

ARTIKELEN | 1 APRIL 2019

ILLUSORY RISK MANAGEMENT

Auteur: Drs. Marinus de Pooter RA CMA CFM CIA CRMA CCS GRCP GRCA

Beeld: Adobe Stock - Josh Calabrese

Leestijd: 10 min



Risicomanagement wordt doorgaans vormgegeven als een separaat systeem. In dit artikel ga ik na in hoeverre deze conventionele benadering onttaardt in een illusoir geheel. Als alternatief bespreek ik de waardemanagementbenadering, die managementteams helpt om samen te werken bij het blijven creëren én beschermen van wat hun kernstakeholders waardevol vinden.

Op de jaarlijkse conferentie van IIA Singapore in oktober 2018 heb ik een presentatie gegeven over illusory risk management. Centraal in mijn verhaal stond het grote verschil tussen enerzijds risicomanagement als een apart systeem en anderzijds waardemanagement. Dat laatste richt zich op het ondersteunen van beslissers bij het afwegen van relevante kansen en bedreigingen.

Conventioneel risicomanagement

Enterprise risk management (ERM) is in essentie een planning- and controlconcept, waarbij de organisatieleiding alle risico's identificeert die van invloed kunnen zijn op de realisatie van doelstellingen. Vervolgens moet zij beheersmaatregelen ontwerpen en implementeren, waardoor de netto-risicoblootstelling valt binnen de geformuleerde risicobereidheid. Door de risicoanalyse periodiek te herhalen en de werking van de beheersmaatregelen te controleren, kan het systeem daar waar nodig worden bijgesteld. Vanuit de behoefte om het systeem in te zetten als verantwoordings-instrument ligt de nadruk op aantoonbaarheid.

Het gaat niet primair om risicomijding, maar om het bewust omgaan met kansen én bedreigingen

In het COSO Enterprise risk management-model van 2004 werd ERM gedefinieerd als: 'a process... to provide reasonable assurance regarding the achievement of entity objectives'. Risico werd omschreven als: 'the possibility that an event will occur and adversely affect the achievement of objectives'. Hiermee werd de toon gezet voor de huidige praktijk. Toezichthouders en consultants vertelden bestuurders dat het om een essentieel proces ging dat zij nog niet hadden. De omvangrijke ERM (later: governance, risk and compliance (GRC)) adviestak was geboren. Gevoed vanuit het oorspronkelijke COSO Internal control-gedachtegoed, lag hierbij bovendien de focus op zaken met negatieve effecten op het behalen van de organisatiedoelstellingen.

Het COSO ERM-model van 2017 geeft overigens een hele andere definitie. Het gaat nu over 'culture, capabilities and practices' in het licht van 'creating, preserving, and realizing value'. Risico wordt nu holistischer omschreven als: 'the possibility that events will occur and affect the achievement of strategy and business objectives'; een definitie zonder 'adversely'. De ISO 31000 Risk management principles and guidelines vat al sinds 2009 onder risico zowel mogelijke positieve als negatieve effecten. Het verwarrende is dat in het normale spraakgebruik risico gaat over zaken die je wilt voorkomen.

Conventioneel risicomanagement als illusoir systeem?

Als risicomanagement het antwoord is, wat was dan ook al weer de vraag? Vol verwondering kijkend naar de praktijk komt onwillekeurig deze gedachte op. Lang niet alles is op voorhand te voorzien, laat staan te beheersen. Het gaat niet primair om risicomijding, maar om het bewust omgaan met kansen én bedreigingen. Helpt de conventionele benadering beslissers echt om betere afwegingen te maken, of is het verworpen tot een op zichzelf staand illusoir systeem? Op basis van de genoemde observaties is dat laatste volgens mij het geval.



