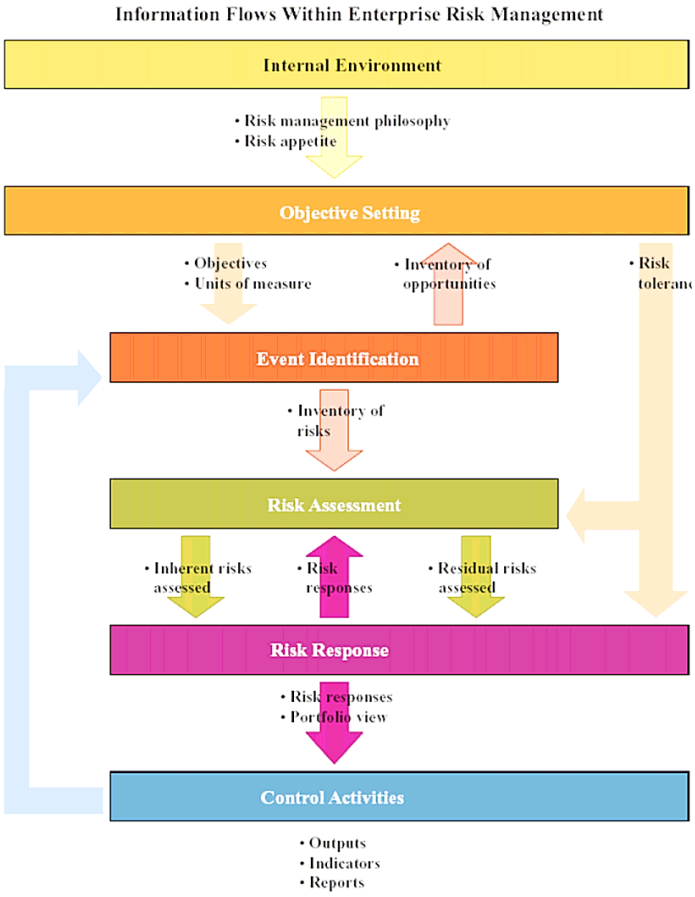
Figuur 56 Enterprise Risk Management Framework (COSO ERM, 2004)

Door de doelstellingen te categoriseren wordt het mogelijk om op de afzonderlijke onderdelen van risicomanagement te focussen. Deze onderscheidende maar overlappende categorieën, een bepaalde doelstelling kan in meerdere categorieën vallen, spreken verschillende behoeften van de organisatie aan en kunnen de directe verantwoordelijkheid van verschillende leidinggevenden zijn. Ook zorgt deze verdeling ervoor wat verwacht kan worden van elke categorie doelstellingen. Omdat de doelstellingen in verband met de betrouwbaarheid van de rapportage en naleving van wetten en regels binnen de macht van de organisatie ligt, kan van risicomanagement worden verwacht dat het redelijke zekerheid verschaft bij het bereiken van deze doelstellingen. Strategische en operationele doelstellingen liggen echter niet altijd binnen de macht van de organisatie. Voor deze doelstellingen voorziet het risicomanagement in redelijke zekerheid dat de directie en het bestuur in toezichthoudende rol, tijdig bekend zijn van de mate waarin de organisatie die doelstellingen bereikt.

Risicomanagement bestaat uit acht gerelateerde componenten. Deze zijn afgeleid van de manier hoe de directie een organisatie leidt en geïntegreerd is in het management proces. De acht onderdelen zijn:

1. Interne omgeving: de interne omgeving zet de toon van een organisatie en stelt de basis voor hoe risico's worden bekeken en behandeld door de mensen van de organisatie, inclusief het risicomanagementbeleid en risicobereidheid, integriteit en ethische waarden en de omgeving waarin ze opereren;
2. Formulering van doelstellingen: doelstellingen moeten bestaan voordat het management mogelijke gebeurtenissen kan identificeren die het bereiken van de doelstellingen kan beïnvloeden. Risicomanagement verzekert dat management een plaats in het proces heeft om doelstellingen te formuleren en dat de gekozen doelstellingen in overeenstemming zijn met de missie van de organisatie en consistent zijn met haar risicobereidheid;
3. Identificatie gebeurtenissen: interne en externe gebeurtenissen die het bereiken van de doelstellingen van een organisatie beïnvloeden moeten worden geïdentificeerd en onderscheiden worden naar risico's en kansen. Kansen worden teruggekoppeld aan de strategie of het proces van het formuleren van doelstellingen;

4. Risicobeoordeling: risico's worden geanalyseerd, rekening houdend met de waarschijnlijkheid en impact, als een basis voor het vaststellen hoe ze moeten worden behandeld. Risico's worden beoordeeld op een inherente en overgebleven risico's;
5. Reactie op risico: het management kiest een reactie op een risico: vermijden, accepteren, verminderen of het delen (overdragen) van risico's. Hierbij wordt een aantal acties ontwikkeld om risico's af te stemmen op de risicotolerantie en risicobereidheid;
6. Beheersingsactiviteiten: richtlijnen en procedures wordt vastgesteld en ingevoerd om te verzekeren dat de reacties op risico's effectief worden uitgevoerd;
7. Informatie en communicatie: relevante informatie wordt geïdentificeerd, verzameld en gecommuniceerd in een vorm en tijdsbestek dat mensen in staat stelt hun verantwoordelijkheden uit te voeren. Effectieve communicatie gebeurt ook in een breder geheel, top-down, bottom-up en peer-to-peer;
8. Monitoring: het geheel van het risicomanagement wordt gemonitord en waar nodig worden veranderingen aangebracht. Monitoring wordt bereikt door voortdurende managementactiviteiten, afzonderlijke evaluaties of beide.[146]



Figuur 57 Informatiestromen binnen risicomanagement (B.J. Reijntjes, 2007)

De stappen drie tot en met vijf vormen het hart van het risicomanagement. Hier speelt de methodiek van risicomanagement zich af. Deze methodiek bestaat uit drie stappen, die achter elkaar moeten worden uitgevoerd:

1. Bedrijfsprocessen per doelstelling vaststellen;
2. Per bedrijfsproces events benoemen;
3. De risk response vaststellen.

Bij stap twee wordt (vaak) een risicomatrix gebruikt, met daarin de impact, de kans en de vereiste maatregelen (risk responses). Op basis van deze matrix kan een organisatie bepalen welke risico's men belangrijk vindt om te beheersen. Deze belangrijkste risico's worden eigenlijk bepaald door de risk appetite. Voor de belangrijkste risico's wordt de risk response vastgesteld: beheersen, vermijden, accepteren en overdragen (delen). Beheersingsmaatregelen kan men indelen in:

- Preventieve maatregelen: maatregelen om risico's te voorkomen;
- Repressieve maatregelen: maatregelen om gevolgen vast te stellen; en

[146] (Committee of Sponsoring Organisations of the Treadway Commission, 2004, p. 9 en 10)

- Correctieve maatregelen: maatregelen om vastgestelde afwijkingen herstellen.[147]

Risicomanagement is niet een proces waar de ene component de volgende component beïnvloedt, maar een iteratief proces waarin bijna elk onderdeel een ander onderdeel kan beïnvloeden.

Vervolgens kan dit worden toegepast op vier niveaus:

4. Subsidiary: een dochteronderneming;
5. Business unit: een groep bedrijven binnen de divisie die zich bezighoudt met dezelfde soort producten;
6. Division: het totaal van bedrijfsonderdelen die tot een bepaalde divisie behoren;
7. Entity level: de organisatie als geheel.[148]

Sterke punten van de COSO-aanpak is dat het een internationaal geaccepteerde standaard is, die wereldwijd veel gebruikt wordt. In Nederland wordt deze aanpak met name door beursgenoteerde ondernemingen gebruikt. In verschillende corporate governance codes (Sarbanes Oxley en Tabaksblat) wordt naar deze aanpak verwezen, waardoor deze ook door accountants wordt geaccepteerd.[149]

In 2013 is het COSO framework geüpdatet. De grootste verandering die doorgevoerd is, is het opnemen van de zeventien principes die de vijf componenten van de kubus (Figuur 56) ondersteunen. Zowel de vijf componenten als de zeventien principes (afkomstig uit het framework van 1992) moeten bestaan en functioneren voor effectieve controls en de vijf componenten moeten samenwerken op een geïntegreerde manier.[150]

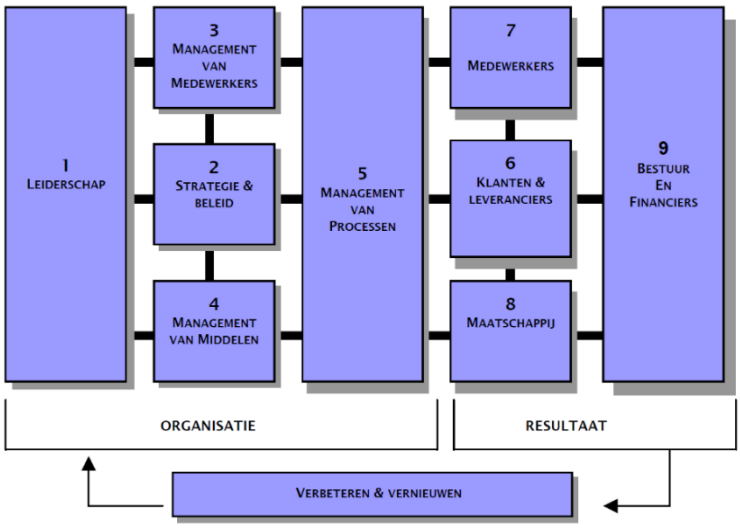
[147] (M. Paur, 2014, pp. 85, 86)
[148] (B.J. Reijntjes, 2007, p. 20)
[149] (Focus op verbeteren, 2015, p. 16)
[150] (KPMG, 2013)

Bijlage 2.2 INK model

Een voorloper van het INK-managementmodel is rond 1990 ontwikkeld door de European Foundation for Quality Management (EFQM).[151] In Nederland is dit model verder ontwikkeld door het Instituut Nederlandse Kwaliteit. Het INK model laat de relatie zien tussen de oorzaak en gevolg van wat de organisatie doet en de resultaten die het bereikt.

