



TEKST – BIANCA VAN DEN BRINK
FOTOGRAFIE – FLICR

Sinds de invoering van het COSO Enterprise Risk Management Framework in 2004 is er veel veranderd in het landschap van organisaties en risicomanagement. Onlangs is een herziene versie uitgebracht. Het nieuwe model legt duidelijker de verbinding met de strategie van de organisatie en met prestatie management. Bovendien is er meer oog voor de invloed van leiderschap en cultuur. Gaat dit nieuwe model het verschil maken?

COSO

**Gaat COSO ERM 2017
het verschil maken?**

we are finance.

“In de herziene versie gaat het over waardecreatie én waardebescherming, over kansbenutting én risicobeperking, over mogelijke positieve én negatieve gevolgen. Eigenlijk gaat het dus gewoon over hoe je een organisatie runt”

Marinus de Pooter, ERM-expert en docent van de masterclass COSO ERM 2017 in de VRC Finance Academy, vindt de aanpassingen een welkome vernieuwing in een ‘VUCA’-wereld (Volatile, Uncertain, Complex, Ambiguous). “Opvallend is dat de definitie nu niet meer gaat over een ‘process’, maar over ‘the culture, capabilities, and practices’. En het model zelf ziet er dynamischer uit dan de bekende kubus”, aldus De Pooter. Hij geeft aan dat ook is gepoogd om de relatie met prestatie management duidelijker te leggen. De component die gaat over het identificeren, analyseren en adresseren van risico’s heet nu ‘Performance’.

Volgens De Pooter ademde het vorige raamwerk sterk de geest van maakbaarheid dat we kennen van het gedachtegoed van planning & control. “Als je je doelen maar scherp hebt, een goede risicoanalyse doet, passende maatregelen treft en die ook nog eens controleert, dan heb je redelijke zekerheid dat de werkelijkheid zich gaat ontvouwen zoals jij die hebt bedacht. Maar in een VUCA-wereld organiseer je dan je eigen frustratie. Het is gevaarlijker om jezelf niet voortdurend aan te passen dan om afwijkingen van je verwachtingen meteen als ‘ongewenst’ te beschouwen.”

Van silo naar integratie

Het voorgaande raamwerk resulteerde in de praktijk vaak in een aparte ‘risicomanagement-silo’. Het ontaarde in een proces, programma, functie, afdeling en commissie, los van de rest van de organisatie. In sommige sectoren is dat zelfs voorgeschreven door toezichthouders. Volgens De Pooter is risicomanagement iets dat moet worden geïntegreerd met de business. “Als bestuurder, lijnmanager of projectleider moet je steeds de kansen benutten én de risico’s beperken. Dat kun je het best in samenhang doen en niet door een afzonderlijk systeem te creëren dat gericht is op het mitigeren van mogelijke onheilen. In de herziene versie gaat het over waardecreatie én waardebescherming, over kansbenutting én risicobeperking, over mogelijke positieve én negatieve gevolgen. Eigenlijk gaat het dus gewoon

over hoe je een organisatie runt. De term risicomanagement werkt dan overigens niet mee, omdat mensen bij risico intuïtief denken aan zaken die je beter niet kunt hebben.”

Leiderschap en gedrag

In de nieuwe editie is er volgens De Pooter meer aandacht voor leiderschap en cultuur: “Als je het mij vraagt, zijn dat dé bepalende factoren. Bij sommige organisaties is het niet erg populair om te spreken over zaken die fout zijn gegaan (incidenten) en die fout kunnen gaan (risico’s). Terwijl goede, inhoudelijke discussies over de veronderstellingen je bedrijfsplannen juist realistischer maken.”

De aandacht voor het belang van leiderschap en cultuur is belangrijk, omdat de mentaliteit van de organisatieleiding bepaalt welke belangen bij beslissingen prevaleren. “Competenties en intenties van leidinggevend zijn cruciaal voor het succes van organisaties”, aldus De Pooter. “In deze editie is meer aandacht voor de effecten van beloning. Dat juich ik zeker toe, vanwege de invloed ervan op het gedrag van mensen.” Maar hoe je als beslisser een passende balans kunt vinden tussen enerzijds ‘opportunities’ en mogelijke ‘rewards’ en anderzijds ‘risks’ en mogelijke ‘penalties’ blijft volgens hem ook in het

nieuwe model mistig. “Daarnaast had ik graag gezien dat er meer handvatten waren geboden hoe je als organisatieleiding een passende invulling kunt geven aan de twintig principes die worden behandeld. Dat kan de kwaliteit van de besluitvorming in de praktijk alleen maar ten goede komen.”

De bijdrage aan evenwichtige besluitvorming is volgens De Pooter de enige echte toegevoegde waarde van het gestructureerd denken over kansen én risico’s. Dat geldt met name bij het bepalen van de missie, visie, strategie en doelen van de organisatie. De belangrijke analyses van mogelijke voor- en nadelen bij het bepalen van het businessmodel komen in het nieuwe COSO ERM model echter minder goed uit de verf. Ook deze editie kan er volgens hem toe leiden dat mensen (kans- &) risicomanagement blijven zien als een doel op zich. En niet primair als een hulpmiddel om na te gaan in hoeverre je als directie- of managementteam je organisatie voldoende toekomstbestendig houdt.

De Pooter: “Uit onderzoeken komt naar voren dat maar weinig bestuurders risicomanagement ervaren als iets dat hen helpt om hun strategie te bepalen en te realiseren. Het is veelzeggend dat zij het blijkbaar niet associëren met succes. De meeste leidinggevenden beleven het meer als ‘compliance corvee’. En het is nog maar de vraag of met deze gegroeide perceptie COSO ERM 2017 het verschil gaat maken.”

Marinus de Pooter is docent van de masterclass COSO ERM 2017 bij de VRC Finance Academy. Hij is directeur, consultant en docent in de vakgebieden governance, risk management & compliance, internal control, compliance, internal audit en finance. Centraal in zijn benadering staat het succes van organisaties, dat afhangt van hun vermogen om waarde te creëren en te beschermen.