Stop met het managen van risico’s!

transcriptie van de presentatie tijdens het IIA jaarcongres in Leusden op 20 juni 2024

1. Wat zeg je me nou?

Als rechtgeaarde internal audit professional doet deze titel natuurlijk onmiddellijk je wenkbrauwen fronsen. Of je nekharen recht overeind staan. Of zelfs je haren ten berge rijzen. Volgens velen hoort het managen van risico’s bij hun vak zoals een caravan bij de zomervakantie.

Zelf werk ik als interimmer, adviseur en trainer. Veel mensen die ik in de praktijk ontmoet vinden stoppen met het managen van risico’s ultradom. Het leiderschap van de organisatie moet juist iets met al die risico's. Dit is ook het onderliggende principe in de internationale standaarden voor risico- en auditmanagement.

Volgens veel experts en hun volgelingen kan en moet risicomanagement worden geïmplementeerd. Volgens hen is het zeer onverstandig om dat niet te doen. Het managen van risico’s behoedt je voor onnodige valkuilen en bovenal helpt het je om je doelen te bereiken.

Volgens de Global Internal Audit Standards (GIAS) versterkt internal auditing de goverance-, risicomanagement- en beheersprocessen. Internal audit wordt verondersteld de effectiviteit ervan te evalueren en bij te dragen aan de verbetering.

In de afgelopen jaren is het begrip van het omgaan met onzekerheid echter aanzienlijk veranderd. In deze sessie komen recente inzichten aan de orde en de implicaties voor internal auditors.

Met het managen van risico’s zijn nogal wat mensen in weer. In de wereld van risicomanagement krijgen zij allerlei rollen toebedeeld. Denk aan degenen die door hun collega's van Risk Management zijn aangewezen als 'risico-eigenaar'.

Weer anderen verdienen hun brood als interne risicomanagers, risk officers en risicoanalisten. En dan hebben we het nog niet eens over de talloze externe risicoadviseurs en leveranciers van risicomanagement software.

Risk consultants blijven ze verkopen en veel organisaties blijven ze maar kopen: risicoraamwerken, risicobeleidstukken, risicoanalyses, risicoregisters, risicodashboards en ga zo maar door. Al deze instrumenten zijn doorgaans ontworpen om individuele risico's of afzonderlijke risicocategorieën te identificeren, te analyseren, te mitigeren en te monitoren.

Leidinggevenden worden geacht om na te gaan wat er in de toekomst allemaal mis kan gaan. Genoemd worden de strategische, operationele, compliance en verslaggevings-risico’s. In de praktijk worden daar flinke lijsten van gemaakt: risicoregisters, risicoportfolio’s of risicodossiers.

Tim Leech en anderen noemen deze aanpak ‘risk list management’. De onderliggende overtuiging en het uiteindelijke doel is om onheilen zoveel mogelijk te beperken en narigheden te bestrijden. Alexei Sidorenko wijst er in zijn boek 'Guide to effective risk management’ op dat het niet gaat om het beheersen van risico's, maar om het nemen van betere beslissingen.

Als risicomanagement het antwoord is, wat was dan ook alweer de vraag? Hoe goed helpen de gebruikelijke benaderingen besluitvormers om te gaan met onzekerheden, disrupties en dilemma's?

Of is het meer een geloofssysteem? Zouden er missionarissen, gelovigen en inquisiteurs zijn die serieuze commerciële belangen hebben bij het instand houden van dit omvangrijke ecosysteem?

De ontwikkelingen die we nader gaan bekijken zijn op hoofdlijnen als volgt:

- van risico's managen en mogelijke onheilen afweren;
- via beslissingen nemen onder onzekerheid en de kansen op succes inschatten;
- naar belangen van stakeholders afwegen en dilemma's verzoenen.

2. Hoe hebben internal auditors te maken met risicomanagement?

Het managen van risico's staat centraal in het werk van internal auditors. Zij moeten zelf risicogebaseerde audits doen. Daarbij worden zij geacht om assurance en advies te geven met betrekking tot het beheersen van de belangrijke risico's door de geauditeerden.

Internal auditors helpen het management om te begrijpen in hoeverre hun risicobeheerprocessen toereikend zijn. Volgens de Global Internal Audit Standards moeten zij inzicht krijgen in de te auditeren activiteiten om de relevante risico's te kunnen beoordelen.

Het 'Three Lines Model' is erg populair. Althans bij internal auditors vanwege de rechtvaardiging van hun eigen onafhankelijke positie. Het is een intern beheerssysteem voor het verduidelijken van risico-eigenaarschap: wie er is verantwoordelijk voor het managen van de risico's? In de praktijk lijkt dit model vooral gedoe op te leveren. Over wie al dan niet bij welke lijn hoort en wat die al dan niet mag of moet doen.

De eerste lijn wordt geacht de risico's te managen. Zij vormen de uitvoerende macht. In sporttermen zijn ze de spelers. De tweede lijn wordt gevormd door specialisten die verstand hebben van compliance en risicomanagement. Zij vormen de wetgevende macht. Ze zijn de architecten van het beheerssysteem. In sporttermen heb je het dan over de coaches die de spelregels uitleggen.

Internal audit is de derde lijn, die als rechterlijke macht een oordeel velt over wat er in de praktijk van terecht komt. In sporttermen zijn zij de scheidsrechters. Hun rol omvat het geven van onafhankelijke en objectieve assurance en advies over alle zaken met betrekking tot het realiseren van de doelstellingen. In de praktijk komt dat vaak neer op het rapporteren van 'major deficiencies' in de interne beheersing.

De tweede lijn lijkt in werkelijkheid vaak op de 'vierde macht': de ambtelijke burocratie. Overigens vinden sommigen dat de tweede lijn wordt gevormd door alle bedrijfsvoeringsfuncties. Deze staffuncties stellen organisatiebreed beleid op met betrekking tot personeelszaken, informatievoorziening, financiën, facilitaire zaken et cetera.

