Is risicomanagement overtollig?

Auteur: Marinus de Pooter
Gepubliceerd op https://www.norea.nl/magazine/is-risicomanagement-overtollig in februari 2023

Dit artikel is eerder gepubliceerd in Audit Magazine van het IIA en overgenomen met toestemming van de redactie van Audit Magazine en de auteur.

Veel internal auditors zullen hun wenkbrauwen fronsen bij de kop van dit artikel. Voor hen hoort het beheersen van risico's bij internal audit zoals vuurwerk bij oudjaarsavond. De afgelopen jaren zijn de inzichten echter sterk veranderd. In dit artikel de recente ontwikkelingen die belangrijke implicaties hebben voor internal auditors.

Confronterende vraag

Volgens velen kan en moet risicomanagement worden geïmplementeerd. Dat het uiterst onverstandig is om dit niet te doen leggen consultants je graag uit. Het behoedt je voor onnodige valkuilen. En bovenal helpt risicomanagement je bij het behalen van je doelen. Hoe kan het dan overtollig zijn?

Adviseurs blijven ze maar verkopen: risicobereidheidsverklaringen, risicoregisters, risicomatrices en risicodashboards. En veel organisaties blijven ze maar kopen. Tim Leech en anderen noemen deze aanpak 'risk list management'. De onderliggende overtuiging is dat het uiteindelijke doel is: het beperken van wat er allemaal mis kan gaan. Echter, zoals Alexei Sidorenko en anderen opmerken, het gaat niet primair over het mitigeren van risico's, maar over het nemen van afgewogen beslissingen.

Je kunt je afvragen in hoeverre beslissers separaat risicomanagement nodig hebben, als het volgende op hen van toepassing is.

- Zij begrijpen dat doelstellingen gaan over het creëren en beschermen van waarde voor hun kernstakeholders. Ze nemen het gestructureerd vooruitkijken serieus als onderdeel van hun reguliere managementtaken. Ze stellen vragen als: wat kan er gebeuren dat de realisatie van onze doelstellingen kan helpen of belemmeren? Ze proberen realistische inschattingen te maken van mogelijke positieve én negatieve effecten op de belangen van hun belanghebbenden.
- Zij laten zien dat ze consequentiebewust zijn. Ze realiseren zich dat ze de keuze hebben om dingen te doen of na te laten. Ze overwegen de mogelijke positieve én negatieve gevolgen van hun opties voor de concurrerende of zelfs botsende belangen van hun kernstakeholders.
- Zij tonen dat ze over de juiste competenties beschikken om de mogelijke voor- en nadelen van hun beslissingen af te wegen. Ze geven ook blijk van een mentaliteit die leidt tot evenwichtige beslissingen en oprechte pogingen om dilemma's te verzoenen.

Implicaties van overtollig risicomanagement

Als organisatieleiding moet je iets met risico's. Dit is het uitgangspunt in de internationale internal auditstandaarden. #2120 schrijft voor dat de interne auditfunctie de effectiviteit van de risicomanagementprocessen moet evalueren en moet bijdragen aan het verbeteren ervan.

Volgens #2010 moet de *chief audit executive* minimaal één keer per jaar een risicoanalyse uitvoeren als basis voor het risicogebaseerde interne auditplan. Het audituniversum moet alle risico's omvatten die ertoe doen. Het doel is voldoende zekerheid te verschaffen dat de significante risico's effectief zijn gemitigeerd door de risicobeheersings- en controlesystemen.

Als risicomanagement overtollig is, heeft dat ook implicaties voor degenen die door hun collega's van risicomanagement zijn aangemerkt als 'risico-eigenaar'. En voor degenen die lid zijn van een *risk committee* of die zelfs *chief risk officer* zijn. Om het nog maar niet te hebben over de talloze risicomanagers, adviseurs en leveranciers van applicaties.

Je zou dus kunnen denken: het kan niet waar zijn dat het overtollig is. Maar als risicomanagement het antwoord is, wat was dan ook alweer de vraag? Hoe goed helpt de conventionele aanpak besluitvormers om met onzekerheden, verstoringen en dilemma's om te gaan? Of is het meer een geloofssysteem? Kan er sprake zijn van missionarissen, gelovigen en inquisiteurs die een serieus commercieel belang hebben bij het in stand houden van dit systeem?