Het model kan voor verschillende doeleinden gebruikt worden:

- Als ordeningskader voor het in kaart brengen van verschillende aspecten van het functioneren van een organisatie;
- Als diagnose-instrument om sterke en zwakke punten te identificeren;
- Als besturingsmodel in de jaarlijkse planning- en controlcyclus.[152]



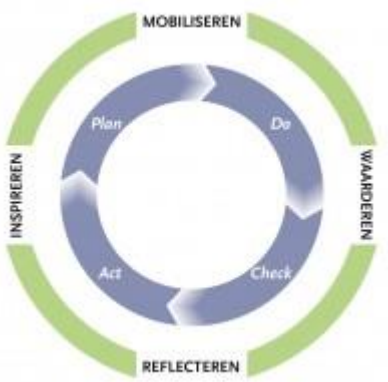
Figuur 58 Het INK-managementmodel (VU medisch centrum, 2004)

Het INK-managementmodel bestaat uit tien aandachtsgebieden, vijf organisatiegebieden, vier resultaatgebieden en het aandachtsgebied 'verbeteren en vernieuwen'. Deze staan weergegeven in de figuur hier rechtsboven. In de organisatiegebieden wordt beschreven hoe doe organisatie is ingericht. De organisatiegebieden zijn van invloed op de score van de resultaatgebieden.

Succesvolle organisaties hebben vijf fundamentele kenmerken:

1. Inspirerend leiderschap;
2. Bouwen op vertrouwen;
3. Samenwerking;
4. Resultaatgerichtheid; en
5. Continu verbeteren en vernieuwen.[153]

Bij het vijfde punt 'continu verbeteren en vernieuwen' kent het model twee veranderwielen. Het binnenste wiel is de PDCA-cyclus, deze bestaat uit plan, do, check en act. Het buitenste wiel is de IMWR-cirkel: inspireren, mobiliseren, waarderen en reflecteren. Deze cirkel is complementair aan de PDCA-cyclus, deze cirkel zijn dus eigenlijk de 'menselijke' oorzaken hoe men zich voortdurend kan verbeteren en vernieuwen.



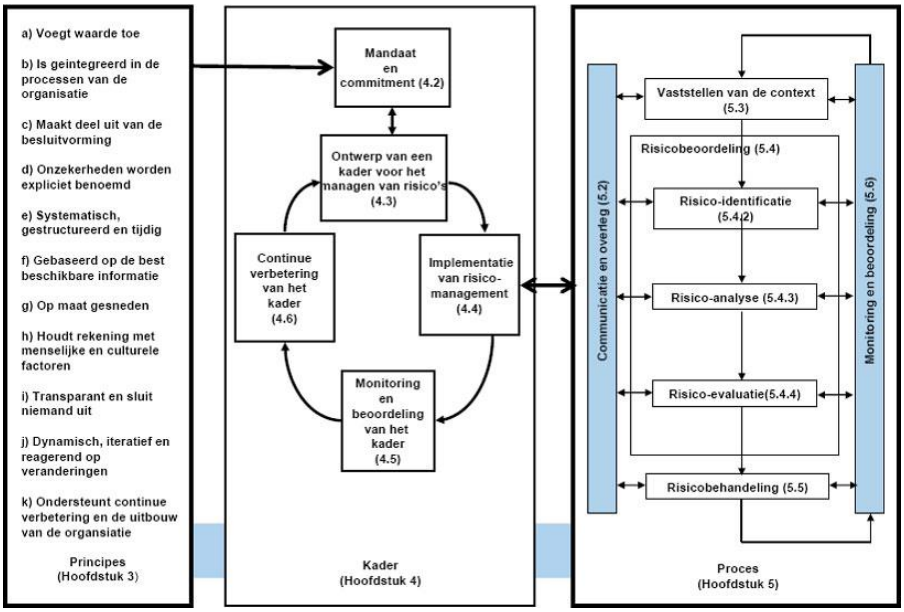
Figuur 59 Relatie PDCA-cyclus en IMWR-cirkel (INK, n.d.)

Om de kwaliteit van een organisatie te kunnen beoordelen kent het INK-managementmodel vier dimensies: activiteit, proces, organisatie en keten. De dimensies lopen dus van klein naar groot.[154]

[151] (Gert Jan Schop, 2017)
[152] (Eppink, Dr. D. en Keuning, Dr. D.J., 2012, p. 578)
[153] (Instituut Nederlandse Kwaliteit (INK))
[154] (Instituut Nederlandse Kwaliteit (INK))

Bijlage 2.3 ISO 31000-richtlijn

Eind 2009 is de ISO 31000 richtlijn gepubliceerd, deze hangt samen met de herziening van Guide 73. Hierin werd de terminologie aangesloten met de nieuwe inzichten in risicomanagement. ISO 31000 bestaat uit drie hoofdonderdelen: de principes van risicomanagement, het kader van risicomanagement en het risico managementproces.



Figuur 60 De drie hoofdonderdelen van ISO 31000 (focus op verbeteren, 2015)

Wanneer risicomanagement een effectief instrument worden voor een organisatie, moet aan de elf genoemde (zie figuur hierboven) principes worden voldaan.

Het kader (zie figuur hierboven) is bedoeld om risicomanagement te integreren in het al bestaande managementsysteem van de organisatie. Het raamwerk moet dus aangepast worden aan de organisatie zelf. In het kader kan men ook een variant op de PDCA-cyclus herkennen. De termen ontwerpen, implementeren, monitoring en beoordeling en continue verbetering komen grotendeels overeen met de termen plan, do, check en act.

Bij het proces is de context het uitgangspunt van de organisatie. Vanuit deze context worden risico's geïdentificeerd, geanalyseerd en geëvalueerd. Uit deze risicobeoordeling volgen de beheersingsmaatregelen. Van deze maatregelen meet je het effect en wat dit voor gevolgen heeft voor de context. Dit proces wordt periodiek herhaalt.[155]

Sterke punten van ISO 31000 zijn dat het rapport over deze richtlijn minder dan dertig pagina's telt en dat de structuur duidelijk is. Verder worden principes gekoppeld met de eerste stap van het kader: Mandaat en commitment, deze principes moeten wel zo goed mogelijk aansluiten bij de organisatie. Ook sluit deze richtlijn aan bij andere ISO-normen, zoals de ISO 9001 richtlijn over kwaliteit.[156]

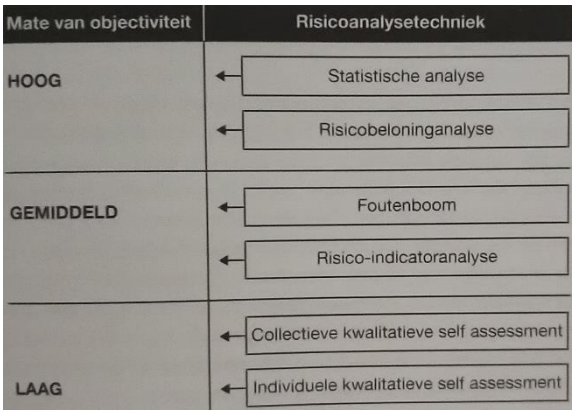
[155] (Erik van de Crommenacker, Peter Dona, Siebrand van der Ploeg, 2015, p. 138)
[156] (Focus op verbeteren, 2015, pp. 18,19)

Bijlage 3 Technieken risicobeoordeling[157]

Het inschatten van de omvang en waarschijnlijkheid van risico's gaat in de praktijk vaak samen met een grote mate van subjectiviteit. Wanneer het echter belangrijk is om de omvang en/of de waarschijnlijkheid goed in te schatten, kan men deze subjectieve inschatting niet langer hanteren. Risico's worden dan met behulp van rekenkundige modellen onderbouwd.