Naast expertise biedt de tweede lijn ook ondersteuning. In de praktijk beperken ze dat doorgaans tot het over de schutting werpen van het opgestelde beleid. Als lijnmanager hoop je juist dat zij de mouwen opstropen en jou komen helpen bij het doorvertalen van het beleid naar passende procedures in jouw processen. Sommigen vinden dat de tweede

lijn bovendien een inspectierol heeft: ook monitoren en aanspreken worden tot hun vaste taken gerekend.

De Global Internal Audit Standards (2024) definiëren risicomanagement als: 'a process to identify, assess, manage and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives'.

Dit is in lijn met COSO ERM (2004) dat risicomanagement eveneens definieerde als een proces. Als je dat nog niet geïmplementeerd had, stonden de consultants inclusief ikzelf in de rij om je daarbij te helpen.

Een relevante en interessante observatie is dat in COSO ERM (2017) risicomanagement niet langer wordt beschouwd als een proces, maar is geherdefinieerd als: 'the culture, capabilities and practices that organizations rely on to manage risk'.

Ook volgens ISO 27001 moet je een risicobeoordeling uitvoeren om mogelijke bedreigingen te identificeren. Vervolgens moet je beheersmaatregelen implementeren om ze te mitigeren. Gevolgd door reviews en audits om na te gaan of je blijft voldoen aan de normen.

Dit wordt ook wel aangeduid als de 'ORCA'-benadering. Als je weet wat je wilt ('objectives'), uitvoerig bedenkt wat er mis zou kunnen gaan ('risks'), passende maatregelen implementeert ('controls') en zekerheid verkrijgt dat deze werken ('assurance'), dan zal de werkelijkheid zich ontvouwen zoals gewenst. Dit ontaardt al snel in een illusoire wereld van interne beheersing. In deze wereld is ongepland succes een onaangename ervaring.

Beheersmaatregelen spelen in deze benadering een belangrijke rol. Die moeten namelijk de risico's mitigeren. Als je dat werkwoord hoort, weet je dat het over conventioneel risicomanagement gaat. Dat wil zeggen: risicomanagement zoals het in de praktijk doorgaans wordt vormgegeven. Bij het beoordelen van die beheersmaatregelen moet je uiteraard allerlei inschattingen maken van hun adequaatheid en effectiviteit.

Over het geheel wordt dan periodiek gerapporteerd aan de directie en toezichthouders. Zij ontvangen informatie over 'the state of risk'. Deze benadering kom je veel tegen. Let wel, je hebt het over staffunctionarissen die jou als lijnmanager zouden moeten ondersteunen. In de praktijk komen ze vooral informatie bij jou ophalen die jij dan later – gegoten in hun format - in periodieke rapportages kunt teruglezen.

De nieuwe Verklaring Omtrent Risicobeheersing ademt de geest van risicobeheersings- en controlesystemen. Het bestuur van de vennootschap is verantwoordelijk voor het identificeren en beheersen van de risico's verbonden aan de strategie en de activiteiten. In het jaarverslag moet het bestuur een beschrijving opnemen van de belangrijkste risico's.

Een meer 'old school' benadering van risicomanagement dan dit vind je nauwelijks. Om de belangrijkste risico's te vinden wordt er veel belang gehecht aan volledigheid. Stel je voor dat je een risico vergeet dat belangrijk kan zijn. Daardoor worden die risicolijsten niet alleen lang, maar ook al gauw breed: vele kolommen in een spreadsheet.

Het bestuur dient de opzet en de werking van de interne risicobeheersings- en controlesystemen te monitoren. Het voert ook ten minste jaarlijks een systematische beoordeling uit van de opzet en de werking van die systemen.

Heeft formeel risicomanagement waarde anders dan het geruststellen van toezichthouders? Is er afgezien van het voldoen aan compliance vereisten iets in risicomanagement dat niet al deel uitmaakt van het dagelijkse management?

Omgaan met onzekerheid is inherent aan het dagelijks werk. Er is geen management zonder onzekerheid. Besluitvorming gaat over het analyseren en afwegen van potentiële voor- én nadelige effecten van keuze-opties op datgene waar de kernstakeholders waarde aan hechten. Als je gaat beleggen, dan ben je hopelijk niet alleen bezig met mogelijke verliezen, maar ook met potentiële rendementen.

Heeft het zin om eerst allerlei ERM-attributen te ontwikkelen en te implementeren (zoals risicoregisters, risicobehandelplannen, risicorapportages et cetera) en vervolgens te proberen deze parafernalia te integreren in de reguliere werkwijzen?

Of is het verstandiger om:

- risicomanagement te vergeten - afgezien van compliance doeleinden;
- het perspectief van de besluitvormers en hun dilemma's als uitgangspunt te nemen;
- hen waar mogelijk te helpen om de verwachtingen van hun kernstakeholders te managen?

3. Wat is de oorsprong van de conventionele risicomanagementpraktijken?

De verzekeringssector heeft een voorname rol gespeeld in de ontwikkeling van risicomanagement. Zij helpen hun klanten om zich te beschermen tegen mogelijke narigheden. Denk aan brand-, ongevallen- of arbeidsongeschiktheidsverzekeringen. Zij verkopen polissen die bescherming bieden tegen kwantificeerbare mogelijke onheilen.

In de context van beursintroducties kwamen in de jaren zestig de eerste vereisten van de Securities and Exchange Commission voor het opnemen van risicofactoren in de documenten. In 2005 kwamen er eisen om ze op te nemen in jaar- en kwartaalverslagen.

Dit betreft factoren die aandelen speculatief maken voor aandeelhouders. Hieruit ontstond de eis om een 'Risk Management Framework' te hebben: een samenhangend geheel van risico-identificatie, -analyse, -mitigatie en -monitoring. Allemaal gericht op het voorkomen van financiële verliezen voor de betrokkenen.

Interne specialisten en externe consultants gebruikten vervolgens risicobeoordelingen en -behandelingen om organisaties te helpen om ongewenste uitkomsten te beperken. Dit leidde tot het ontwikkelen en codificeren van methoden en best practices.