Percepties met betrekking tot risicomanagement

Veel bestuurders zien risicomanagement vooral als een compliance-aangelegenheid. Effectief risicomanagement betekent voor hen dat ze geen gedoe hebben met hun externe of interne toezichthouders. Door hun rol zijn die toezichthouders nauwelijks geïnteresseerd in de 'upside' van risico's. Zij zien het vooral als hun taak om mogelijke onheilen te minimaliseren.

Veel brochures en artikelen over risicomanagement proberen te ontsnappen aan de focus op compliance. In snel veranderende tijden, zo stellen ze, moeten de stuurlieden effectief door turbulente wateren navigeren. Het begrijpen en beheersen van risico's is daarom essentieel voor succesvol leiderschap. Ziedaar de businesscase voor het implementeren van risicomanagement.

Commissarissen leren tijdens trainingen te vragen naar de top-10-risico's. Dat is blijkbaar een teken dat het management goed heeft nagedacht over mogelijke onheilen, narigheden en kwetsbaarheden. En dat er passende maatregelen zijn genomen om deze zoveel mogelijk te beperken.

Opmerkelijk is dat je bij risicomanagementtrainingen, -webinars en -congressen zelden ondernemers, lijnmanagers en projectleiders tegenkomt. Dat is best opvallend, want de standaarden en brochures beloven immers dat risicomanagement hen in staat stelt hun doelstellingen beter te realiseren. De meesten zijn niet achterlijk. Als het hen echt zou helpen, zouden ze dan niet allemaal op de eerste rij willen zitten om te leren hoe ze hier hun voordeel mee kunnen doen?

De ISO 31000 Risk Management Guidelines stellen dat risicomanagement effectief is als het is ingebed in de besluitvorming. De realiteit is dat risicomanagement een verantwoordingsinstrument is geworden. Dat is heel wat anders dan een hulpmiddel om onder onzekerheid je doelen te bereiken.

Ernstige problemen met conventioneel risicomanagement

Recente inzichten onderstrepen de problemen met conventioneel risicomanagement. Roger Estall en Grant Purdy concluderen in hun boek *Deciding* dat het als een molensteen om de nek van organisaties hangt.

Waar hebben we het trouwens over als we het woord 'risico' gebruiken? Er bestaat geen universele definitie van. Opvallend is dat ISO – notabene de International Organization for Standardization – zelf meer dan veertig(!) verschillende definities van 'risico' gebruikt in hun eigen documenten.

In COSO IC (2013), COSO ERM (2004) en ook in het gewone spraakgebruik verwijst 'risico' naar iets negatiefs. Naar iets wat je geld kan kosten, dat slecht kan zijn voor je gezondheid of dat je in diskrediet kan brengen. Anderzijds hanteren ISO 31000 (vanaf de eerste editie in 2009) en COSO ERM (2017) een neutraal risicobegrip. Het gaat om zowel positieve als negatieve effecten op het behalen van de doelstellingen.

Deze verandering heeft verstrekkende gevolgen. Oorspronkelijk gebruikte COSO vier zogenaamde risk responses: *accept*, *avoid*, *reduce*, *share*. COSO voegde in 2017 *pursue* toe als de vijfde optie: een verhoogd risico accepteren om betere prestaties te bereiken. Dit sluit beter aan bij het gangbare concept van het zoeken naar een passende balans tussen risico en rendement.

Het feit dat risico zeer uiteenlopende betekenissen heeft, impliceert dat het simpelweg gebruiken van de term al een bron van verwarring is. De conventionele aanpak richt zich op dingen die fout kunnen gaan. Dit is bepaald niet holistisch, want bij besluitvorming gaat het om het afwegen van ingeschatte voor- én nadelen. Als je bijvoorbeeld gaat beleggen, ben je hopelijk niet alleen bezig met mogelijke verliezen, maar ook met waardestijging.

Als je de modernere definitie gebruikt (risico omvat zowel de positieve als de negatieve effecten), dan ben je gelijk de meest mensen kwijt. In het gewone spraakgebruik heeft risico nu eenmaal een negatieve connotatie.

Vanwege al deze verwarring stellen Norman Marks en anderen voor om het 'r-word' te vermijden. Onzekerheidsmanagement, succesmanagement, of verwachtingsmanagement zijn al betere termen. Zelf gebruik ik vaak de term waardemanagement. Zowel COSO ERM als ISO 31000 geven immers aan dat het gaat om het creëren én beschermen van waarde. Deze term houdt ook rekening met het feit dat verschillende belanghebbenden waarde hechten aan hele verschillende aspecten, zoals veiligheid, rendement en maatschappelijke betekenis.