Drs. Urjan Claassen RA RE CIA (2009) onderscheidt de volgende methoden om risico's te beoordelen:

- Risico-indicatoranalyse;
- Statistische analyse;
- Risicobeloningsanalyse;
- Foutenboom;
- Risico self assessments.



Figuur 61 Risicoanalysetechnieken in relatie tot de mate van objectiviteit (DeLoach, 2000)

Risico-indicatoranalyse

Door middel van (gerichte) vragenlijsten worden betrokkenen gevraagd factoren te benoemen die het bereiken van de doelstellingen kunnen beïnvloeden. Het is aan te bevelen om bepaalde vragen een bepaald gewicht toe te kennen, zodat er prioritering kan plaatsvinden.

Statistische analyse

Bij deze methode wordt (een deel van) de populatie door middel van een steekproef geanalyseerd. Door deze steekproef kan er een oordeel (met enige mate van zekerheid) worden gevormd over de waarschijnlijkheid of over de omvang van het risico. Een steekproef kan op twee manieren gebeuren:

1. Een aselecte steekproef: alle elementen uit de populatie hebben dezelfde kans om in de steekproef te vallen;
2. Een selecte steekproef: bepaalde elementen uit de populatie hebben meer of minder kans om in de steekproef te vallen.

Risicobeloningsanalyse

In deze analyse wordt de afweging gemaakt tussen het risico en de verwachte gevolgen in relatie tot de opbrengsten en kosten. Als de opbrengsten beduidend hoger zijn dan de kosten kan er gekozen worden om voor een risicovollere optie te kiezen. Bij deze analyse gebruikt men scenario's, zo kan men een afgewogen keuze maken die past bij het risicoprofiel en de risicohouding.

Foutenboom

Bij deze techniek wordt door middel van 'wat-als'-vragen de waarschijnlijkheid en de impact van het risico achterhaald. Bij complexere relaties tussen de risico's en de doelstellingen kan deze methode het beste worden toegepast in combinatie met de risico-indicatoranalyse.

Risico self assessments

Hiermee kunnen managers en medewerkers zelf beoordelen welke risico's zich voordoen en van welk belang deze zijn.

[157] (Drs. Urjan Claassen RA RE CIA, 2009, p. 115 t/m 117)

Bijlage 4 Risicoprofiel

Onderstaand risicoprofiel (voorbeeld) maakt gebruik van een kwantitatieve methode met risicofactoren, de factoren zijn ingedeeld van 1 tot en met 4, waarbij 1 'laag' is en 4 'hoog' is.

Tabel 15 Risicoprofiel (o.b.v. literatuur Lizanne Vroom, 2014)

Nr.	Risico	Omschrijving	Situatie	Kans	Gevolg	Risico
1	Imagoschade	Wanneer een organisatie negatief in het nieuws komt	De organisatie is nog nooit negatief in het nieuws geweest	1	4	4
2	Fraude	Wanneer medewerkers of directie zichzelf onrechtmatig bevoordelen	Hiervan is nog nooit sprake geweest (ontdekt)	1	4	4
3	Activiteiten in buitenland (derde wereldlanden)	De veiligheid van medewerkers in het buitenland	Medewerkers gaan alleen naar buitenland en verblijven op onveilige locaties	2	3	6
4	Wet-en-regelgeving	Het voldoen aan wet-en-regelgeving, onder andere op het gebied van de verantwoording	Nieuwe wet-en-regelgeving dwingt tot aanpassingen	3	3	9

Het risicoprofiel kan ook worden uitgebreid met de genomen beheersingsmaatregelen en het nettorisico.

Tabel 16 Risicoprofiel inclusief netto-risico (o.b.v. literatuur Lizanne Vroom, 2014)

Nr.	Risico	Kans	Gevolg	Inherent risico	Beheersingsmaatregelen	Netto-risico
1	Imagoschade	1	4	4	Er is een gedragscode opgesteld	2
2	Fraude	1	4	4	Functiescheiding doorgevoerd Interne auditafdeling opgericht	1
3	Activiteiten in buitenland (derde wereldlanden)	2	3	6	Medewerkers verblijven 's nachts in een veilig aangemerkt hotel Medewerkers gaan minimaal met z'n tweeën naar het werkgebied	3
4	Wet-en-regelgeving	3	3	9	Interne auditafdeling opgericht Deskundig (financieel) personeel aangetrokken	3

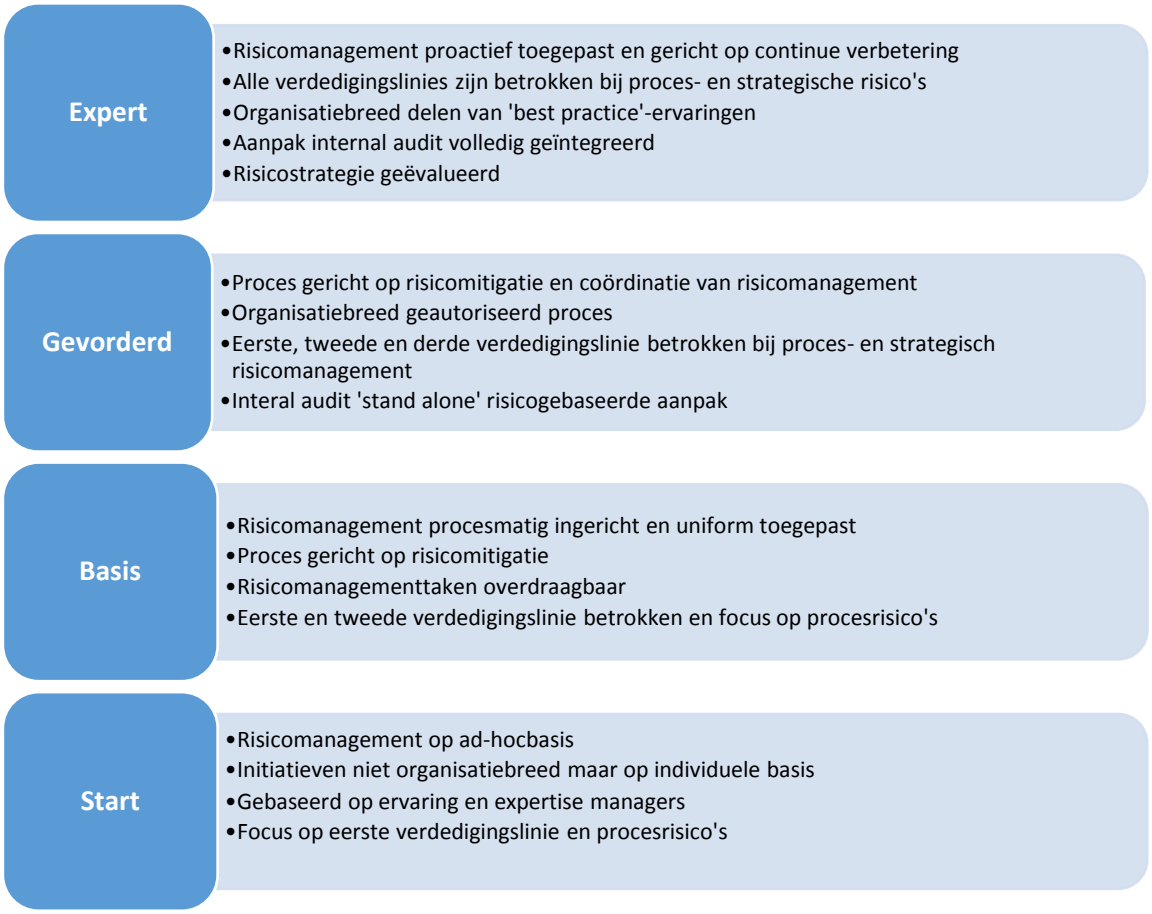
Bijlage 5 De taken, benodigde bewustzijn en kennis per verdedigingslinie

Tabel 17 Risicomanagementtaken, benodigde bewustzijn en kennis rondom risicomanagement (Drs. Urjan Claassen RA RE CIA, 2009)

