

overtollig risicomanagement

In de internal audit wereld wordt risicomanagement als iets vanzelfsprekends gezien. De IIA definitie van het eigen vakgebied refereert er aan: *It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*

Risicomanagement wordt doorgaans vormgegeven door na te gaan wat er in de toekomst allemaal mis kan gaan, daar allerlei beheersmaatregelen voor in te richten, te controleren of die ook werken en ze bij te stellen als dat nodig geacht wordt. Het is een managementsysteem naast andere zoals bijvoorbeeld quality, safety, information security, business continuity en compliance management.

Maar als risicomanagement het antwoord is, wat was dan ook alweer de vraag? Hoe goed helpt een risicomanagementsysteem beslissers bij het omgaan met onzekerheid en disruptie? Of gaat het eigenlijk meer om een *belief system*? Is er sprake van missionarissen, gelovigen en inquisiteurs die er belang bij hebben om het systeem in stand te houden? In hoeverre is het overtollig? Ofwel: wat mis je, als je er niet (meer) in gelooft?

Het is aansprekend om fouten te vermijden, ongelukken te voorkomen en onheilen af te wenden. Je kunt daar lastig tegen zijn. Interne specialisten en externe consultants grepen dit aan om organisaties te verbeteren. Het leidde tot codificatie van best practices. Overheden en regelgevers omarmden vervolgens deze standaarden als methoden om aantoonbaar te krijgen dat organisaties hun zaken op orde hebben. Aan risicomanagement doen werd zo gaandeweg gezien als kenmerk van goed organisatiebestuur.

In de 2004 editie van het COSO ERM Framework werd risicomanagement gezien als een proces. Als je dat nog niet had ingericht, dan stonden de adviesburo's in de rij om je te helpen bij de implementatie. Hoe meer het verplicht werd gesteld, des te lucratiever hun verdienmodel werd. Omvangrijke maturiteitsmodellen zorgden voor steeds meer toeters en bellen. Er werden allerlei speciale ERM en GRC applicaties ontwikkeld. Het is nu een multimiljarden bedrijfstak.

Wellicht heb jij je ook wel eens verbaasd over het steeds uitdijende jargon. Zo wordt er gesproken over 'risk governance' naast gewone governance, 'risk culture' naast de organisatiecultuur en 'risk owner' naast resultaatverantwoordelijke. Ook zou je 'risk intelligence' nodig hebben naast gewone mensen-intelligentie. Dit leidt ertoe dat veel risicospecialisten in een andere wereld leven dan hun medekantoortuinbevolkers.

In de praktijk wordt 'risico' geassocieerd met negatieve effecten op zaken die voor mensen waardevol zijn. Beslissers wegen echter steeds pro's én cons af. Expliciet en impliciet. Formeel en informeel. Dat geldt voor hun governancestructuren, bedrijfsprocessen en projecten. Ze moeten mogelijke voor- én nadelen afwegen bij het ontwerpen, uitvoeren, evalueren en verbeteren ervan. Het voortdurend vooruitkijken is inherent aan hun reguliere PDCA-cyclus, die bedoeld is om de waarschijnlijkheid van hun succes te vergroten.

We kennen geen wetenschap die 'risicologie' heet. Er is wel een op zichzelf staande risicomanagement-wereld gecreëerd. Die vervolgens uit alle macht moet worden geïntegreerd in de bestaande managementcyclus. Dat valt in de praktijk niet mee, want het gaat veelal over bijzondere concepten. Neem het begrip 'risico' zelf. Daar bestaat geen universele definitie van. Veelbetekenend is het dat ISO - de organisatie voor wereldwijde standaardisatie - zelf in haar publicaties meer dan 40 verschillende definities van risico gebruikt.

Bij risicomanagement trainingen en congressen tref je hoogst zelden bestuurders, lijnmanagers of projectleiders aan. Dat is best opvallend, omdat risicomanagement belooft dat het hen helpt om hun doelstellingen beter te halen. De meesten zijn niet achterlijk. Als het hen echt zou helpen, zouden zij dan niet vooraan zitten om te leren hoe ze er hun voordeel mee kunnen doen?

Ondertussen zijn er duizenden mensen in de weer met compliance-gedreven risicomanagement. Capaciteit die ook ingezet kan worden om de beslissers in hun organisaties te ondersteunen. Bij het eerlijk in beeld brengen van kansen én bedreigingen. Bij het maken van realistische scenario's en prognoses. Bij het evenwichtig afwegen van mogelijke pro's én cons bij belangrijke beslissingen. Bij het proactief managen van de verwachtingen van de klanten, financiers en toezichthouders.

Wat betekent dit voor internal auditors? Toekomstbestendigheid hangt niet zozeer af van risicoregisters, beheersraamwerken en testresultaten. Het hangt met name af van de kwaliteit van de besluitvorming. Als internal auditors waarde willen toevoegen, dan moeten zij vooral nagaan in hoeverre de beslissers binnen de organisatie capabel en integer zijn. Hebben zij toereikende competenties? Stemt hun mentaliteit overeen met de kernwaarden van de organisatie? Zijn zij zich bewust van belangrijke veronderstellingen in hun plannen en scenario's? Zorgen zij voor goede discussies bij dilemma's? Brengen zij de juiste deskundigen aan tafel? Stellen zij afwijkende inzichten op prijs? Wegen zij de belangen van hun kernstakeholders evenwichtig af?

Marinus de Pooter is zelfstandig gevestigd als interim professional, adviseur en trainer. Hij ondersteunt ondernemers, bestuurders en managers bij het toekomstbestendig houden van hun organisaties.