Focus op verbeteren

Partner van associates partners in beweging

Risicomanagement:

een pragmatische benadering

in tien stappen

0. Inleiding

Risicomanagement is zo oud als de mens. De holbewoner deed al aan risicomanagement door ’s nachts het vuur aan te steken in de grot om wilde dieren op afstand te houden.
Het proces van risicomanagement vond tot ver in de vorige eeuw meestal impliciet plaats, ook in organisaties.

In het rapport van de eerste Nederlandse corporate governance commissie “Commissie Peters” in 1997 werd echter opgenomen “dat de Raad van Bestuur de risico’s verbonden aan het gekozen beleid onderscheidenlijk de strategie **schriftelijk** aan de Raad van Commissarissen zal rapporteren.” Genoemde code heeft model gestaan voor de vele latere governance codes in profit en not-for-profit sector, waarbij ook het woord “risicomanagement model” ten tonele is verschenen.

Er zijn verschillende goede modellen voor integraal risicomanagement. De keuze voor een bepaalde norm hangt af van wat een organisatie belangrijk vindt: status/bekendheid (COSO, ISO), praktische hulpmiddelen (M_o_R), toegankelijkheid (ISO, M_o_R) of specifiek de publieke sector (INTOSAI).

Deze risicomanagementmodellen (die in de bijlagen beknopt zijn beschreven) bieden structuur en geven handvatten, waardoor ze bijdragen aan het slagen van de implementatie van integraal risicomanagement.
Ongeacht het gekozen model zijn een juiste positionering in de organisatie, expliciete steun vanuit de top en ondersteuning en stimulering van risicobewustzijn bij individuele managers de sleutels tot succes. Gedragsverandering speelt bij het invoeren van risicomanagement een belangrijke rol.

Ondanks de beschikbaarheid van en de aandacht voor risicomanagementmodellen blijkt het implementeren van risicomanagement, met name ook voor middelgrote en kleinere organisaties, nog een weerbarstige operatie. Gezien het steeds hogere tempo van nieuwe ontwikkelingen is de noodzaak van goed en expliciet risicomanagement echter alleen maar toegenomen.

Dit document beoogt inzicht te geven in wat risicomanagement nu precies is en reikt een handzaam model en een stappenplan aan om risicomanagement in de praktijk op een pragmatische wijze handen en voeten te geven.

De opbouw van dit document is als volgt:

Bijlagen:

Wilt u meer weten of van gedachten wisselen?

Mail info@focusopverbeteren.nl en ik neem contact met u op.

niet instaan voor de juistheid, volledigheid en actualiteit van de geboden informatie en wijst iedere aansprakelijkheid ten aanzien van het gebruik van de geboden informatie uitdrukkelijk van de hand.

1. Theoretisch kader

1.1 Algemeen

Risicobeheer of risicomanagement is een continu ‘plan-do-check-act’ proces dat ten aanzien van de doelstellingen risico's identificeert en beoordeelt.
Er bestaan verschillende definities van risicomanagement. In deze position paper gebruiken wij de definitie van Committee of Sponsoring Organisations of the Treadway Commission (COSO), waarbij het woord onderneming is vervangen door organisatie omdat risicomanagement ook in not-for-profit organisaties toepasbaar en wenselijk is:
‘Het risicomanagement van organisaties is een proces dat bewerkstelligd wordt door het bestuur van de organisatie, het management en ander personeel en wordt toegepast bij het formuleren van de strategie en binnen de hele organisatie, ontworpen om potentiële gebeurtenissen die invloed kunnen hebben op de organisatie te identificeren en om risico’s te beheren zodat deze binnen de risico acceptatiegraad vallen, om een redelijke zekerheid te bieden ten aanzien van het behalen van de organisatiedoelstellingen’.

Belangrijke argumenten om risicomanagement als proces in te richten zijn:

- Risicomanagement kan organisaties inzicht geven in wat kan gebeuren.
- Risicomanagement stelt organisaties in staat om prioriteiten toe te kennen aan onderkende risico’s en daardoor gestructureerd acties te ondernemen, waardoor lukrake acties voorkomen kunnen worden.
- Risicomanagement maakt het organisaties mogelijk om bij besluitvorming een betere financiële afweging te maken om maatregelen te treffen.
- Risicomanagement maakt het voor organisaties mogelijk om genomen beslissingen aangaande risico’s te verantwoorden.

1.2 Risico, risicobereidheid en risicoprofiel

Risico is de kans dat een gebeurtenis plaatsvindt, vermenigvuldigd met het gevolg van die gebeurtenis, kortgezegd: risico = kans x effect.

De **risicobereidheid** (de ‘risk appetite’) is een beeld op hoog abstractieniveau van de hoeveelheid risico dat het bestuur en het management willen lopen of accepteren bij het nastreven van hun doelstellingen. De risicobereidheid wordt uitgedrukt als het niveau van risico dat een organisatie bereid is te lopen of te accepteren tijdens het leveren van waarde aan stakeholders. De risicobereidheid bepaalt de aard en diepgang van de beheersingsmaatregelen.