Doelgroep	Risicomanagementtaken	Benodigde bewustzijn	Benodigde kennis
Directie (verdedigingslinie 1c	Aansturing van de jaarlijkse risicomanagementcyclus Ondertekening van documenten omtrent de interne beheersing Onderhoud strategisch risicoprofiel van de organisatie	Bewust van het belang en de toevoegde waarde van risicomanagement voor de organisatie; Aandacht voor het creëren van risicobewustzijn bij het middenkader en de medewerkers	Externe en interne wet-en-regelgeving omtrent governance en integraal risicomanagement Organisatiebrede risicomanagementtaal Ontwerp van beheersingsmaatregelen op strategisch niveau
Afdelingsmanager (verdedigingslinie 1b)	Het actueel houden van de administratieve organisatie en interne control alsook bijbehorende IT-gerelateerde beheersingsmaatregelen Onderhouden van risicoprofielen op operationeel niveau Verbeteracties opstellen n.a.v. de bevindingen bij audits Houden van toezicht op de effectiviteit van beheersingsmaatregelen op operationeel niveau Uitvoeren van het afdelingsplan	Bewust van de rol van de afdeling in het organisatiebrede waardecreatieproces Belang integraal risicomanagement Onderkennen en uitdragen van risicomanagement Prioriteiten stellen en capaciteit ter beschikking stellen Dubbelrol afdelingsmanagement: toezichthoudend ten aanzien van procesrisico's en uitvoerend bij strategische risico's	Plus hierboven Het beheersingskader en de soorten beheersingsmaatregelen Het jaarlijks testproces Borging van criteria rondom compliance en integraal risicomanagement in andere projecten Begrip en interpretatie van risicomanagementrapportages Ontwerpen beheersingsmaatregelen op strategisch niveau AO/IC referentiedocumentatie Beoordelen en begrijpen van processen en hierin opgenomen beheersingsmaatregelen
Medewerkers (verdedigingslinie 1a)	Uitvoeren van operationele testactiviteiten en rapportage Uitvoeren beheersingsmaatregelen en het opvolgen van de signaallijst	Belang van testwerkzaamheden onderkennen Actief betrokken bij het verbeteren van processen en beheersingsmaatregelen	Wat is integraal risicomanagement Soorten controls Testprocedures, testrichtlijnen Processen en IC's eigen afdeling
Auditfunctie (verdedigingslinie 3 + 4)	Opstellen jaarlijks controleplan Uitvoeren controles en rapportages hierover Advisering aan de 1e, 2e en 3e verdedigingslinie omtrent het verbeteren van de interne beheersing Ondersteuning van de 2e en 3e verdedigingslinie bij het onderhouden van risicoprofielen op strategische en procesniveau	Integratie van financiële operationele en IT-audits Bewustzijn dat de auditfunctie een belangrijke rol speelt in het creëren van een lerende organisatie Risicogebaseerde aanpak: hoge risico's intensief en frequent beoordelen. Lage risico's minder intensief en frequent beoordelen	Dezelfde kennis als de directie Risicogebaseerde controleaanpak Samenhang van de auditfunctie en een zelf controlerende organisatie ter voorkoming van inefficiënties rondom risicobeheer

Bijlage 6 Verschillende niveaus van risicomanagement

Het niveau hangt af van de aandacht die er voor risicomanagement is, het belang ervan, maar ook de omvang de organisaties.

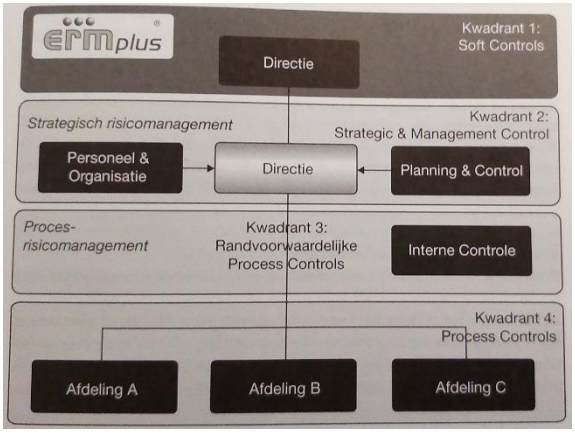


Figuur 62 Volwassenheidsniveaus risicomanagement (Drs. Urjan Claassen RA RE CIA, 2009)

Het niveau van risicomanagement kan ook uitgebreid worden door verschillende aspecten toe te voegen. Zo kan het niveau per stap in het risicomanagement verschillen maar ook wat betreft de infrastructuur.

Bijlage 7 Soorten beheersingsmaatregelen op verschillende niveaus

Hiernaast staat het raamwerk voor de inrichting van de beheersing volgens Drs. Urjan Claassen RA RE CIA weergegeven. Dit kader bevat verschillende soorten beheersmaatregelen, in relatie tot de verschillende soorten van risico's. De verantwoordelijkheden voor de uitvoering van deze maatregelen in de organisatie hebben betrekking op de verschillende verdedigingslinies (Figuur 47).



Figuur 63 ERM plus-beheersingskader (Drs. Urjan Claassen RA RE CIA, 2009)

Soft controls (kwadrant 1)

Een definitie van soft controls die vaak gebruikt wordt is die van De Heus en Stremmelaar (2000): "een verzameling van (beheersings)maatregelen welke – meer dan 'hard controls' – ingrijpen op c.q. appelleren aan het persoonlijk functioneren van medewerkers."[158] Van belang is dat het bij soft controls gaat om niet-tastbare gedrag beïnvloedende factoren in een organisatie (Roth, 2010). Volgens het NBA zijn de belangrijkste vijf elementen van soft control: leiderschap en voorbeeldgedrag, communiceren en informeren, motiveren en waarderen, stimuleren en faciliteren en aanspreken en handhaven.[159] Deze elementen zijn over het algemeen moeilijker te meten dan hard controls. Soft controls zullen gecombineerd moeten worden met hard controls; in de praktijk moet hier een juiste balans tussen worden gevonden (De Heus en Stremmelaar, 2000). Het is niet zo dat hoe meer hard controls er zijn, hoe beter de organisatie haar doelstellingen kan behalen. Een overvloed aan hard controls kan leiden tot onwerkbare situaties en kan daarmee het verantwoordelijkheidsbesef van managers en personeel ondermijnen. De werking van hard controls hangt af van het draagvlak onder het management en het personeel. Zij zullen deze hard controls moeten begrijpen en kunnen toepassen in de praktijk (Kapitein en Wallage, 2010).[160]

Zo komt Cools (2005) tot de conclusie dat control, vertrouwen en een sterke cultuur de 3 bouwstenen zijn voor interne beheersing waarmee een organisatie succesvol kan opereren. Control is dan de randvoorwaarde voor het kunnen geven van vertrouwen.[161]

Strategic & managementmodel (kwadrant 2)[162]

Drs. Urjan Claassen RA RE CIA (2009) onderscheidt binnen strategic & management control drie groepen beheersingsactiviteiten:

1. Strategic Control: bij deze groep horen de activiteiten die gericht zijn op het formuleren van de doelstellingen (op lange termijn), de missie en visie en de middelen die hiervoor gebruikt worden om deze doelstellingen te realiseren. Maar ook de activiteiten om de uitvoering van de strategie te bewaken. De strategische planning is hierbij een belangrijk onderdeel, strategische planning is verdeeld in vijf stappen:
    a. Strategisch venster: in deze fase wordt een beschrijving gemaakt van de financiën, het bedrijfsmodel en het personeel van de organisatie;
    b. Analyse: het strategische venster vormt de basis voor de analyse, die zowel intern als extern wordt uitgevoerd. Om deze te combineren wordt de SWOT-analyse gebruikt;

[158] (Jeroen de Kort, 2014, p. 31)
[159] (Nederlandse Beroepsorganisatie van Accountants, 2013, p. 8)
[160] (Annfinance, 2011)
[161] (Prof. dr. Kees Cools RA, 2006, pp. 140, 141)
[162] (Drs. Urjan Claassen RA RE CIA, 2009, pp. 133,134 en 143 t/m 166)

c. Strategisch plan: op basis van de analyse kunnen de missie en visie, de doelstellingen en kritische succesfactoren van de organisatie worden geformuleerd;
d. Businessplanning: in deze fase wordt het strategisch plan vertaalt naar de korte termijn en wordt er detaillering aangebracht;
e. Persoonlijke planning: per personeelslid worden doelstellingen geformuleerd, waarbij rekening wordt gehouden met de individuele taken en bevoegdheden. Het eindproduct is een persoonlijk ontwikkelingsplan;

2. Management Control: de activiteiten in deze groep zijn gericht op het vertalen van de strategische planning naar concrete taken in de lagere niveaus van de hiërarchie. Twee belangrijke kenmerken van management control zijn:
   a. Management control is gericht op het menselijk (gewenst) gedrag;
   b. Management control komt voort uit de strategie;

   Voor een correcte vertaling dient een vijftal aandachtsgebieden evenwichtig te worden uitgewerkt:
   - Organisatiestructuur: er zijn verschillende vormen van organisatiestructuren, zo kan men denken aan de juridische organisatievorm, de organisatorische organisatievorm en organisatiedelen;
   - Bedrijfsprocessen: het ontwerp en inrichting van bedrijfsprocessen hebben een grot e invloed op de wijze waarop de doelstellingen worden behaald;
   - Resultaatgebieden: de samenhang en voortgang van resultaten zijn van groot belang voor het realiseren van de strategische doelstellingen. Om dit te waarborgen wordt in belangrijke mate gesteund op de planning- en controlcyclus;
   - Budgettering: hierbij moeten er doelstellingen worden geformuleerd voor het komende jaar, deze zijn dan uitgewerkt in resultaatgebieden. Nadat het budget is goedgekeurd, moeten de verantwoordelijkheden (van managers) worden bepaald;
   - Beoordelen en belonen: het meten, beoordelen en belonen van prestaties vormt de basis voor de inrichting van prestatiesystemen;

3. Task Control: deze activiteiten zijn erop gericht dat de concrete taakopdrachten op de lagere niveaus in de hiërarchie efficiënt en effectief worden uitgevoerd. Bij task control worden vier vormen van taakbeheersing onderscheiden:
   a. Managementtoezicht: de beoordeling door het management of strategische en procesrisico's voldoende worden beheerst;
   b. Stuurgroepen en programmamanagement: managers die verantwoordelijk zijn voor bepaalde bedrijfsprocessen en/of projecten zijn het beste in staat om risico's snel te herkennen;
   c. Prestatie-indicatoren en benchmarking: door de resultaten van de organisatie uit te drukken in prestatie-indicatoren kunnen deze resultaten beter vergeleken worden met concurrenten;
   d. Auditrapportages: door middel van auditrapportages kan inzicht worden verkregen in de kwaliteit van management control.