Uitgebreide maturiteitsmodellen resulteerden in meer toeters en bellen. Er werden talloze speciale ERM-, GRC- en ESG-toepassingen ontwikkeld. Hoe meer de risicomanagement-praktijken verplicht werden, des te lucratiever de verdienmodellen van de adviseurs werden. Het is nu een multimiljoenen sector met dito belangen.

Door de jaren heen werd risicomanagement steeds meer behandeld als een op zichzelf staand proces en functie. In de financiële sector kwamen wetgevers en regelgevers zelfs met een risicomanagementfunctie die onafhankelijk moet zijn van het management. Dit is een sheriffachtige rol die cowboys met foute intenties op het rechte pad moet houden.

Je moet je wel afvragen hoe realistisch het is om te denken dat je met een zwerm risk managers en compliance officers de echte 'bad boys' en 'bad girls' op het rechte pad kunt

houden. Als leidinggevenden en medewerkers alleen gewaardeerd en beloond worden voor hun commerciële prestaties, dan delven compliance en moraliteit al snel het onderspit.

Je kent zelf ook vast mensen met kernwaarden als:

- 'Als ze niet willen dat wij dit doen, dan moeten ze het maar verbieden.'
- 'Boetes van toezichthouders moet je gewoon zien als bedrijfskosten.'
- 'Zolang wij niet zijn gepakt hebben we officieel niks verkeerds gedaan.'

Om de huidige risicomanagementpraktijken te begrijpen, moeten we ook teruggaan naar de oorsprong van de risicoregisters. Deze risico-inventarisatielijsten werden gemeengoed in fabrieken in de jaren '70. Daar was men begonnen met het gebruiken van overzichten met aandachtspunten ten aanzien van de veiligheid van de werknemers.

Toen er steeds meer regelgeving kwam op dit gebied werden die lijsten vooral gebruikt om de aandacht te vestigen op mogelijke gevaarlijke situaties. Deze lijsten kregen al snel een functie in het kader van compliance: ze waren handig voor de inspecteurs die de bedrijven kwamen controleren.

Overheden, regelgevers en toezichthouders omarmden vervolgens deze werkwijzen als methoden om aan te tonen dat organisaties hun zaken op orde hebben. Ze verwachten dat interne toezichthouders de risicolijsten reviewen. 'Risicomanagement bedrijven' (lees: risicolijsten bijhouden en toprisico's benoemen) werd gaandeweg beschouwd als een kenmerk van goed organisatiebestuur.

4. Wat is er vooral problematisch aan conventioneel risicomanagement?

Recente inzichten onderstrepen aanzienlijke problemen met de gebruikelijke benaderingen. Roger Estall en Grant Purdy concluderen in hun boek 'Deciding' dat risicomanagement een molensteen is die om de nek van organisaties hangt. Volgens hen kan de organisatieleiding zich er beter van ontdoen.

Het begint al met het kernbegrip 'risico'. Waar hebben we het dan eigenlijk over? Er bestaat helaas geen universele definitie van. Veelbetekenend is het dat ISO – nota bene dé internationale organisatie voor standaardisatie – in haar eigen documenten zelf meer dan 40 verschillende definities van risico gebruikt.

Als mensen het woord 'risico' bezigen, kunnen ze uiteenlopende zaken bedoelen:

- de kans op een (ongewenste) gebeurtenis, zoals een fraudegeval;
- de oorzaak van de gebeurtenis, ook wel 'risicofactor' genoemd, zoals een medewerker die gokverslaafd is;
- de gebeurtenis zelf, zoals het ontvreemden van geld of goederen;
- het gevolg van de gebeurtenis, ook wel 'impact' of 'effect' genoemd, zoals de kosten voor juridische procedures.

Weer anderen bedoelen de volatiliteit van de verwachte uitkomsten, als zij het over 'risico' hebben.

De oorzaken en de gevolgen zijn op zichzelf ook gebeurtenissen. Het hele leven bestaat uit ketens van voorvallen en omstandigheden die op elkaar inwerken. Er zijn dan ook experts die erop wijzen dat risico niet gaat over dingen die kunnen gebeuren, maar juist over de relaties tussen gebeurtenissen die kunnen optreden.

In COSO IC (2013), COSO ERM (2004) en in de volksmond verwijst 'risico' naar iets negatiefs: mogelijk verlies. Bijvoorbeeld: iets wat je geld kan kosten, slecht kan zijn voor je gezondheid of je in diskrediet kan brengen. Risico is dan de maatstaf voor de waarschijnlijkheid en de ernst van nadelige effecten.

De ISO 31000 Risk Management Guidelines (vanaf de start in 2009) en COSO ERM (2017) hanteren daarentegen een neutraal risicobegrip. Het gaat om zowel positieve als negatieve effecten op het behalen van de doelstellingen. Risico is dan een onzeker gevolg van een gebeurtenis of activiteit met betrekking tot iets wat mensen waardevol vinden.

Deze verandering had verstrekkende gevolgen. Oorspronkelijk gebruikte COSO vier zogenaamde 'risk responses': 'Accept', 'Avoid', 'Reduce', 'Share' voor mogelijke narigheden. In 2017 voegde COSO 'Pursue' toe als vijfde smaak: 'accept increased risk to achieve improved performance'. Dit is meer in lijn met het gangbare concept van het in evenwicht brengen van risico en rendement.

COSO nam in 1992 met het Internal Control framework een fatale afslag door aan te geven dat 'opportunities' geen onderdeel vormen van interne beheersing, maar moeten worden teruggeleid naar het doelstellingsbepalingsproces.

Aanvankelijk hanteerden ze er een inituïtieve definitie voor: 'the possibility that an event will occur and positively affect the achievement of objectives'. Voor 'risico' hadden ze een gelijkluidende definitie. In plaats van 'positively' gebruikten ze 'adversely'.

