ORGANISEREN VAN INTERNAL CONTROL; VALKUILEN EN KANSEN

Door Mario Cornel

June 2017

Het beheersen van risico's (en kansen) bepaalt de continuïteit en performance van organisaties en staat dan ook onverminderd op de bestuursagenda. Dit als gevolg van:

- de impact op bedrijfsimago/branding bij missers in bijvoorbeeld financiële verslaglegging;
- de onverminderde druk van wet- en regelgeving en
- de steeds korter durende productlevenscycli en bijbehorende rendementen.

Het behalen van de bedrijfsdoelstellingen zonder aantoonbare organisatie van risicobeheersing is voor stakeholders, waaronder aandeelhouders, management en toezichthouders, nooit voldoende. Hoe risicobeheersing te organiseren is voor veel organisaties een periodiek terugkerend thema en is o.a. afhankelijk van de omvang en complexiteit van de organisatie, de systemen, de strategie en het verdienmodel. Daarbij staan centraal het periodiek herijken van risico matrices, het bepalen van de te accepteren risico's en van de te nemen beheersmaatregelen en uiteindelijk het inbedden van de beheersmaatregelen in de bedrijfsvoering. Een belangrijk onderdeel daarvan zijn het scherp maken van de rollen en verantwoordelijkheden tussen business, finance, internal control/internal audit.

De vier meest voorkomende valkuilen (en dus ook kansen) in de organisatie van beheersing en risico management zijn:

- ✓ **Scoping en detail**

Vaak richt het management zich op de volledigheid van het risicoregister in plaats van focus op de relevante top-risico's. De toegevoegde waarde van risicomanagement zit niet in die juistheid en volledigheid van de risico vastlegging en de veelheid aan beheersmaatregelen, maar juist in het creëren van bewustwording en doorvoeren van adequate beheersmaatregelen op met name de relevante risico's. Een lijst met de twintig belangrijkste risico's die concreet worden beheerst, zegt meer dan een

gedetailleerde lijst met honderden mogelijke risico's. Een voorbeeld van tooling op basis waarvan een priorisering kan gemaakt binnen LeanSixSigma gedachtegoed is *Risk Priority Numbering*. De kwantificering van 'Impact' maal 'Kans' maal 'mitigerende werking van de bestaande beheersmaatregel' kan behulpzaam zijn.

- ✓ **Commitment van management**

Management is vaak onvoldoende sponsor in de inrichting en keuzes in de formalisering van Het beheersen van risico's (en kansen). Een belangrijke voorwaarde voor succesvol risicomanagement is dat de directie en bijbehorend management team belang hecht aan de toegevoegde waarde ervan, dit ook ondersteunt en er actief bij betrokken is. De belangrijkste risico's van de organisatie moeten dus vooral ook op de bestuursagenda staan van directie met sturing op de gekozen beheersmaatregelen (de 'controls').

- ✓ **Integrale aanpak**

Wat lastig blijkt en bij veel organisaties ontbreekt, is een integrale aanpak.

Vanuit een organisatie breed perspectief de risico's identificeren, kwantificeren en vervolgens de beheersmaatregelen implementeren blijft in veel gevallen een ambitie. Aanpak binnen business units/afdelingen/profit centers is vaak eenvoudiger; we zijn immers minder afhankelijk van brede afstemming en de soms verschillende processen/systemen dan bij een integrale aanvliegroute. Bij een integrale aanpak waarbij alle relevante disciplines van het bedrijf betrokken zijn is er betere aansluiting bij bedrijfsstrategie te verwachten die immers afdelingen/profit centers overstijgt. Normaliter is het management team een goede representatie omdat alle disciplines hierin vertegenwoordigd zijn.

- ✓ **Integratie in management control cyclus**

Als risicomanagement géén onderdeel uitmaakt van de planning en control cyclus verwordt het tot een losse discipline die in de praktijk vooral wordt gebruikt om externe toezichthouders tevreden te stellen met focus op documentatie. Dan wordt risicobeheersing als rem ervaren op het behalen van doelstellingen in plaats van als katalysator.

De huidige COSO richtlijn geeft een goed beeld van wat van het management verwacht wordt. Dit alom toegepaste model bestaat uit een raamwerk dat 3 dimensies kent, te weten organisatiedoelstellingen, organisatiestructuur en de 5 componenten die bepalend zijn voor behalen van genoemde organisatie doelstellingen.

Deze 5 componenten zijn:

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Ontleent aan https://www.coso.org/Documents/2014-2-10-COSO-Thought-Paper.pdf

Het bovenstaande raamwerk moet vooral gezien worden als een middel om internal control te organiseren. Van een noodzakelijk ongemak dat alleen controleert en documenteert, tot een beheerstructuur dat met een grotere reikwijdte en bredere blik op risico's zijn toegevoegde waarde toont.

Met de huidige roep om veerkrachtige strategieën ('strategy & business resilience') zorgt het periodiek toetsen van alle 5 onderdelen van deze structuur dat de onderneming in staat blijft om risico's (en kansen) te blijven beheersen.

De 4 bovengenoemde valkuilen komen met name voort uit onvoldoende borging van de Plan Do Check Act (PDCA) cyclus van deze 5 onderdelen.

Door los van dit raamwerk ‘lines of defence’ te organiseren met interne- en externe audits ligt het risico op de loer dat de echte risico’s over het hoofd worden gezien, lijnverantwoordelijkheden in de staf blijven belegd en daarmee vooral wordt gebruikt om externe toezichthouders tevreden te stellen met focus op documentatie.

Is dit eenvoudig op te lossen? Het vereist focus op gezamenlijk optrekken vanuit het management, capaciteit structureel inzetten op het periodiek doorlopen van de vijf stappen en de bewustwording dat het lijn management verantwoordelijk blijft voor haar processen en beheersmaatregelen als onderdeel van de reguliere bedrijfsvoering.

Mario Cornel, Managing Consultant bij RGP