Operational control (kwadrant 3 en 4)[163]

Bij operationele beheersing worden bedrijfsprocessen benaderd vanuit de beheersingsoptiek: welke operationele taken en beheersmaatregelen zijn nodig om processen efficiënt en effectief te laten verlopen. Bij kwadrant 3, randvoorwaardelijke beheersingsmaatregelen, worden de volgende maatregelen onderscheiden:

- Functiescheiding: van oorsprong komt deze maatregel uit het vakgebied van de Administratieve Organisatie en dan met name de waardekringloop. Binnen deze kringloop kunnen verbanden worden gelegd tussen de opgeofferde en de verkregen waarde en tussen een toestand en een gebeurtenis. Bij het bewaken van deze verbanden worden vijf

[163] (Drs. Urjan Claassen RA RE CIA, 2009, p. 166 t/m 175)

verschillende functies onderscheiden: beschikkend, bewarend, registrerend, controlerend en uitvoerend. Vanuit economisch perspectief is functiescheiding een verantwoorde maatregel en vormt het fundament voor gebruikerscontroles en zorgt voor een effectieve werking van procescontroles;
- Algemene ICT-controles: ICT-controles dienen effectief te worden ingericht op te kunnen steunen op applicatiecontroles. De volgende soorten ICT-controles kunnen onderscheiden worden: IT-beleid en –management, change management, systeemontwikkeling, logische toegangbeveiliging, systeembeheer, continuïteit en fysieke beveiligingsmaatregelen.

Kwadrant 4, procesgerelateerde beheersingsmaatregelen, kan vanuit twee verschillende hoeken worden bekeken, vanuit:
- Procesbeheersing:
    - Gebruikerscontroles: deze kunnen vervolgens weer verdeeld worden in drie groepen:
        - Gebruikerscontroles die niet gerelateerd zijn aan de geautomatiseerde gegevensverwerking, bijvoorbeeld het controleren van stamgegevens;
        - Gebruikerscontroles die steunen op de (effectieve werking van de) applicatiecontroles, denk aan het onderzoeken van gegevens die 'geproduceerd' zijn door de applicatie;
        - Gebruikerscontroles die gericht zijn op de (effectieve werking van de) applicatiecontroles, zoals een handmatige narekening van een bruto-nettoberekening van een salarisrun die de applicatie heeft uitgerekend.
    - Applicatiecontroles: ook applicatiecontroles kunnen worden verdeeld:
        - Configuratie-instellingen: bijvoorbeeld voorraadwaarderingen;
        - Masterdatabeveiliging: het wijzigen van stamgegevens moet door middel van autorisatie gebeuren;
        - Control override: bijvoorbeeld het vrijgegeven van geblokkeerde betalingen;
        - Functiescheidingen op applicatieniveau: bijvoorbeeld de scheiding tussen de invoer en de autorisatie van betalingen;
        - Interfaces: een voorbeeld is de overdracht van inkooporders uit inkoopsysteem naar het betalingssysteem;
        - Signaleringslijsten: deze lijsten zijn ontdekkend van aard en kunnen zowel geautomatiseerd als handmatig zijn.
- Procesnormen:
    - Normen voor de invoer: deze normen zijn gericht op een juiste, tijdige en complete invoer van input in het proces;
    - Normen voor de uitvoer: deze normen gaan niet over de input, maar over de output;
    - Normen voor de doorvoer: in tegenstelling tot de normen voor de invoer en de uitvoer, zijn deze normen meer gericht op de uitvoering van het proces dan op het eindresultaat ervan.

Bijlage 8 De gunstige effecten van evenwichtig risicomanagement in een gezonde bedrijfscultuur

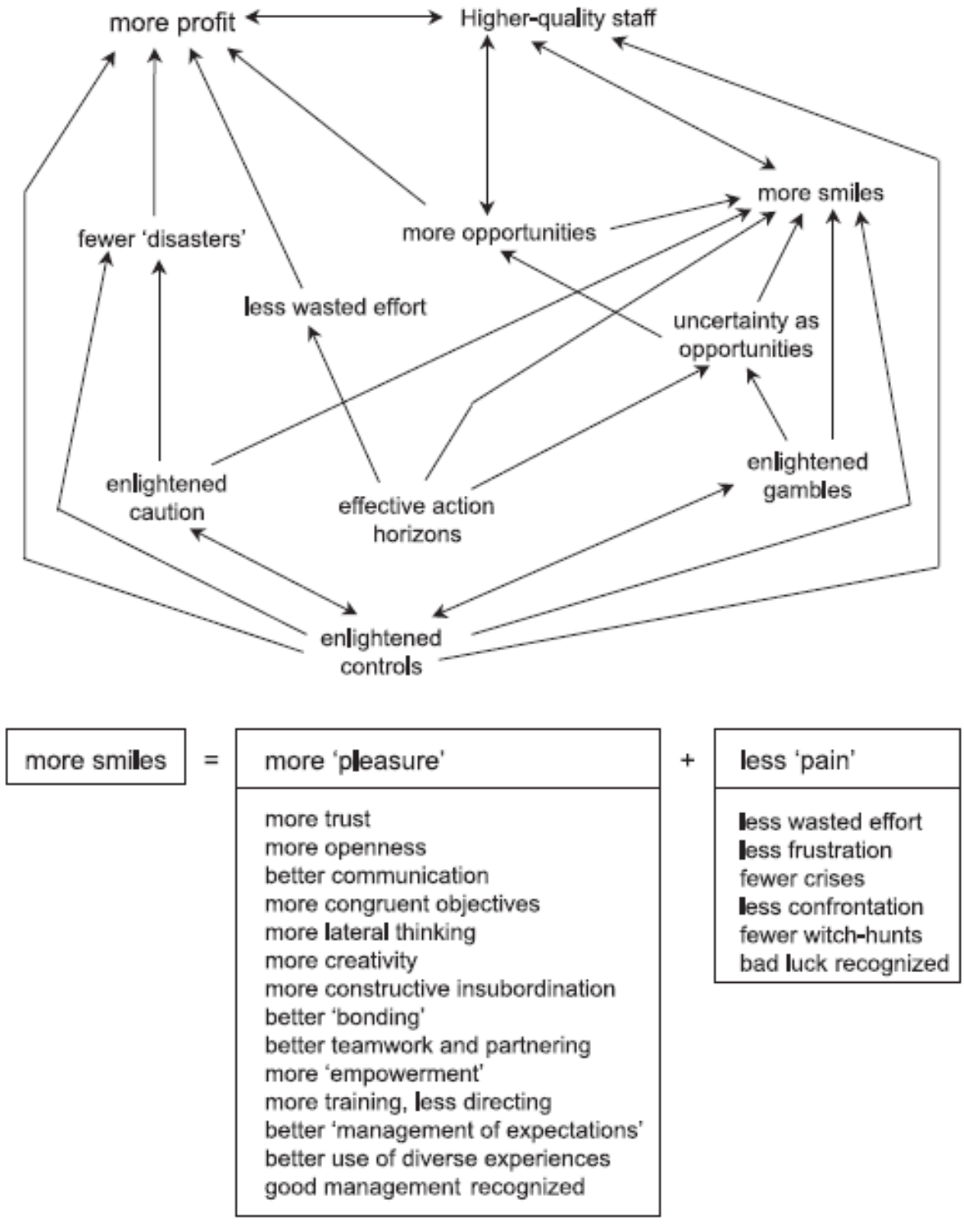


Figure 17.2—Corporate benefits of a risk management culture

Figuur 64 Voordelen van een risicomanagementcultuur (Chapman en Ward, 2003: 347)

Bijlage 9 Het Dynamisch Business Model

Het Business Canvas Model is de basis voor het Dynamisch Business Model. Zoals eerder gezegd is het Business Canvas Model ontwikkeld door Alexander Osterwalder en Yves Pigneur. Dit model bestaat uit een aantal onderdelen die voor elke organisatie van toepassing zijn. Deze onderdelen zijn: partners, activiteiten, middelen, waarde propositie, klantrelaties, klantsegment, kanalen, kostenstructuur en opbrengstenstromen.