Toen ze later in de 2017 editie van COSO ERM de definitie van risico neutraal hadden gemaakt, kwamen ze met een hele andere definitie van 'opportunity': 'an action or potential action that creates or alters goals or approaches for creating, preserving and realizing value'. Dat is niet hetzelfde als ISO's definitie van 'opportunity': 'combination of circumstances expected to be favorable to objectives'.

Het feit dat het begrip 'risico' zeer verschillende betekenissen heeft, impliceert dat het simpelweg gebruiken van de term al een bron van verwarring is. De traditionele focus ligt op wat er mis kan gaan. Dit is bepaald niet holistisch.

Als je gaat solliciteren, ben je niet alleen bezig met de kwade kans dat je een nare bovengeschikte krijgt, een beroerde werk-privébalans hebt en dat je kunt worden ontslagen, maar ook met gave ontplooiingsmogelijkheden, boeiende opdrachten en inspirerende collega's.

Als je daarentegen de neutrale definitie gebruikt, die zowel 'upside risks' als 'downside risks' omvat, raak je de meeste mensen in je publiek meteen kwijt. Voor hen heeft 'risico' een negatieve connotatie.

Vanwege al deze verwarring stellen sommige opinieleiders voor om het 'R-word' te mijden. Als je het hebt over kansen en bedreigingen, weet iedereen wat je bedoelt. Mogelijke alternatieven voor risicomanagement zijn bijvoorbeeld onzekerheids-management, succesmanagement of verwachtingsmanagement.

Hetzelfde geldt voor waardemanagement. Zowel COSO als ISO geven aan dat het doel van risicomanagement is het creëren en beschermen van waarde. De term houdt er nadrukkelijk rekening mee dat verschillende stakeholders waarde hechten aan verschillende zaken. Begrippen als 'waarde', 'succes' en 'resultaat' zijn op zich inhoudsloos. Je moet eerst verduidelijken wat je bedoelt, zoals veiligheid, rendement en punctualiteit.

Beslissers moeten - bewust van de afhankelijkheden en de mogelijke consequenties - keuzen maken onder onzekerheid en dilemma's verzoenen. Volgens ISO 31000 is risicomanagement effectief, als het onderdeel is van de besluitvormingsprocessen. Daar zijn echter geen aansprekende praktijkvoorbeelden van bekend.

Risicomanagement kenmerkt zich door een steeds uitdijend jargon. Zo pleiten sommigen ervoor om 'risicodialogen' te gaan voeren. Andere voorbeelden zijn:

- 'risk goverance', terwijl de taken, bevoegdheden en verantwoordelijkheden al in de reguliere governance zijn geregeld;
- 'risk culture' naast de bestaande normen, waarden en gedragingen;
- 'risk owner' terwijl er al mensen verantwoordelijk zijn voor het bereiken van de resultaten;
- 'risk intelligence' naast de aanwezige bedrijfsinformatie;
- 'risk reporting' terwijl - als het goed is - er in de prognoses al wordt uitgegaan van relevante sterkten en kansen, zwakheden en dreigingen.

Het grote nadeel van al het jargon is dat gewone mensen denken: dit lijkt over iets heel anders te gaan dan mijn dagelijkse werk; hier heb je aparte deskundigen voor nodig. Een separate risicomanagement afdeling leidt ertoe dat andere collega's al snel zeggen: als je vragen hebt over risico's, dan moet je bij hunnie zijn, want die zijn d'r van.

In dit verband moeten we het ook even hebben over 'risicomanagers'. Management gaat over het inzetten van schaarse mensen en middelen om - door middel van beleid, processen en procedures - producten en diensten voort te brengen die voldoen aan de vereisten en verwachtingen. Een risicomanager managet niks, maar faciliteert, analyseert en rapporteert slechts.

Conventionele benaderingen focussen op het tot een aanvaardbaar nivo terugbrengen van individuele risico's of risicocategorieën door middel van beheersmaatregelen. Ook de nieuwe Global Internal Audit Standards gaan uit van deze benadering. Als het management een risiconivo heeft geaccepteerd dat de risicobereidheid van de organisatie te boven gaat, moet de kwestie met het senior management worden besproken.

Dit gaat over een van de kroonjuwelen van conventioneel risicomanagement: het 'risk appetite statement'. Het is een typisch COSO ERM begrip: 'the types and amount of risk that an organization is willing to accept in pursuit of value'.

ISO 31000 gebruikt de term zelf niet, maar heeft het over: 'the amount and type of risk that it may or may not take'. Risico nemen heeft een andere connotatie dan risico accepteren.

Maar wacht eens even. Waar hebben we het eigenlijk over bij 'amount of risk'? We hebben daar helemaal geen meeteenheid voor. Bij risicoprofielen wordt wel gesuggereerd dat je voor het gemak allerhande verschillende risico's kunt aggregeren.

De risicobereidheidsuitspraken zijn bedoeld om beslissers te helpen om mogelijke voor- en nadelen af te wegen. En om niet meer nadelige effecten te veroorzaken dan zij zich kunnen veroorloven. Maar helpen ze daadwerkelijk?

Zeggen dat je een lage risicobereidheid hebt, klinkt misschien stoer of geruststellend, maar heeft weinig praktische betekenis. Wat houdt 'laag' precies in en hoe weet je of je daadwerkelijke risicoblootstelling inderdaad 'laag' is?

De uitspraken zijn veelal gebaseerd op de oude negatieve definitie van risico: mogelijke narigheid. Het concept 'risicobereidheid' werkt hooguit enigszins bij financiële afwegingen, zoals het verstrekken van verzekeringen of leningen. Die zaken kun je in geld uitdrukken. Het werkt niet goed in het geval van bijvoorbeeld compliance of veiligheidsdoelstellingen.

De uitspraken zijn statisch, terwijl de werkelijkheid dynamisch is. Het ene moment kan het met de beschikbare kennis verstandig zijn om een risico te nemen, terwijl dat een paar weken later niet meer het geval is. Tolerantie is een beter hanteerbaar begrip: de bandbreedte van de aanvaardbare uitkomsten van een belangrijke doelstelling.