We moeten ons ook realiseren dat er geen 'risicologie' wetenschap bestaat. Er is wel een op zichzelf staande risicomanagementwereld gecreëerd met allerlei door adviseurs aanbevolen praktijken. Die werkwijzen moeten vervolgens worden geïntegreerd in het bestaande managementsysteem. Helaas zijn hier geen succesverhalen van bekend.

Een van de artefacten van conventioneel risicomanagement is de risicobereidheidsverklaring. Het verwijst naar de typen en de hoeveelheid risico die je bereid bent te nemen. Er is echter geen meeteenheid of valuta om de hoeveelheid risico uit te drukken. Bij risicoprofielen is het gebruikelijk om gemakshalve risico's te aggregeren. Als je dat probeert te doen op basis van geldwaarde, ontdek je al snel dat wat je in je leven het meest waardeert moeilijk in pecunia uit te drukken is.

Wat we ons wellicht niet altijd realiseren, is dat kansen en bedreigingen geen dingen zijn, maar gedachten: mentale beelden van mogelijke toekomstige gebeurtenissen, veranderingen in omstandigheden en trends. Deze beelden worden sterk beïnvloed door onze persoonlijkheid, kennis en ervaringen. Bovendien blijken wij mensen veel last te hebben van vooringenomenheden, zoals Daniel Kahneman heeft aangetoond.

In de praktijk wordt risicomanagement vaak kwalitatief uitgevoerd. Scores worden toegekend aan geschatte waarschijnlijkheden en effecten met behulp van waarden op ordinale schalen (bijvoorbeeld van 1 tot 5). Dit type schalen wordt gebruikt in opiniepeilingen en om de kwaliteit van hotels te beoordelen. Je kunt echter niet ongestraft ordinale waarden vermenigvuldigen om tot risicoscores te komen.

Risicokwantificering is weer sterk afhankelijk van de veronderstelde parameters in het model en van de kwaliteit en kwantiteit van de gegevens. Als de gehanteerde aannamen niet meer gelden, vervalt de waarde van het model. Bovendien blijven het slechts modellen, een kaart is niet het gebied dat het voorstelt.

Beslissers worden voortdurend geconfronteerd met dilemma's vanwege de niet-gelijklopende belangen van de belanghebbenden. In de praktijk gaat het nemen van beslissingen niet over één enkel doel. Uitzonderingen daargelaten, zoals de eenzijdige aandeelhouderswaarde-maximalisatiebenadering. Daarbij worden risico's vooral gezien als bedreigingen voor het winstpotentieel. We hebben allemaal kunnen zien tot welke ontsporingen de opvatting 'geld als doel' in plaats van 'geld als middel' heeft geleid.

De essentie van recente inzichten

Volgens de conventionele benadering is het verstandig om een apart systeem te implementeren dat gericht is op het bestrijden van narigheden: risicomanagement. Nieuwe inzichten geven aanleiding om te focussen op consequentiebewust vooruitkijken en het omgaan met dilemma's. Dat komt neer op het overwegen van de mogelijke effecten van handelen of nalaten als onderdeel van de dagelijkse taken en verantwoordelijkheden.

Als beslisser moet je voortdurend de voor- én nadelen van je opties afwegen. Er is niets in het leven dat alleen voordelen biedt. Er zijn ook altijd potentiële of daadwerkelijke nadelen. Neem bijvoorbeeld het kopen van een huis. Het brengt niet alleen voordelen met zich mee, zoals kapitaalopbouw, meer vrijheid om het naar eigen smaak aan te passen en lagere maandlasten dan huren. Het is essentieel om ook de mogelijke nadelen in overweging te nemen. In wezen speculeer je, wanneer je een hypothecaire lening afsluit, met geleend geld. Ook kun je in ongelukkige omstandigheden terechtkomen, zoals verzakkende funderingen en akelige buren.

Als managementteam word je niet succesvol door alleen maar onheilen tegen te gaan en mislukkingen te beperken. Succes vereist zowel het benutten van je kansen als het beperken

van je bedreigingen. Het periodiek bijwerken van een lijst met dingen die fout kunnen gaan, is niet hetzelfde als nagaan hoe je het best dilemma's kunt verzoenen.

De essentie van management is het nemen van beslissingen. Het gaat over het toewijzen van schaarse mensen en middelen om producten en diensten te leveren die voldoen aan de eisen en verwachtingen. Norman Marks benadrukt het belang van het focussen op vergroting van de kans op succes.