L. Vroom heeft dit model doorontwikkeld tot het Dynamisch Business Model. Met dit model kan een organisatie een goed beeld krijgen van zijn omgeving. Verder kan het worden gebruikt om risico's te identificeren. Hieronder wordt het Dynamisch Business Model gekoppeld aan de risico-inventarisatie op bedrijfsonderdelen.

Figuur 65 Dynamisch Business Model (Jaap Zijlstra & Lizanne Vroom, 2014)

Risicoanalyse op bedrijfsonderdelen	
Algemeen	00 Algemene organisatiegegevens
Omgeving	01 Omgeving
Waarom, hoe en wat	02 Missie, visie, strategie
	03 Waardepropositie
	04 Producten / diensten
Wie	05 Directie
	06 Medewerkers
Processen / activiteiten	07 Juridische zaken
	08 Financiële zaken
	09 Automatisering
	10 Inkoop / Import
	11 Productieproces
	12 Opslag & (Intern) Transport
	13 Verkoop / Export
Bedrijfsmiddelen	14 Onroerende zaken
	15 Inventaris, machines & electronica
	16 Materieel & Wagenpark

Per onderdeel kunnen verschillende risico's worden benoemd. Men moet zich niet gaan focussen op de verschillende bedrijfsonderdelen, de samenhang tussen de onderdelen en afdelingen moeten altijd in beeld blijven.

Op basis van de hiernaast weergegeven structuur kan een risico-inventarisatiechecklist worden samengesteld.

Bijlage 10 Wet- en regelgeving met betrekking tot verenigingen en stichtingen

Organisaties die RJ 650 toepassen zijn opgericht als vereniging of stichting. Er zal daarom, eerst vanuit het Burgerlijk Wetboek en later (kort) vanuit de Raad voor de Jaarverslaggeving ingegaan worden op de wet- en regelgeving die betrekking heeft op de rechtsvormen 'stichting' en 'vereniging'.

Het Burgerlijk Wetboek

In het Burgerlijk Wetboek is in vergelijking met andere rechtsvormen maar een beperkt aantal regels en voorschriften opgenomen voor stichtingen en verenigingen.
Een vereniging is volgens art. 2:26 BW "een rechtspersoon met leden die is gericht op een bepaald doel, anders dan een dat is omschreven in artikel 53 lid 1 of 2."[164] Met het laatste gedeelte worden doelen bedoeld van een coöperatie of van een onderlinge waarborgmaatschappij. Organisaties die RJ 650 toepassen zijn echter niet opgericht in deze rechtsvormen. Een ander belangrijk kenmerk is dat de vereniging geen winst onder haar leden mag verdelen.

Een stichting is volgens art. 2:285 BW "een door een rechtshandeling in het leven geroepen rechtspersoon, welke geen leden kent en beoogt met hulp van een daartoe bestemd vermogen een in de statuten vermeld doel te verwezenlijken."[165] Ook een stichting mag geen (winst) uitkeringen doen, behalve wanneer deze uitkeringen een ideëel of sociaal karakter hebben en deze gedaan worden aan derden.

Onafhankelijk van de bepalingen van Titel 9 moeten rechtspersonen voldoen aan de algemene administratieverplichting (art. 2:10 lid 1 BW). Dit betekent dat het bestuur een administratie moet voeren waarin rechten en verplichtingen kunnen worden gekend. In het tweede en derde lid van datzelfde artikel worden aanvullende eisen genoemd:

- Het bestuur is verplicht om elk jaar binnen zes maanden na afloop van het boekjaar de balans en de staat van baten en lasten van de rechtspersoon op te maken en op papier te stellen; en
- Het bestuur is verplicht om de administratie, zoals bedoeld in lid één en twee zeven jaar te bewaren.[166]

In Titel 9 staan nadere bepalingen met betrekking tot de jaarrekening en het bestuursverslag. Deze titel is echter alleen van toepassing op de coöperatie, de onderlinge waarborgmaatschappij, de naamloze vennootschap, de besloten vennootschap met beperkte aansprakelijkheid en stichtingen en verenigingen die één of meerdere ondernemingen in stand houden waarvan de netto-omzet € 6 miljoen of meer bedraagt (art. 2:360 BW). [167] Stichtingen en verenigingen die bij wet verplicht zijn een financiële verantwoording op te stellen die gelijkwaardig is aan een jaarrekening zoals bedoeld in Titel 9 en die ook openbaar wordt gemaakt, vallen buiten de werking van Titel 9.[168] Dit is het geval bij organisaties die bijvoorbeeld RJ 650 toepassen.

Volgens het CBF waren er eind 2002, 12 instellingen van de 159 fondsenwervende instellingen die een CBF-keurmerk bezaten en een onderneming dreven, deze organisaties stelden hun jaarverslag echter ook op volgens richtlijn 650.[169]

Verenigingen die niet onder de werkingssfeer van Titel 9 vallen, moeten toch nog rekening houden met andere voorschriften van het Burgerlijk Wetboek. Zo moet onder andere bij een vereniging het

[164] (Mw. mr. A.M.M.M. van Zeijl, Mr. J. Keizer, Mr. J.M.K. Burger e.a., 2016, p. 384)
[165] (Mw. mr. A.M.M.M. van Zeijl, Mr. J. Keizer, Mr. J.M.K. Burger e.a., 2016, p. 467)
[166] (Mw. mr. A.M.M.M. van Zeijl, Mr. J. Keizer, Mr. J.M.K. Burger e.a., 2016, p. 376)
[167] (Mw. mr. A.M.M.M. van Zeijl, Mr. J. Keizer, Mr. J.M.K. Burger e.a., 2016, p. 503)
[168] (Raad voor de Jaarverslaggeving, 2014, p. 1)
[169] (Bart Sterenborg, 2003, p. 47)

bestuur op een algemene vergadering binnen zes maanden na afloop van het boekjaar, een verlenging van deze termijn niet meegenomen, een bestuursverslag uitbrengen (art. 2: 48 BW lid 1).[170]
De stichting die wel een onderneming in stand houdt, moet ook nog voldoen aan art. 2:300 BW.

In de versie van 2016 van het Burgerlijk Wetboek is het wetvoorstel publicatieplicht stichtingen nog niet opgenomen. Hierbij wordt het bestuur van een stichting verplicht de balans en de staat van baten en lasten binnen acht dagen na het opmaken ervan openbaar te maken via het handelsregister.[171] Organisaties die RJ 650 toepassen hebben echter veelal een ANBI-status, deze status verplicht organisaties wel diverse informatie te publiceren (via internet).[172] Verenigingen hebben deze plicht (nog) niet.

Gezien de geringe wettelijke verplichtingen heeft de Raad voor de Jaarverslaggeving richtlijnen opgesteld voor deze rechtsvormen.

De Raad voor de Jaarverslaggeving

Specifiek met betrekking tot fondsenwervende instellingen heeft de Raad voor de Jaarverslaggeving een specifiek hoofdstuk opgenomen, richtlijn 650.

[170] (Mw. mr. A.M.M.M. van Zeijl, Mr. J. Keizer, Mr. J.M.K. Burger e.a., 2016)
[171] (Overheid.nl, sd)
[172] (Intervivos B.V., sd)

Bijlage 11 Enquête risicomanagement bij fondsenwervende instellingen

Welkompagina

Bedankt dat u de tijd en moeite heeft genomen om deze enquête in te willen vullen. Het invullen ervan zal ongeveer 10 tot 15 minuten in beslag nemen. Voordat u begint is het handig dat u het (concept) jaarverslag van 2016 voor u heeft liggen.

Algemene vragen organisatie

1. Wat is uw functie? (verplicht)

Open antwoord

2. Wat was de hoogte van de baten in 2015 en 2016? (verplicht)

2015: Open antwoord
2016: Open antwoord

3. Is er sprake van een toezichthoudend orgaan? (RvC, bestuur, RvT)? (verplicht)

Als deze vraag met 'nee' beantwoord wordt, dan kunt u de volgende vraag overslaan

- Ja (2 punten);
- Nee (0 punten).

4. Is er binnen het toezichthoudend orgaan sprake van een Audit Commissie?

- Ja (1 punt)
- Nee (0 punten).

5. Wordt in het jaarverslag RJ 650 Fondsenwervende instellingen toegepast? (verplicht)

- Ja;
- Nee.

6. Is de organisatie aangesloten bij de erkenningsregeling? (verplicht)

- Ja (2 punten);
- Nee (0 punten).