Zes stappen

Onzekerheidsreductie was de aanleiding, en maakbaarheid het uitgangspunt voor risicomanagement. In de meeste standaarden zijn deze stappen te herkennen: risico's identificeren, beoordelen en adresseren. Als onvoorspelbaarheid en snelle verandering de boventoon voeren, werkt deze benadering dan? Denk aan de 'unknown unknowns', zwarte

zwanen en chaos. Hoe kunnen we omgaan met toenemende complexiteit en afhankelijkheid, waarbij consistentie en stabiliteit verre van vanzelfsprekend zijn? In plaats van een set van vooraf gedefinieerde beheersmaatregelen komt het dan aan op alertheid, improvisatievermogen en flexibiliteit, op het vermogen om zo goed mogelijk om te gaan met onverwachte grote veranderingen. Een AO/IC-achtige instrumentele benadering van risico's past daar niet bij.

Advocaat van de duivel

In de praktijk gaan de staffunctionarissen van de afdeling Risicomanagement rond om hun risicolijsten te actualiseren. Als stafafdeling komen zij meer ophalen dan dat zij komen brengen. Beslissers daarentegen zijn gebaat bij collega's die hen kunnen helpen om betere afwegingen te maken. Door de veronderstellingen te valideren dan wel ter discussie te stellen. Door te helpen bij het beoordelen van de kwaliteit van (zoveel mogelijk vooruitkijkende) informatie. Door advocaat van de duivel te spelen, relevante wat-alsvragen te stellen, brainstorming te faciliteren, Monte Carlo-simulaties uit te voeren, scenarioanalyses uit te werken, et cetera. Goed geïnformeerde besluitvorming is echter gemakkelijker geroepen dan gedaan. Prognoses vereisen relevante interne en externe informatie. Menig organisatie kampt met suboptimale informatiesystemen, die bovendien vooral terugkijkend ingestoken zijn.

De risicomanagementfunctie wordt soms gepositioneerd als de sheriff die de cowboys in de business in toom moet zien te houden. Dat lijkt mij een vruchteloze structuur

Ook wordt soms de risicomanagementfunctie gepositioneerd als de sheriff die de cowboys in de business in toom moet zien te houden. Dat lijkt mij een vruchteloze structuur als die vrijbuiters niet uit het goede hout gesneden zijn, wegkomen met handelen in strijd met de gedragscode of niet evenwichtig worden beloond.

De waardemanagementbenadering

De nieuwe edities van COSO ERM (2017) en ISO 31000 (2018) waren een mooie gelegenheid om de term risk management te vervangen door value management. Volgens beide standaarden draait het immers allemaal om het creëren en beschermen van meer(-)waarde. Het was echter nog niet zover. Je zou het ook success management kunnen noemen. Activiteiten ondernemen brengt altijd onzekerheid met zich mee. Om je succes te vergroten, moet je kansen benutten én onnodige verliezen beperken. Uiteindelijk wil je de zekerheid vergroten dat je bereikt wat je wel wilt én dat je niet krijgt wat je niet wilt.

Je bent als organisatie toekomstbestendig, als je erin slaagt om waarde te blijven creëren én te beschermen voor je kernstakeholders. Begrippen als 'waarde', 'succes' en 'verbetering' zijn op zich echter inhoudsloos. Ze krijgen inhoud door de betekenis die de stakeholders eraan hechten. Belanghebbenden kijken door verschillende brillen naar je organisatie. Vanuit hun belangen vinden zij bepaalde zaken waardevol. Denk bijvoorbeeld aan: innovatiekracht, punctualiteit, privacy, veiligheid, rechtmatigheid, integriteit, rendement en continuïteit.

Anticiperen

Toekomstbestendigheid gaat over anticiperen op wat er zou kunnen gebeuren. Je wilt als managementteam weten waar je naar verwachting ongeveer zult uitkomen, en in hoeverre dat afwijkt van wat je kernstakeholders van je verwachten. Zijn jullie op de juiste weg? Of is er een gerede kans dat jullie het niet gaan halen? Proberen jullie in dat geval de juiste maatregelen te treffen? Of gaan jullie mogelijk de verwachtingen juist overtreffen, doordat jullie zo goed kunnen omgaan met onzekerheid? Zo bezien gaat het gewoon over (integraal) management. In plaats van een apart(e) programma, functie of commissie te hebben voor risico's, kun je beter verbinding creëren tussen al degenen die vanuit hun deskundigheid een bijdrage kunnen leveren aan het benutten van kansen en het beperken van bedreigingen.