Spreken over hoeveel verlies je bereid bent te accepteren moet je steeds zien in samenhang met het mogelijke voordeel dat eraan verbonden is. Het heeft weinig zin om een lijst met risico's te mitigeren los van de mogelijke voordelen. Bij het maken van afwegingen heb je dan ook meer aan risicobewustheid dan aan risicoafkerigheid.

Een praktijkvoorbeeld van lastige afwegingen op de werkvloer. Als je leidinggevende bent in een distributiecentrum, moet je een aanvaardbare balans vinden tussen botsende belangen. Denk aan commercie versus compliance of veiligheid.

De gecertificeerde heftruckchauffeurs zijn al naar huis. Er moeten dringend pallets met goederen worden geladen voor een belangrijke klant. Sta je toe dat een niet-gecertificeerde chauffeur de vorkheftruck bedient?

- Als het goed afloopt, ben je een bewonderde pragmaticus. Toegegeven, je overtreedt de regels, maar het is voor het grotere goed. Nood breekt wetten.
- Als het fout gaat, ben jij een onverantwoordelijke manager. Die regels zijn er niet voor niets.

Helpen de gangbare risicomanagement praktijken je om hier een professionele afweging te maken?

Wat is er nog meer problematisch aan conventioneel risicomanagement? Wat we ons wellicht niet altijd realiseren is dat kansen en bedreigingen onze mentale beelden zijn van mogelijke toekomstige gebeurtenissen, veranderingen in omstandigheden en trends.

Deze beelden worden sterk beïnvloed door onze persoonlijkheden, inzichten en ervaringen. Bovendien hebben wij als mensen veel last van vooringenomenheden en denkfouten zoals Daniel Kahneman en anderen hebben aangetoond.

Er bestaat geen wetenschap die 'risicologie' heet. Wat we wel hebben is een op zichzelf staande risicomanagementwereld met allerlei door consultants aanbevolen praktijken. Die werkwijzen moeten vervolgens worden geïntegreerd in het bestaande management-systeem. De kans om succesverhalen tegen te komen vrijwel nihil.

Risicomanagement wordt in de praktijk vaak kwalitatief ingestoken. Risico's worden dan met woorden omschreven. In tegenstelling tot kwantitatieve benaderingen waarbij risico's getalsmatig worden uitgedrukt.

Als er aan ingeschatte waarschijnlijkheden en effecten punten worden toegekend, is er sprake van een hybride vorm. Die punten zijn waarden op ordinale schalen (bijvoorbeeld van 1 tot en met 5 of 6). Dit type schalen wordt ook gebruikt bij opiniepeilingen of om door middel van een aantal sterren de kwaliteit van hotels uit te drukken.

Als je wordt gevraagd om toprisico's te benoemen, is een risicoregister handig. Met het grootste gemak worden de toegekende waarden voor kans en effect met elkaar vermenigvuldigd in Excel. Of je mooie GRC applicatie doet dat voor je. En zo krijg je dan je

gevraagde toprisico's. Ordinale waarden kun je echter niet probleemloos met elkaar vermenigvuldigen om risicoscores te berekenen.

De risico's worden vervolgens op basis van de ingeschatte waarden in de bekende 'heatmap' geplot. Het 'Probability Impact Diagram' is voor velen hét symbool voor het managen van risico's. Met twee assen: voor waarschijnlijkheid en impact. Met kleuren per vakje in het raster.

Het risicodiagram blijft een verleidelijk instrument. Het is visueel, eenvoudig en intuïtief: groen is goed en rood is fout. Toch kun je het beter niet gebruiken, want het is erg misleidend. Een paar overwegingen:

a. De focus ligt ten onrechte op risico's of risicocategorieën. De aandacht moet uitgaan naar de verwachte mate van realisatie van doelstellingen. Of nog scherper: naar het vinden van een balans tussen botsende belangen.
b. Het is een ernstige oversimplificatie van de werkelijkheid. De punten in het raster suggereren een exactheid die niet bestaat.
c. Er wordt uitgegaan van enkelvoudige punten, terwijl er sprake is van verdelingen: reeksen van mogelijke uitkomsten, elk met een bepaalde kans. Neem het betaalgedrag van klanten. Het kan gaan over grotere of over kleinere bedragen met verschillende waarschijnlijkheden.
d. Het is gericht op negatieve zaken, terwijl succes afhangt van kansen benutten én bedreigingen beperken.
e. Risico's inschatten met behulp van kleuren en termen als zelden of mogelijk, laat staan als hoog, midden en laag, is een heilloze weg. Het is sterk subjectief, volstrekt arbitrair en niet gebaseerd op empirische data.
f. Het betreft individuele risico's of afzonderlijke risicocategorieën en gaat voorbij aan de onderlinge afhankelijkheden ertussen.
g. Onduidelijk blijft welke impact de geplotte risico's hebben op de realisatie van welke doelstellingen.
h. De risico's in de rechterbovenhoek, de rode risico's met hoge waarschijnlijkheid én ernstige gevolgen, worden wel 'fantoomrisico's' genoemd. Hoge kans betekent dat iets vaak voorkomt en hoge impact betekent 'game over'. De rechterbovenhoek geeft aan dat je naar verwachting wekelijks failliet gaat.
i. Als er belangrijke beslissingen moeten worden genomen, worden de 'heatmaps' niet geraadpleegd.

Het is een valkuil om te denken dat kwantitatieve analyses objectief en superieur zijn en dat kwalitatieve analyses subjectief en inferieur zijn. Kwantitatieve analyses kunnen gemakkelijk gebaseerd zijn op ondeugdelijke aannames. Ook bij modellen is er altijd sprake van subjectiviteit.

Bij kwantitatieve benaderingen wordt geprobeerd om onzekerheid uit te drukken in geld (zoals 'value at risk', 'cashflow at risk' en 'earnings at risk'). Dat kan in specifieke gevallen nuttig zijn. Als je risiconivo probeert uit te drukken op basis van geldwaarde, zul je wel al gauw ontdekken dat wat je het meeste waardeert in je leven lastig is uit te drukken in geld.