Marketing is een ingenieus vak met krachtige beïnvloedings- en framingtechnieken. Je moet je er altijd van bewust zijn dat er mensen zijn die erop uit zijn om de voordelen te markeren en de nadelen te maskeren. Vandaar het belang van mensen die constructief en kritisch meedenken. Die jou als beslisser bevragen en uitdagen. Die jou willen helpen om je kans op succes te vergroten.

Deze 'kritische huisvrienden' zijn erg nuttig, omdat zij je scherp houden. Zij waarborgen dat je realistische veronderstellingen hanteert in je plannen, scenario's en prognoses. En dat je belangen evenwichtig afweegt bij dilemma's. Waarom zou je eerst een apart risicomanagementsysteem creëren en dit vervolgens proberen te integreren in je reguliere managementsysteem? Het ligt veel meer voor de hand om de positie van de beslissers als vertrekpunt te nemen.

De waarde voor internal auditors

Afzonderlijk conventioneel risicobeheer ontaardt gemakkelijk in een illusoir, compliance-gedreven systeem. Wat geauditeerden echt zouden moeten willen weten is hoe waarschijnlijk het is dat ze succesvol zullen zijn. Onderzoek daarom als internal auditor in hoeverre de beslissers gestructureerd consequentiebewust vooruitkijken. Ga bijvoorbeeld na of en hoe zij 'wat kan er gebeuren'- en 'wat als x'-vragen stellen.

Onderzoek hoe zij omgaan met de uitgangspunten in hun plannen, voorstellen en extrapolaties. Zijn hun inschattingen realistisch en evenwichtig? Zijn de juiste experts erbij betrokken? Is er ruimte voor kritische stemmen? Als de beslissers besluiten te gaan voor een optie vanwege de ingeschatte voordelen, gaan ze dan ook na in hoeverre ze in staat zijn goed om te gaan met de bijbehorende nadelen?

Let vooral op de mentaliteit van de leidinggevenden. In de praktijk gaat besluitvorming altijd over tegenstrijdige belangen zoals commercie versus compliance. Denk aan een potentiële klant met allerlei dubieuze zakelijke activiteiten die een aanzienlijke financiële inkomstenbron kan worden voor jouw organisatie. Als beslisser moet je kiezen welke belangen van welke stakeholders prioriteit krijgen. Dilemma's gaan over ethische afwegingen.

Kijk altijd welke doelstellingen leidend zijn. Als alleen commerciële belangen de boventoon voeren, is dat een teken aan de wand. Ga voorbij aan de aansprekende kernwaarden op de website, maar ga na welke belangen leidinggevenden in de praktijk voor laten gaan. Als bij compliance de belangrijkste drijfveer is om te voorkomen dat ze betrapt worden, dan is dat een observatie die niet onvermeld mag blijven.

Focus niet langer op risico-inventarisaties. Het blijft opmerkelijk dat veel mensen denken dat risicomanagement gaat over het actualiseren van risicolijsten. Stop met risicoregisters die elk jaar of kwartaal worden bijgewerkt. Besteed geen tijd aan het eindeloos classificeren van

risiconiveaus. Want het gaat helemaal niet om de risico's, maar om het inschatten van de kans op succes.

Maak je niet druk over hoe de kwaliteit van risicobereidheidsverklaringen kan worden verbeterd. Maar focus op in hoeverre de leidinggevenden worden ondersteund om betere beslissingen te nemen. Beschikken ze over de informatie die nodig is om bewust de voor- en nadelen af te wegen bij belangrijke keuzen, zoals met betrekking tot productintroducties, overnames en ketenpartners?

Besef vooral dat er alle reden is voor bescheidenheid. Onze menselijke vermogens om de toekomst te voorspellen zijn beperkt. Het is een volstrekte illusie dat je je van tevoren goed kunt voorstellen wat er allemaal kan gebeuren in een wereld met zoveel actoren en factoren. Je hebt veel meer aan mensen die alert blijven op wat er gebeurt, aan een cultuur waarin ook ongunstig nieuws welkom is en aan het vermogen om als team te improviseren

Marinus de Pooter is zelfstandig gevestigd als interimmanager, adviseur en trainer. Daarvoor was hij director of finance bij Ernst & Young Global Client Consulting, European director Internal Audit bij Office Depot en ERM solution leader bij EY Advisory.