"Forget about traditional risk management!"

Marinus de Pooter, 29 juni 2015

Onder deze titel heb ik eerder deze maand in Milaan een presentatie gegeven op het congres "Perspectives in Enterprise Risk Management". De aanwezigen waren vooral beroepsbeoefenaars, adviseurs en wetenschappers uit Europa, Rusland en de USA.

Ik stelde een thema aan de orde, dat mij de afgelopen jaren steeds meer is gaan fascineren. Als risicomanagement inderdaad zoveel goeds brengt (zoals doorgaans wordt beweerd), hoe kan het dan dat lijnmanagers niet massaal afkomen op trainingen en congressen? Waarom staan zij niet in de rij om meer te leren over al die prachtige concepten en instrumenten (inclusief de vele indrukwekkende software applicaties)?

De beperkte waardering voor traditioneel risicomanagement komt volgens mij door meerdere faktoren. Zo wordt het doorgaans negatief ingestoken. Als je je alleen maar richt op zaken die mis kunnen gaan, dan ben je niet holistisch met de toekomst bezig. Kansen en risico's gaan immers altijd hand in hand. Als je naar je werk gaat, dan kun je onderweg aangereden worden. Als je op rekening levert aan je klanten, dan loop je debiteurenrisico. Als je mensen in dienst neemt, dan kun je te maken krijgen met personeelsfraude. Integraal kans- en risicomanagement gaat daarom vooral over het steeds met elkaar hebben over de afwegingen die je maakt.

Je mist de aansluiting met de meeste ondernemers, bestuurders en managers, als je risico's geïsoleerd bekijkt van kansen. Idem als je iets met risicomanagement doet, omdat het nu eenmaal moet van je toezichthouder of omdat het hoofdkantoor dat van je verlangt. Het zou velen enorm helpen, als ook toezichthouders zouden inzien dat compliance geen goede intrinsieke motivator is om effectief met risico's om te gaan. Het creëren van een aparte afdeling Risicomanagement of een aparte CRO functie is volgens mij eveneens een heilloze weg.

Het "lines of defence" model is een veelbesproken concept. Dat wil zeggen door mensen in specifieke staffuncties. Business managers hebben er weinig mee; zij zijn meer van het aanvallen. Het is mijn observatie dat die staffunctionarissen onderling nogal wat tijd besteden aan het afbakenen en verdedigen van hun wederzijdse territoria. In plaats van zichzelf te beschouwen als de hofhoudig van de CEO (de wetgevende macht) zouden ze zich in de praktijk beter dienstbaar kunnen opstellen voor hun collega's in de primaire processen. Die moeten namelijk steeds lastige afwegingen maken en kunnen waardevolle input gebruiken voor optimale besluitvorming. Uiteindelijk ligt de toegevoegde waarde van risk managers, controllers, compliance officers, etc. in het ondersteunen van de "eerste lijn" bij het realiseren van meer klantwaarde.

Cruciaal is dat die collega's in de primaire processen dan wel zódanig worden aangestuurd en beloond dat zij ethisch verantwoorde dingen doen. Niet alles waar je mee weg komt (bijvoorbeeld door gebrekkige wetgeving of handhaving) is immers daarmee ook goed om te doen. Denk aan de derivatenporteuilles die aan mkb-bedrijven werden verkocht.

De gemiddelde staffunctionaris (zoals een risk manager in de "tweede lijn") kan onvoldoende tegenwicht bieden aan 'hardliners', alfa-mannetjes, haantjes, ego-trippers, "dikke ikken", etc. in de commercie. Als de persoonlijkheid van iemand op een belangrijke positie een cocktail is van dominantie, actiegerichtheid, narcisme, optimisme en arrogantie, dan kan alleen een goede Raad van

Commissarissen of Raad van Toezicht nog uitkomst bieden. Is die voldoende alert op de mogelijke kwalijke gevolgen voor de organisatie van het gedrag van zo'n persoon?

Ik heb in het bovenstaande een aantal zaken aangestipt die bij traditioneel risicomanagement niet of slechts beperkt aan de orde komen. Daar gaat het in de praktijk meeestal over uitgebreide risicoregisters en de bekende groen-geel-rode plaatjes. Gevaarlijke dingen overigens, als je het mij vraagt. Zo leggen ze de focus op risico's en geven nauwelijks inzicht in de mate waarin de organisatiedoelstellingen naar verwachting gerealiseerd zullen worden. En dan heb je nog de vaak omvangrijke "control frameworks", die vervolgens uitvoerig gecontroleerd worden door in- en externe auditors. Al met al voornamelijk een formele, instrumentele benadering met een hoog "'t is rot, maar 't mot" gehalte.

Traditioneel risicomanagement past binnen het gedachtengoed dat de wereld maakbaar is. Als je doelen helder zijn, je je risico's goed inschat, je passende maatregelen ontwerpt, invoert en uitvoert, dan heb je redelijke zekerheid dat de werkelijkheid zich zal ontvouwen zoals jij het bij de 'P' van je PDCA-cyclus hebt bedacht. Als je daarentegen uitgaat van het principe dat deze wereld slechts beperkt beheersbaar is, dan heeft het bijvoorbeeld veel meer zin om in te zetten op agiliteit, de behendigheid van je organisatie om in te spelen op verander(en)de omstandigheden.