Risicokwantificering (getalsmatige beschrijving) is sterk afhankelijk van de veronderstelde parameters in het model en van de kwantiteit en kwaliteit van de beschikbare data. Als de gebruikte veronderstellingen niet langer geldig zijn, vervalt de waarde van het model.

Bovendien blijven het slechts modellen, sterke vereenvoudigingen van de werkelijkheid. Een kaart is niet het gebied dat het weergeeft. Bovendien ontbreken vaak de tijd en informatie om bruikbare modellen op te stellen.

Naarmate de vraagstukken groter en ingewikkelder worden, neemt niet alleen de onzekerheid, maar ook de subjectiviteit toe. Er zijn immers zoveel actoren en factoren die van invloed zijn op wat er kan gebeuren. Je kunt die nooit allemaal in je model opnemen. De complexiteit overstijgt al snel onze menselijke vermogens. Persoonlijke visies en opvattingen gaan dan de kans, impact en urgentie bepalen.

In de praktijk gaat het nooit over één doelstelling. Ja misschien in het oude 'shareholder value' denken: zoveel mogelijk waarde (bijvoorbeeld dividend) realiseren voor de aandeelhouders.

Vanwege de focus op aandeelhouderswaarde werden risico's vooral gezien als bedreigingen van het winstpotentieel. We hebben met z'n allen gezien tot welke ontsporingen de insteek 'geld als doel' in plaats van 'geld als middel' heeft geleid.

Denk overigens niet dat dit alleen speelt in commerciële omgevingen. Bij sommige gemeenten lijkt de geldgedreven planning- & controlcyclus het primaire proces te zijn. Als je weinig presteert, maar netjes binnen je budget blijft, heb je minder problemen dan wanneer je je budget overschrijdt om waardevolle dingen te doen voor de burgers.

Er zijn opinieleiders die aangeven dat risicomanagement zich vooral met modelleren en kwantificeren zou moeten bezighouden. De vraag is wat je hier aan hebt, als er echte keuzen gemaakt moeten worden.

Het wordt pas interessant, als er (ethische) dilemma's zijn. Als er sprake is van mogelijke positieve én negatieve gevolgen voor niet-gelijksporende belangen. Als er gekozen moet worden tussen botsende belangen.

Veel leidinggevenden zien risicomanagement primair als een compliancekwestie. De nieuwe Corporate Sustainability Reporting Directive verplicht organisaties om uitgebreid te rapporteren over duurzaamheidsrisico's. En in de Corporate Goverance Code nemen we een nieuwe verplichte Verklaring Omtrent Risicobeheersing op.

Commercieel gezien is het ESG-circuit (of: circus) overigens uiterst lucratief. Een echte compliance goudmijn. Je kunt eerst aardig verdienen met het opstellen van normen en standaarden. Daarna kun je fors vangen voor ondersteuning bij de implementatie en vervolgens loop je binnen op het controleren van de naleving.

Vanwege hun rol zijn toezichthouders nauwelijks geïnteresseerd in de 'upside' van risico. Het is hun taak om de keerzijde te minimaliseren. Voor bestuurders betekent effectief risicomanagement vooral dat ze niet in de problemen komen met hun externe of interne toezichthouders.

Risk consultants proberen aan deze compliance focus te ontsnappen. In snel veranderende tijden, zo stellen zij, moeten bestuurders als stuurlui effectief navigeren in woelige wateren. Het begrijpen en beheren van risico's is daarbij noodzakelijk voor effectief leiderschap. Ziedaar de business case voor het implementeren van risicomanagement.

Tijdens trainingen wordt commissarissen geleerd om te vragen naar de top tien risico's. Dat is blijkbaar een teken dat het management goed heeft nagedacht over de kwetsbaarheden van de organisatie als basis voor het nemen van passende maatregelen.

Opvallend is dat je ondernemers, lijnmanagers of projectleiders zelden tegenkomt bij risicomanagement trainingen, webinars en conferenties. Dit is best bijzonder, aangezien de standaarden beloven dat risicomanagement hen in staat stelt om hun doelstellingen beter te realiseren. De meesten van hen zijn niet achterlijk. Als het hen echt zou helpen, zouden zij dan niet op de eerste rij zitten te popelen om te leren hoe ze er hun voordeel mee kunnen doen?

We hebben gezien dat het volgens de conventionele aanpak verstandig is om iets aparts te implementeren, 'risicomanagement' geheten, gericht op het tegengaan van geïdentificeerde potentiële narigheden.

Om onheilen af te weren moet je investeren in het identificeren, analyseren, mitigeren en monitoren van risico's. Individuele risico's (of risicocategorieën) moeten op het gewenste nivo gehouden worden. Om effectief te worden moeten de risicomanagement parafernalia geïntegreerd worden in het bestaande managementsysteem.

De nadruk ligt op het je druk maken over het mitigeren van mogelijke onheilen en niet op het beslissers helpen om succesvol te worden en te blijven. In goed Nederlands: het optimaliseren van de 'risk-return balance'. Dat ben je uiteraard niet mee bezig, als je alleen aandacht hebt voor de 'downside'.

Helpt het gebruikelijke risicomanagement besluitvormers echt om met hun dilemma's om te gaan? De realiteit is dat het is verworden tot verantwoordingsinstrument. Dat is iets heel anders dan een hulpmiddel om te proberen om je doelen te bereiken onder onzekerheid.

5. Wat is de essentie van de nieuwe inzichten?

Recente inzichten in het omgaan met de onzekere toekomst zijn niet gericht op risico's. De focus ligt op de realisatie van de organisatiedoelstellingen onder onzekerheid. Wat je als beslisser wil weten is: hoe waarschijnlijk is het dat ik mijn doelstellingen ga realiseren?