AUDIT

MAGAZINE



Keuzen maken

Strategische, tactische en operationele beslissingen nemen betekent: keuzen maken. Werkstandaarden en werkwijzen zijn bedoeld om de afwegingen van de beslissers in goede banen te leiden. Het bepalen van die spelregels is het domein van gespecialiseerde (staf)afdelingen. Al die experts houden zich bezig met het omgaan met specifieke kansen en bedreigingen. Doorgaans bouwen die enthousiast allerlei afzonderlijke managementsystemen, beheersraamwerken en rapportages. Hoe voorkom je met zijn allen dat dit leidt tot de bekende silovorming, wildgroei en daardoor waardevernietiging?

Samenwerking is nodig

Samenwerking is nodig zowel bij het inrichten van de interne organisatie als bij het rapporteren over hoe de vlag er naar verwachting bij zal hangen de komende periode. Risicomanagement is bij veel organisaties een van de vele functionele silo's geworden. Naast alle andere soorten management, zoals: account-, asset-, compliance-, continuïteits-, crisis-, data-, incident-, informatie-, kennis-, kwaliteits-, lean-, logistiek-, personeels-, prestatie-, proces-, project-, reputatie-, security-, treasury-, veiligheids- en verandermanagement. Als managementteam ben je vooral gebaat bij het organiseren van één platform dat zorgt voor de verbinding tussen al die deskundigen.

Vijf kernvragen

Om dat te bereiken ga je bij de waardemanagementbenadering als team aan de slag met vijf kernvragen. Het zijn de bouwstenen voor de praktische analyses die je kunt uitvoeren voor een afzonderlijk(e) bedrijfsproces, project, afdeling, vestiging, divisie, keten of voor de hele organisatie. Het zijn basisvragen die je aan iedere collega kunt voorleggen in het kader van het optimaliseren van de interne organisatie. Samen vormen ze de puzzel die elk team moet oplossen om effectief met kansen en bedreigingen om te gaan. De vijf componenten vormen samen ook de kapstok waar je alles aan op kunt hangen wat op dit moment al is geregeld (zie figuur 1).

Wie?

Bij het inrichten en optimaliseren van de interne organisatie moeten er steeds keuzen worden gemaakt. Dat vraagt om duidelijke mandatering, regie en coördinatie. Waardemanagement staat of valt met de effectiviteit van de governance:

degenen die de keuzen mogen of moeten maken. Dit geldt zowel met betrekking tot de dagelijkse operatie als de voortdurende transformatie. Wie is én voelt zich in het team verantwoordelijk voor het behalen van welke geformuleerde doelstellingen? Diegene moet ook kunnen meebeslissen hoe het best kan worden omgegaan met de kansen en bedreigingen. Een prominent en praktisch vraagstuk betreft het mandaat van de experts van de stafafdelingen. In hoeverre mogen zij aan de collega's die de klanten bedienen werkwijzen voorschrijven, dan wel mogen zij hen slechts adviseren? Hoe zorg je er als managementteam enerzijds voor dat de stafspecialisten de lijnverantwoordelijken scherp houden, en hoe voorkom je anderzijds dat deze experts in hun enthousiasme te ver doorschieten?

Heldere werkafspraken stroomlijnen de besluitvorming, vergemakkelijken de werkoverdracht tussen collega's en geven een duidelijk normenkader voor audits

Wat?