Wat integraal kans- en risicomanagement vooral uitdagend maakt, is dat het over de toekomst gaat. En die is nu eenmaal onzeker. Zo weet niemand of Bitcoin de valuta van de toekomst wordt of de volgende zeepbel. We kunnen alleen maar inschattingen maken. Verder zijn risico's niet tastbaar of aanwijsbaar. Het zijn conceptuele voorstellingen van toekomstige gebeurtenissen of omstandigheden. En daardoor voor iedereen verschillend. Het helpt ook al niet dat onze menselijke vermogens beperkt blijken te zijn, als het gaat over het bepalen van mogeljke gevolgen van gevolgen van gevolgen, etc. En dan heb ik het nog niet over alle moeilijkheden bij het bepalen van waarschijnlijkheden.

Mijn stelling bij het congres was: degenen die verantwoordelijk zijn voor het behalen van de organisatie-doelstellingen zijn ook verantwoordelijk voor het benutten van de kansen en het beheersen van de risico's. Er kan specialistische hulp nodig zijn bij het realiseren van die doelstellingen, bijvoorbeeld omdat de wet- en regelgeving complex is, omdat de technologieën snel wijzigen, etc. De eigenaren van de doelstellingen (en van de processen die nodig zijn om die te bereiken) moeten daarbij voortdurend afwegingen maken. Namelijk welke waarde zij willen creëren en behouden voor welke stakeholders.

Een essentieel aspect, dat vaak onderbelicht blijft, betreft de kernwaarden. Die bepalen namelijk welke stakeholders (en hun belangen) dominant zijn, wat het zwaarste weegt bij netelige kwesties en welk gedrag er wordt verwacht van managers en overige medewerkers. Dat heeft alles te maken met hun morele kompas en hun mentaliteit. In de praktijk komt dat regelmatig neer op de kwestie of geld het doel is of een middel? Ik hoorde onlangs dat pasgeboren kalveren in de bio-industrie poedermelk krijgen, omdat dat de boeren minder geld kost. Kun je in je bedrijfsmodel nog verder vervreemden van je oorspronkelijke doel? Want voor wie was die verse moedermelk in de eerste plaats ook weer bedoeld?

Kernwaarden gaan ook over de vraag of het doel de middelen heiligt. Je leveranciers uitknijpen (zoals zzp-ers standaard pas betalen na 90 dagen) helpt vast om je eigen werkkapitaal te optimaliseren, maar vind je dat ook 'normaal' (d.w.z. passend binnen jouw ethische kaders)? Medewerkers worden doorgaans geslecteerd op hun IQ en voor sommige functies tevens op hun EQ. Je zou je mensen vooral moeten kiezen op basis van gedeelde kernwaarden: ook wel hun "Spiritual Quotient" (SQ)

genoemd. Kernwaarden spelen overigens ook een sleutelrol bij het operationaliseren van het moeilijke begrip 'risicobereidheid' (en de tegenhanger 'kansbenutting').

De integratie van prestatiemanagement en risicomanagement kan worden aangeduid als 'waardemanagement'. Woorden als 'waarde' (evenals 'resultaat', 'succes' en 'verbetering') zijn echter vacuüm gezogen termen: op zich zeggen ze weinig. Je standaardvraag zou moeten zijn: wat bedoel je eigenlijk? Dat je er meer geld aan overhoudt? Dat het veiliger wordt? Of schoner, duurzamer, sterker of zuiniger? Of dat je medewerkers er gelukkiger van worden? ("Happy cows give more milk.") Vanzelf komt de discussie dan op waar deze over hoort te gaan: voor welke stakeholders willen wij welke waarde creëren en behouden?

Als het mij vraagt, blijft het moeilijkste aspect van het omgaan met kansen en risico's dat het over menselijk gedrag gaat. Het komt daarbij vooral aan op moed. Als iedereen 'hosanna' en 'halleluja' roept over een mogelijke overname, durf jij dan bijvoorbeeld als controller het aanstaande feestje te bederven, als de risico's volgens jou te groot zijn? Onder meer omdat de onderbouwingen in de business case boterzacht en flinterdun zijn. Of omdat de culturen voor geen meter aansluiten. Met die actie plaats je jezelf dan wel (deels) buiten de groep. En dat blijft voor iedereen erg lasting om te doen! Goede leiders waarderen echter juist tegengeluiden - in het belang van hun organisatie. Zij weten ook dat fouten mogen maken een onmisbare voorwaarde is om een "High Reliability Organization" te worden.

Bij het congres had ik de nodige tegenwerpingen verwacht van de aanwezige COSOïsten, ISOïsten, etc. Het tegendeel bleek het geval te zijn: er was ruime instemming dat de traditionele benaderingen slechts beperkt effectief gebleken zijn. De boeiende discussies die volgden geven veel inspiratie om te gaan ontdekken hoe we besluitvorming (keuzen maken met betrekking tot de toekomst) beter kunnen organiseren.