Verschillende stakeholders hechten waarde aan uiteenlopende zaken. Als besluitvormer moet je daarom omgaan met de potentieel botsende belangen van je stakeholders. De focus verschuift naar besluitvorming, naar keuzen maken, naar de kwaliteit van de belangenafwegingen onder onzekerheid.

Het is verstandiger om te beginnen vanuit het perspectief van de besluitvormers. Wat zij moeten weten is: wat is de waarschijnlijkheid dat ik in staat ben om te creëren én te beschermen waar mijn belangrijkste stakeholders waarde aan hechten?

Recente inzichten gaan daarom uit van het perspectief van de besluitvormers. Zij moeten zich niet richten op het managen van risico's, maar op het managen van de business, op het managen van de verwachtingen van hun kernstakeholders.

Het doel van analyses wordt dan om de beslissers te helpen om op een afhankelijkheids- en consequentiebewuste manier vooruit te kijken. En om daarbij rekening te houden met de mogelijke gevolgen van hun handelen of nalaten voor de belangen van hun stakeholders.

Als leidinggevende ben je bezig met toekomstbestendigheid. Dat gaat over continuïteit – op kortere en langere termijn. 'Resilience', kunnen blijven voortbestaan, betekent dat je organisatie tegen een stootje kan. Denk aan digitale weerbaarheid. Dat vergt eigenschappen als flexibiliteit, wendbaarheid en improvisatievermogen.

Hoe verder je als bestuurder vooruit kunt kijken en hoe breder je gezichtsveld is, hoe beter je kunt anticiperen. Hoe vlotter en veiliger je de organisatie door de onoverzichtelijke bochten van de samenleving kunt loodsen. Deze taken, activiteiten en verantwoordelijkheden maken integraal deel uit van je gewone managementverantwoordelijkheden.

De toekomst is onvoorstelbaar onvoorspelbaar. Het enige wat je kunt doen is zo goed mogelijk gefundeerde afwegingen maken en die waar nodig bijstellen. Als er slechts beperkte tijd beschikbaar is, moet je op je gevoel en intuïtie beslissingen nemen.

Handelen en daarvan af zien hebben voor- en nadelen. Als besluitvormer moet je proberen om die in te schatten voor je verschillende opties om ze vervolgens tegen elkaar af te wegen.

Er is niets in het leven dat alleen maar voordelen heeft. Er zijn ook altijd potentiële of daadwerkelijke nadelen. Als je voor een optie kiest vanwege de vermeende pro's, moet je nog steeds kunnen omgaan met de bijbehorende cons.

Neem bijvoorbeeld het kopen van een huis. Huiseigenaarschap brengt niet alleen voordelen met zich mee, zoals vermogensopbouw, meer vrijheid om het aan je eigen smaak aan te passen en lagere maandelijkse lasten dan huren.

Het is essentieel om ook de mogelijke nadelen in overweging te nemen. In wezen speculeer je met geleend geld als je een hypothecaire lening hebt. Je kunt ook in de ongelukkige situatie terechtkomen dat je te maken krijgt met verzakkende funderingen of akelige buren.

Norman Marks benadrukt het belang van focussen op het vergroten van de kans op succes, bijvoorbeeld in zijn boek 'Risk Management in Plain English: A Guide for Executives'. Het periodiek bijwerken van een lijst met dingen die fout kunnen gaan is niet hetzelfde als nagaan hoe je het beste je doelen kunt bereiken onder onzekerheid.

Evenwichtige besluitvorming vereist dat er ook rekening wordt gehouden met ongewenste informatie. Marketing is een ingenieus vak met krachtige beïnvloeding- en framingtechnieken.

Als beslisser moet je je ervan bewust zijn dat mensen er belang bij hebben om de voordelen te markeren en de nadelen te maskeren. Als internal auditor, maar ook privé, doe je er goed aan om je steeds af te vragen: wie heeft er belang bij dat ik dit voor waar aanneem?

Afzonderlijk risicomanagement ontaardt gemakkelijk in een illusoir compliance-gedreven systeem. Waarom zou je eerst een apart risicomanagementsysteem opzetten en vervolgens proberen om het te integreren in je bestaande managementsysteem? In de afgelopen 20 jaar ben ik daar geen succesverhalen van tegengekomen.

Het blijft opmerkelijk dat veel mensen - afgezien van compliancevereisten - nog steeds geloven dat het waardevol is om risico-inventarisaties bij te werken. Hetzelfde geldt voor het oeverloos tijd besteden aan het beoordelen van risiconivo's.

In plaats van te focussen op de 'risicostatus' zouden leidinggevenden zich moeten bekommeren om het vergroten van de kans om te presteren conform de verwachtingen van hun belangrijke stakeholders.

Het gaat niet om het managen van individuele risico's. Het gaat niet om het beter halen van individuele organisatiedoelstellingen. Het gaat om het omgaan met tegenstrijdige belangen van kernstakeholders en om het verzoenen van dilemma's.

Risicomanagement dient in de praktijk vooral om toezichthouders gerust te stellen. Instrumenten als risicoregisters en 'heatmaps' zijn bedoeld om de 'state of risk' voor de toprisico's te presenteren. Niemand raadpleegt deze informatie, als er belangrijke beslissingen moeten worden genomen.

Risicomanagement fungeert als een verantwoordingsdocument in het kader van narigheidsbestrijding. Het floreert alleen in een compliance gedreven context. Afgezien daarvan is het als een aparte discipline overtollig. Er is niks wat je niet ook al doet als onderdeel van gewoon management.

We hebben inmiddels een flinke denktocht afgelegd:

- van risico's managen en mogelijke onheilen afweren;
- via beslissingen nemen onder onzekerheid en de kansen op succes inschatten;
- naar belangen van stakeholders afwegen en dilemma's verzoenen.

En dat laatste gaat dan vooral over de mentaliteit van degenen die deze afwegingen maken.

Er is alle reden voor bescheidenheid. Onze menselijke vermogens om de toekomst te voorspellen zijn zeer beperkt. Het is nooit mogelijk om vooraf te voorspellen wat er zou kunnen gebeuren in een wereld met zoveel actoren en factoren. Dat is een volstrekte illusie. Vandaar de noodzaak om het improvisatievermogen van teams te blijven ontwikkelen.