Voor elk team is het zinvol om een integraal overzicht te hebben van de geclusterde activiteiten waarmee iedereen zich bezighoudt. Het geeft het gemeenschappelijke speelveld weer voor alle betrokkenen. Dit gaat over de 'leefwereld', het 'verrichten'. Dit overzicht van besturende, primaire en ondersteunende processen geeft inzicht in alle relevante transactiestromen en -volumes. Het vormt ook de basis voor het applicatielandschap voor de verwerking van die transacties. Het is daarmee het substraat voor de informatieverwerking, business intelligence en dus prognoses. Het voordeel van beter inzicht in wie wat doet is evident bij integratietrajecten en ketensamenwerking.

Waarom?

Het succes van elke organisatie wordt bepaald door de mate waarin de kernstakeholders tevreden zijn. Dit gaat over de 'bedoeling', het 'richten'. De belanghebbenden kijken vanuit uiteenlopende perspectieven naar de te leveren prestaties. Zij zijn bij uitstek geïnteresseerd in de effecten ervan op hun belangen. Vandaar dat de stakeholdersanalyse een essentiële stap vormt. Als het goed is sluiten de ambities hierop aan: de meerwaarde die het managementteam wil creëren en beschermen voor specifieke belanghebbenden. Uitgedrukt in de missie, visie en strategie en doorvertaald naar concrete succesfactoren, doelstellingen en indicatoren.

Hoe?

Bij hun werkzaamheden moeten de verantwoordelijken afwegingen maken. Om dat goed te laten verlopen hebben zij kaders en andere spelregels nodig. Dit gaat over de 'systeemwereld', het 'inrichten'. Het betreft de afgesproken werkstandaarden en -wijzen. De praktische uitwerking van deze spelregels zijn de interne afspraken, die zijn vastgelegd in de reglementen, voorschriften, richtlijnen, procedures, protocollen, werkinstructies, et cetera. Doorgaans zijn deze opgenomen in een 'policy house'. Voor het opstellen van deze documenten is expertise nodig van vakmensen. Heldere werkafspraken stroomlijnen de besluitvorming, vergemakkelijken de werkoverdracht tussen collega's en geven een duidelijk normenkader voor audits. De meestbepalende factor bij het 'hoe' is de organisatiecultuur. Kenmerkt de cultuur zich door voorbeeldgedrag van de leidinggevendenden? Willen beslissers de mogelijke consequenties van hun keuzen onder ogen zien? Wordt het gewaardeerd dat collega's veronderstellingen in (te) ambitieuze plannen ter discussie stellen?

Verbetering

Een voortdurend verbeterprogramma maakt het eenvoudiger om te focussen op wat er echt toe doet. Gevraagd naar de 'beste verbeteringen' noemen mensen in de praktijk situaties waarbij volgens hen de risicoblootstelling groter of de kansbenutting kleiner is dan gewenst. De benodigde verbeteringen gaan meestal over het beter ontwerpen, invoeren, toepassen of monitoren van de werkwijzen en werkstandaarden. Deze 'verbouwingen' gaan nadrukkelijk ook over de

AUDIT

MAGAZINE

competenties van de betrokkenen. Niet alleen hun vakinhoudelijke kennis en vaardigheden, maar vooral ook hun persoonlijke leiderschapskwaliteiten. Een voortdurend verbeterprogramma stelt de organisatieleiding in staat om mogelijke verbeterinitiatieven te identificeren, prioriteren en realiseren. Hoe beter de interne informatievoorziening op orde is én hoe meer collega's zich vrij voelen om zaken te melden, hoe eerder aandachtvragende trends gesignaleerd kunnen worden.

Conclusie

Conventioneel risicomanagement kan gemakkelijk verworden tot een separaat illusoir systeem met een hoog compliancegehalte. Waardemanagement daarentegen is een verbindende benadering waarbij je als team één gezamenlijk platform creëert voor alle relevante typen management. Het stelt je in staat om steeds te prioriteren welke aanpassingen van je interne organisatie nodig zijn om je kernstakeholders blijvend tevreden te houden.