7. Wordt de jaarrekening door een accountant gecontroleerd? (verplicht)

Meerdere antwoorden mogelijk:

- Nee (0 punten);
- Nee, de jaarrekening wordt door een accountant opgesteld (1 punt);
- Nee, er wordt een beoordelingsverklaring afgegeven (2 punten);
- Ja, er wordt een vrijwillige controle uitgevoerd (3 punten);
- Ja, er wordt een wettelijke controle uitgevoerd (3 punten).

8. Waarom doet de organisatie aan risicomanagement?

Mocht u bij deze vraag niet het antwoord 'Om er voordeel mee te behalen' hebben gegeven, dan kunt u de volgende vraag overslaan. Mocht de organisatie niet aan risicomanagement doen, dan kunt u naar het einde van de enquête gaan.

Meerdere antwoorden zijn mogelijk (Maximaal 2 punten):

- De organisatie doet niet aan risicomanagement (0 punten);
- Het is verplicht vanuit de wet- en-regelgeving (1 punt);
- Om er voordeel mee te behalen (2 punten).

9. In welke mate verwacht u er voordeel mee te behalen?

(Schaal: zeer weinig voordeel (1) tot zeer veel voordeel (5)):

- Stabielere resultaten (financieel);
- Het beperken van de impact van risico's;
- Het verminderen van de kans op risico's;
- Het verbeteren van het resultaat.

Voorbereiding op risicomanagement

10. Worden er binnen de organisatie managementrapportages uitgebracht waarin de veranderingen binnen en buiten de organisatie aan bod komen?

Mocht u bij deze vraag het antwoord 'Niet' hebben gegeven, dan kunt u de volgende vraag overslaan

- Niet (0 punten);
- Minder dan één keer per jaar (1 punt);
- Jaarlijks (2 punten);
- Elk kwartaal (3 punten);
- Maandelijks (4 punten);
- Wekelijks (4 punten).

11. Gebruikt de organisatie de opgedane informatie van de managementrapportages voor risicomanagement? Denk bijvoorbeeld aan de risico-inventarisatie.

- Ja (2 punt);
- Nee (0 punten).

De organisatie van risicomanagement

12. Is er sprake van een CRO (Chief Risk Officer) binnen de organisatie (of een vergelijkbare functionaris die eindverantwoordelijk is voor risicomanagement)?

Mocht u het antwoord 'Er is geen CRO en ook geen vergelijkbare functie' hebben gegeven, dan kunt u de volgende vraag overslaan

- Er is een CRO op het niveau van de Raad van Bestuur/Directie (2 punten);
- Er is een CRO, maar niet op niveau van de Raad van Bestuur/Directie (2 punten);
- Er is geen CRO, maar wel een vergelijkbare functie op het niveau van de Raad van Bestuur/Directie (1 punt);
- Er is geen CRO, maar wel een vergelijkbare functie op een andere niveau (1 punt);
- Er is geen CRO en ook geen vergelijkbare functie (0 punten).

13. Heeft de CRO of de vergelijkbare functie een uitvoerende of adviserende taak?

- Adviserend;
- Uitvoerend;
- Zowel adviserend als uitvoerend.

14. Wie coördineert de activiteiten met betrekking tot risicomanagement?

- Niet georganiseerd (0 punten);
- Een aparte risicomanagementfunctie/afdeling (1 punt);
- Een aparte commissie (1 punt);
- De financiële afdeling (1 punt);
- Het bestuur/directie (1 punt);
- Het lijnmanagement (1 punt).

15. Zijn de verantwoordelijkheden, taken en bevoegdheden binnen de organisatie met betrekking tot risicomanagement binnen de organisatie bekend?

- Niet (0 punten);
- Vrijwel niet (0,5 punt);
- Deels (1 punt);
- Grotendeels (1,5 punten);
- Bij iedereen (2 punten).

Risicobeleid (maximaal 2 punten toekennen bij vraag 17)

16. Heeft de organisatie risicomanagementdoelstellingen opgesteld?
- Nee (0 punten);
- Ja (1 punt);
- Ja, deze zijn gekoppeld aan de organisatiedoelstellingen (2 punten);

17. Welke voorwaarden heeft de organisatie gesteld voor (effectief) risicomanagement?
Meerdere antwoorden mogelijk
- Geen (0 punten);
- De verantwoordelijkheden zijn duidelijk op alle niveaus (0,5 punt);
- Risicobewustzijn op verschillende risicogebieden op alle niveaus (0,5 punt);
- Risicomanagement is onderdeel van (besluitvormings)processen (0,5 punt);
- Risicomanagement sluit aan bij de doelstellingen van de organisatie (0,5 punt);
- Anders, namelijk: (open antwoord) (0,5 punt).

18. Hoe voert de organisatie het risicomanagementproces uit?
Met risicomanagementproces wordt het geheel van de te nemen stappen bedoeld, zoals inventarisatie, evaluatie, beheersing etc.

- Niet (0 punten);
- Ad-hoc (1 punt);
- Als onderdeel van de (jaarlijkse) planning & controlcyclus (2 punten);
- Anders, namelijk (open antwoord) (1 punt);

19. Welk model gebruikt de organisatie voor het risicomanagement?
- Geen (0 punten);
- COSO / COSO ERM (1 punt);
- INK / EFQM Model (1 punt);
- ISO 31000 (1 punt);
- Management of Risk (M_o_R) (1 punt);
- INTOSAI (1 punt);
- Andere, namelijk: (open antwoord) (1 punt).

20. Is binnen de organisatie de risicobereidheid bepaald, vastgelegd en gecommuniceerd?
Meerdere antwoorden zijn mogelijk
- Nee (0 punten);
- De risicobereidheid is bepaald (1 punt);
- De risicobereidheid is vastgelegd (1 punt);
- De risicobereidheid is gecommuniceerd (1 punt: communicatie).

21. Wordt beloning en waardering gekoppeld aan de uitvoering van risicomanagement?
- Nee (0 punten),
- Ja, er is een indirecte (formele) relatie tussen de prestaties op het gebied van risicobeheersing en beloning (1 punt);
- Ja, er is een directe formele relatie tussen de prestaties op het gebied van risicobeheersing en beloning (1 punt).

Risicocultuur (maximaal 8 punten toekennen)

22. In welke mate zijn de volgende stellingen over risicomanagement van toepassing binnen de organisatie?

(zeer veel van toepassing (1) tot zeer weinig van toepassing (5))

- Risicomanagement leidt tot toevoeging van waarde aan de organisatie (0 – 2 punten);
- Personeelsleden mogen fouten maken, zolang ze er maar van leren (0 – 2 punten);
- Het bestuur/directie geeft het goede voorbeeld (0 – 2 punten);
- Overtredingen van interne regels worden serieus genomen (0 – 2 punten);
- Medewerkers kunnen vrij communiceren over risico's richting leidinggevenden (0 – 2 punten);
- De beloningsstructuur zorgt voor effectief risicomanagement (0 – 2 punten).

Risicobewustzijn (maximaal 6 punten toekennen)

23. In welke mate zijn de volgende stellingen van toepassing binnen de organisatie?

(vrijwel niemand tot vrijwel iedereen)

- Iedereen binnen de organisatie is zich bewust van de noodzaak van risicomanagement (0 – 2 punten);
- Iedereen binnen de organisatie is bekend met de (belangrijkste) risico's (0 – 2 punten);
- Iedereen binnen de organisatie voert de genomen maatregelen uit (0 – 2 punten, 1 punt: risicobeheersing);
- Iedereen binnen de organisatie is er zich van bewust dat elk moment er zich risico's kunnen voordoen (0 – 2 punten).

Risico-inventarisatie en evaluatie (maximaal 14 punten, maximaal 4 punten toekennen bij vraag 26)

24. Hoe vaak wordt binnen de organisatie een (bedrijfsbrede) risico-inventarisatie en risico-evaluatie uitgevoerd?

Als u deze vraag met 'Nooit' heeft beantwoord, kunt u de volgende vragen overslaan

- Nooit (0 punten);
- Minder dan één keer per jaar (1 punt);
- Jaarlijks (2 punten);
- Elk kwartaal (3 punten);
- Maandelijks (3 punten).

25. Wat voor soort risico's brengt de organisatie hierbij in kaart?

Meerdere antwoorden mogelijk:

- Strategische risico's (1 punt);
- Operationele risico's (1 punt);
- Financiële risico's (1 punt);
- Verslaggevingsrisico's (1 punt);
- Wet- en regelgevingsrisico (1 punt).

26. Van welke hulpmiddelen maakt de organisatie gebruik bij risico-inventarisatie en risico-evaluatie?

Meerdere antwoorden mogelijk

- Documentenstudie (0,5 punt);
- Interviews (0,5 punt);
- Vragenlijsten/checklists (0,5 punt);
- Incidentenregistraties (0,5 punt);
- Scenarioanalyses (0,5 punt);
- Gevoeligheidsanalyses (0,5 punt);
- Simulaties (0,5 punt);
- Foutenboom (0,5 punt);

- Visgraatmethode (0,5 punt);
- Andere (0,5 punt).