Tot slot mogen we niet vergeten dat (on)gunstige resultaten altijd een onontwarbare combinatie zijn van (on)wijsheid en (on)geluk.

Colofon
Marinus de Pooter
marinus@mdpmct.com
+31 6 5206 2166
www.stay-future-proof.com
nl.linkedin.com/in/marinusdepooter

Bijlage - Wat zijn relevante aandachtspunten voor internal auditors?

Als internal auditor ben je een soort sportarts, coach, kritische huisvriend(in). Iemand die de kwaliteit van beslissingen beoordeelt en helpt om besluitvormingsprocessen te verbeteren. Hoe kun je - afgezien van compliancevereisten - met de kennis van de nieuwe inzichten waarde toevoegen voor je opdrachtgevers en geauditeerden?

1. Meer energie steken in dingen doen om te slagen dan om niet te falen.
2. De aandacht richten op het zo goed mogelijk realiseren van doelstellingen onder onzekerheid in plaats van op narigheidsbestrijding.
3. Je bekommeren om relevante informatie voor evenwichtige besluitvorming bij dilemma's in plaats van collega's lastig te vallen met het actualiseren van risicolijsten.
4. Beslissers informatie verschaffen over de mogelijke pro's en cons van hun opties bij belangrijke keuzen in plaats van lijsten met mogelijke onheilen te onderhouden.
5. Risico's zien als middel om mogelijke afwijkingen van de toekomstige resultaten in te schatten en om daarop te acteren en niet beschouwen als doel op zich.
6. De nadruk leggen op het afwegen van mogelijke voor- en nadelen bij impactvolle beslissingen in plaats van risicoregisters te onderhouden ten behoeve van risicostatusrapportages.
7. Besluitvormers helpen met geschikte analyse-instrumenten om hun specifieke afwegingen te maken in plaats van te streven naar één allesomvattende risicomanagement methodologie.
8. Actief de vele verschillende expertisegebieden met elkaar te verbinden in plaats van een separate functie of -commissie te creëren die zich bezighoudt met risico's.
9. Eigenaarschap van resultaten benadrukken om succesvol te blijven in plaats van aparte risico-eigenaren te benoemen.
10. Beseffen dat het bij elk beleidsterrein gaat over het omgaan met onzekerheid in plaats van afzonderlijke risicomanagement beleidsstukken op te stellen.
11. De waarschijnlijkheden nagaan van mogelijke afwijkingen van de doelstellingen (toleranties) in plaats van allerhande risicobereidheidsuitspraken te formuleren.
12. Het kritische gesprek aangaan over de veronderstellingen in voorstellen, plannen en prognoses in plaats van uitgebreide risicolijsten bij te houden.
13. De focus leggen op de waarschijnlijkheid dat belangrijke doelstellingen worden bereikt in plaats van zich druk te maken over risicoscores en risiconivo's.
14. Uitspreken dat veel toekomstige ontwikkelingen inherent chaotisch en onvoorspelbaar zijn in plaats van uit te gaan van recht-toe-recht-aan relaties tussen oorzaken en gevolgen.
15. Oog hebben voor de enorme complexiteit van de toekomst die mede veroorzaakt wordt door de afhankelijkheid van talloze actoren met hun eigen belangen.
16. Weten dat mensen beroerd slecht zijn in het inschatten van waarschijnlijkheden in plaats van eindeloos te delibereren over het bepalen ervan.

17. Aandacht besteden aan het belang van afhankelijkheids- en consequentiebewustheid in plaats van afzonderlijke risico's of risicocategorieën te managen.

18. Zorgen dat beslissers beschikken over evenwichtige informatie voor hun afwegingen in plaats van omvangrijke 'control frameworks' te bouwen en te testen.

19. Het belang zien van competenties (beoordelingsvermogen) en intenties (integriteit) van de beslissers in plaats van vol in te zetten op preventieve 'hard controls'.

20. Bij benoemingen leidinggevenden beoordelen op hun persoonlijke waarden en niet primair op hun diploma's, intelligentie en werkervaring.

21. Veel aandacht besteden aan het werkelijke gedrag van de leidinggevenden in plaats van naïef te refereren aan de marketingversie van de kernwaarden op de website.

22. Zorgen dat de schattingen die worden gebruikt in voorstellen, budgetten en prognoses gebaseerd zijn op realistische aannames in plaats van alleen gunstige informatie te verwelkomen.

23. Focussen op het afwegen van botsende belangen in plaats van na te gaan wat de realisatie van individuele organisatiedoelstellingen bedreigt.

24. In de reguliere managementrapportages opnemen met welke mate van waarschijnlijkheid de ingeschatte resultaten zullen vallen binnen de aanvaardbare bandbreedtes in plaats van separate risicorapportages op te stellen.

25. De nadruk leggen op het leren van positieve en negatieve ervaringen in plaats van te verwachten van managers dat zij (schone) interne 'in control statements' afgeven.

26. Je inzetten voor het uitwisselen van kennis en best practices in plaats van vooral bezig te zijn met compliancevereisten, zoals de nieuwe Verklaring Omtrent Risicobeheersing.

27. Complexe strategische beslissingen op een andere manier aanvliegen dan eenvoudiger vraagstukken waarbij je beschikt over bruikbare modellen en historische data.

28. Je bewust zijn van wensdenken, groepsdenken en tal van andere veel voorkomende vooringenomenheden in plaats van mee te gaan in het aanlokkelijke maakbaarheidsdenken.

29. Beseffen dat je nog steeds om moet kunnen gaan met de bijbehorende nadelen, als je kiest voor een optie vanwege de vermeende voordelen.

30. Benadrukken dat het bij alle zakelijke beslissingen gaat om keuzen maken onder onzekerheid in plaats van 'Risicomanagement' als een apart agendapunt te behandelen.