Observaties vanuit de praktijk

Tijdens mijn presentatie in Singapore deelde ik deze observaties met betrekking tot conventioneel risicomanagement. Dit is het beeld dat opdoemt in de praktijk:

- Afzonderlijk vocabulaire gebruiken met veel woorden die beginnen met 'risico-', zoals risicocultuur naast organisatiecultuur en risico-indicatoren naast prestatie-indicatoren.
- Streven naar één overkoepelende methodologie in plaats van beslissers te helpen met instrumenten die hen het best ondersteunen bij het omgaan met kansen en bedreigingen in hun specifieke situatie.
- Risico's zien als doel en niet als middel om mogelijke afwijkingen van de toekomstige resultaten in te schatten om vervolgens de interne organisatie waar nodig aan te passen.
- Nagaan wat de realisatie van individuele organisatiedoelstellingen bedreigt en voorbijgaan aan het afwegen van conflicterende belangen bij het oplossen van dilemma's
- Een separate functie of -commissie creëren die gaat over risico's in plaats van actief de vele verschillende expertisegebieden met elkaar te verbinden
- Aparte risico-eigenaren benoemen, alsof het omgaan met onzekerheid geen onderdeel is van de reguliere managementverantwoordelijkheid en het proceseigenaarschap.
- Afzonderlijke risicomanagementbeleidsstukken opstellen, terwijl het bij elk beleidsterrein gaat over het omgaan met kansen en bedreigingen.
- Focussen op het formuleren van risicobereidheidsuitspraken in plaats van op het gesprek (als kritische huisvriend) over de veronderstellingen in voorstellen, plannen en prognoses.
- Uitgebreide risicoregisters en risicodossiers bijhouden in plaats van de waarschijnlijkheden na te gaan van mogelijke toekomstige afwijkingen van de geformuleerde doelstellingen.
- Omvangrijke control frameworks bouwen en testen (vaak ondersteund door dure applicaties), terwijl beslissers bij hun afwegingen vooral evenwichtige informatie nodig hebben.
- Inzetten op preventieve hard controls (voorkómen is beter dan genezen) en beperkt oog hebben voor het belang van competenties (beoordelingsvermogen) en intenties (integriteit).
- Zich druk maken over risicoscores (risiconiveau) en weinig aandacht hebben voor de afhankelijkheden tussen risico's en ons beperkte vermogen om waarschijnlijkheden goed in te kunnen schatten.
- Risicomatrices ('heatmaps') gebruiken zonder zich te realiseren dat de geplote punten voor waarschijnlijkheden en

AUDIT

MAGAZINE

effecten verdelingen zijn (reeksen van mogelijke uitkomsten, elk met een bepaalde kans).

- Uitgaan van rechttoe rechtaanrelaties tussen oorzaken en gevolgen, terwijl veel toekomstige ontwikkelingen inherent chaotisch en onvoorspelbaar zijn.

Aparte risicorapportages opstellen naast reguliere managementrapportages, die niet aangeven in welke mate de verwachte uitkomsten zullen vallen binnen de aanvaardbare bandbreedtes.

- Van collega's verwachten dat zij (schone) interne in control statements afgeven in plaats van de nadruk te leggen op het leren van (positieve en negatieve) ervaringen.
- Bezig zijn met compliancevereisten, zoals risicoparagrafen, in plaats van zich in te zetten voor het uitwisselen van kennis en best practices tussen de organisatieonderdelen.
- Gemakshalve voorbijgaan aan enorme complexiteit van de toekomst, die mede veroorzaakt wordt door de afhankelijkheid van vele interne en externe actoren met hun eigen belangen.
- Risicomanagement als apart agenda-item beschouwen bij vergaderingen, alsof het bij de andere items niet zou gaan over het succesvol omgaan met kansen en bedreigingen.
- Zich vooral druk maken over het mitigeren van allerlei mogelijke onheilen en niet bezig zijn met het optimaliseren van de risk-returnbalans.

Tags: Risicomanagement, vaktechniek

Bron url: <https://auditmagazine.nl/artikelen/illusory-risk-management/>