27. Voert de organisatie de risico-evaluatie tegelijk uit met de risico-inventarisatie of worden deze apart uitgevoerd?
- Eerst wordt de inventarisatie uitgevoerd dan evaluatie (2 punt);
- Tegelijkertijd (0 punten);
- Geen vaste volgorde (1 punten).

Risicobeheersing (maximaal 9 punten, maximaal 4 punten toekennen bij vraag 28 + 1 punt bij vraag 23)

28. Welke strategie voert de organisatie uit in welke situatie?

(Het vermijden van risico, het verminderen van de kans op risico, het beperken van de impact van risico, het overdragen van risico, het accepteren van risico, geen)
- Risico met hoge kans en hoge impact (1 punt voor vermijden, 0,5 punten voor beperking en vermindering en geen punten bij overdracht, acceptatie en geen strategie);
- Risico met hoge kans en lage impact (1 punt voor zowel overdracht als vermindering, 0,5 punten voor acceptatie, geen punten voor vermijden, beperking en geen strategie);
- Risico met lage kans en hoge impact (1 punt voor zowel overdragen als beperken impact, geen punten voor de rest van de opties);
- Risico met lage kans en lage impact (1 punt voor alleen acceptatie, geen punten voor de rest van de opties).

29. Voert de organisatie voordat een maatregel genomen wordt, een kosten-batenanalyse uit?
- Ja (2 punt);
- Nee (0 punten).

30. Wordt bij het accepteren van risico's, rekening gehouden met de capaciteit om risico te dragen?
- Ja (2 punt);
- Nee (0 punten).

Evaluatie en toezicht (maximaal 8 punten)

31. Hoe vaak worden de genomen beheersingsmaatregelen geëvalueerd?

Mocht u hier het antwoord 'Nooit' hebben gegeven, dan kunt u de volgende twee vragen overslaan

- Nooit (0 punten);
- Minder dan één keer per jaar (1 punt);
- Jaarlijks (2 punten);
- Eén keer per kwartaal (3 punten);
- Maandelijks (3 punten).

32. Hoe evalueert de organisatie de uitvoering van de genomen maatregelen?

Meerdere antwoorden zijn mogelijk
- Niet (0 punten);
- Via herhaling (0,5 punt);
- Via inspectie (0,5 punt);
- Via interview (0,5 punt);
- Via het doorlopen van het proces (0,5 punt);
- Systeemonderzoek (0,5 punt);
- Anders, namelijk: (open antwoord) (0,5 punt).

33. Maakt de organisatie hierbij gebruik van prestatie-indicatoren?

- Ja (1 punt);
- Nee (0 punten).

34. Krijgt de organisatie feedback van de (externe) accountant over risico's en risicomanagement?
- Ja (1 punt);
- Nee (0 punten).

Bijsturing en continue verbeteren (maximaal 6 punten)

35. In welke mate volgt de organisatie de verbeterpunten op die naar voren kwamen uit de evaluatie?

(Onvoldoende tot uitstekend)
- Snelheid (0 – 1 punt);
- Kwaliteit (0 – 1 punt).

36. Formuleert de organisatie ambities met betrekking tot risicomanagement?
- Ja (1 punten);
- Nee (0 punten)

37. Vergelijkt de organisatie haar prestaties op het gebied van risicomanagement met andere organisaties?
- Ja (1 punt);
- Nee (0 punten).

38. Worden de 'best practices' en kennis binnen de organisatie gedeeld/gecommuniceerd?
- Ja (1 punt: bijsturing + 1 punt: communicatie);
- Nee (0 punten).

39. Biedt de organisatie personeelsleden trainingen, cursussen, opleidingen, workshops en dergelijke aan (o.a. met betrekking tot risicomanagement)?
- Ja (1 punt);
- Nee (0 punten).

Informatie en communicatie (maximaal 12 punten, 10 + 2 punten ergens anders)

40. Hoe vaak vindt er binnen de organisatie overleg plaats over risico's en risicomanagement?

Mocht u hier het antwoord 'Niet' hebben gegeven, dan kunt u de volgende twee vragen overslaan
- Niet (0 punten);
- Ad hoc/incidenteel (1 punt);
- Jaarlijks (2 punten);
- Elk kwartaal (3 punten);
- Maandelijks (4 punten).

41. Op welk niveau speelt dit overleg zich af?

Meerdere antwoorden mogelijk
- Op het niveau van het toezichthoudend orgaan (1 punt);
- Op het niveau van het bestuur/directie (1 punt);
- Op het niveau van lijnmanagement (1 punt).

42. Waarover vindt overleg plaats?

Meerdere antwoorden mogelijk
- De belangrijkste risico's (0,5 punt);
- Zich voorgedane risico's/incidenten (0,5 punt);

- De status van beheersingsmaatregelen (0,5 punt);
- Verbeterpunten met betrekking tot risicomanagement (0,5 punt);
- Belangrijke interne en externe veranderingen en de gevolgen daarvan (0,5 punt);
- Anders (0,5 punt).

Verantwoording (maximaal 6 punten, maximaal 5 punten toekennen bij vraag 44)

43. Is de organisatie op de hoogte van de aangepast RJ 400 Jaarverslag en de gevolgen daarvan voor de verantwoording met betrekking tot het risicomanagement?
- Ja (1 punt);
- Nee (0 punten).

44. Wat rapporteert de organisatie in haar jaarverslag over risico's?

Meerdere antwoorden mogelijk

- Niets (0 punten);
- De belangrijkste risico's (0,75 punt);
- De belangrijkste risico's onderscheiden naar categorie (0,75 punt);
- De risicobereidheid van de organisatie (0,75 punt);
- De genomen maatregelen met betrekking tot de belangrijkste risico's (0,75 punt);
- Een uitleg waarom er geen maatregelen met betrekking tot de belangrijkste risico's genomen zijn (0,75 punt);
- De verwachte impact op de resultaten en/of financiële positie als één van de belangrijkste risico's zich zou voordoen (0,75 punt);
- De zich voorgedane risico's die een belangrijke impact hebben gehad inclusief de gevolgen daarvan (0,75 punt);
- Als deze risico's zich hebben voorgedaan, de verbeteringen die zijn doorgevoerd (0,75 punt);
- De wijze waarop het systeem van risicomanagement is verankerd in de organisatie (0,5 punt);
- De maatregelen die genomen zijn ter beïnvloeding van de cultuur, het gedrag en de motivatie van haar werknemers (0,5 punt).

Afsluitende vraag over risicomanagement

45. Welk cijfer geeft u uw risicomanagementsysteem?

(1 tot en met 10)

- Uw cijfer

Overige vragen

46. Wat is de naam van de organisatie?

Open antwoord

47. Wat is uw naam?

Open antwoord

48. Wat is uw e-mailadres?

Open antwoord

49. Heeft u nog opmerkingen, aanvullingen, en dergelijke?

Open antwoord

Bijlage 12 De gebruikte principes voor de scoreleidraad

De zeventien principes van risicomanagement volgens het COSO Model 2013[173]

Controleomgeving

1. Laat de inzet zien voor integriteit en ethische waarden;
2. Verzeker dat de directie/raad van bestuur toezicht houdt;
3. Stel structuren, rapportage manieren, bevoegdheden en verantwoordelijkheden vast;
4. Laat inzet zien voor een bekwaam personeelsbestand;
5. Houd mensen aansprakelijk.

Risicobeoordeling

1. Specificeer de juiste doelstellingen;
2. Identificeer en analyseer de risico's;
3. Evalueer (fraude)risico's
4. Identificeer en analyseer veranderingen die de interne beheersing in belangrijke mate kunnen beïnvloeden.

Controleactiviteiten

1. Selecteer en ontwikkeling controleactiviteiten die risico verminderen;
2. Selecteer ten ontwikkel technologische maatregelen;
3. Voer de controleactiviteiten uit door beleid en procedures;

Informatie en communicatie

1. Gebruik relevante en kwalitatieve informatie die interne beheersingsfunctie ondersteunen;
2. Communiceer intern informatie intern;
3. Communiceer externe informatie extern.

Monitoring

1. Voer doorlopende of periodieke evaluaties uit op de interne beheersing;
2. Communiceer interne controletekortkomingen.

De zeven principes zoals toegepast in het Tweede Nationaal Onderzoek Risicomanagement in Nederland 2014[174]

6. De periodiciteit/frequentie;
7. Een integrale toepassing;
8. Een bedrijfsbrede toepassing;
9. De mate van pro-activiteit;
10. Het expliciete karakter (vastlegging);
11. De aanpak (methodiek); en
12. Rapportage.

[173] (Rich Milo, John G. Giakouminakis, Traci Mizoguchi, Jimmy Yu, 2013, p. 1)
[174] (Nederlandse Beroepsorganisatie van Accountants (NBA), Nyenrode Business Universiteit, Rijksuniversiteit Groningen, PwC, 2014, p. 65)