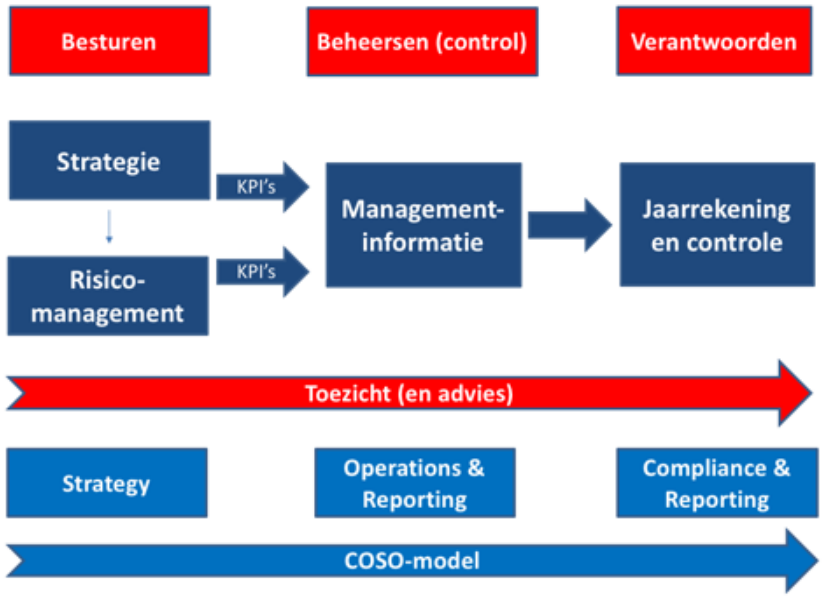
Op basis van de risico-inventarisatie en de risicobereidheid kan het **interne risicoprofiel** worden bepaald. Na implementatie van beheersmaatregelen resteert het **externe risicoprofiel**.

Volgtijdelijk ziet dit proces er als volgt uit:

Het is onmogelijk om alle risico's op een bepaald moment te kennen, laat staan deze volledig te beschrijven en te beheersen. Daarom richt het risicobeheersing- en controlesysteem zich op de belangrijkste risico's. Dit zijn de risico's die van wezenlijke invloed kunnen zijn op de uitkomsten van geformuleerde doelstellingen (strategy & operations), van belang zijn voor de kwaliteit van de verslaggeving (reporting) en het vermogen om te voldoen aan wet- en regelgeving (compliance).

1.3 Plaats in de organisatie

Goed organisatiebestuur kan worden weergegeven als de vier functies Bestuur, Beheersen (control), Verantwoorden en Toezicht die met elkaar samenhangen.



Het bestuur van een organisatie is eindverantwoordelijk voor de strategie en daarmee ook voor het identificeren en monitoren van de risico's die de 'drivers' van de strategie kunnen bedreigen.

Hiervoor zijn veel goede modellen in omloop. Omdat de interne en externe omgeving voortdurend aan wijzigingen onderhevig zijn is continue monitoring van het gekozen risicomanagementmodel een vereiste.

1.4 Risicomanagementmodel

Modelmatig kan risicomanagement als volgt worden weer gegeven:

Beheersen van risico's		
	Passief	Actief
Effect hoog	Overdragen	Vermijden/ elimineren
Effect laag	Accepteren	Reduceren
	Kans laag	Kans hoog

Reduceren		
	Reduceer kans	Reduceer effect
Preventief	* Procedures * Regels en regulering * Opleiding en training	* Communicatie * Contractuele afspraken * Proces-monitoring
Repressief	* "Lessons learned"	* Garantie en service

Bron: Bedrijfsvitaliteit/Van Heeswijk

De verschillende kwadranten kunnen als volgt nader worden toegelicht:

Kans laag – effect laag
Dit zijn risico's die kunnen worden geaccepteerd zonder verdere actie. Accepteren kan door bewust aangaan, consequenties financieren of het incalculeren van de onzekerheid.

Kans laag – effect hoog
Dit zijn risico's die organisaties vanwege hun potentiële omvang niet wil lopen maar die niet zelfstandig te beheersen zijn. Overdragen kan door verzekeren, delen, contracteren, diversificeren of hedgen.

Kans hoog, effect hoog
Dit zijn risico's die organisaties vanwege hun potentiële omvang niet willen lopen maar die niet over te dragen zijn aan derden en daarom bij ontdekking zo snel mogelijk moeten worden geëlimineerd. Elimineren kan door het beëindigen van activiteiten, desinvesteren, het veranderen van doelen of het verkleinen van de schaal. Toekomstgericht denken speelt bij deze risico's een steeds belangrijker rol.

Kans hoog, effect laag
Dergelijke risico's worden gereduceerd zodra ze ontdekt worden. Voor deze risico's onderkennen we vier reductiemogelijkheden die per risico, al dan niet in combinatie, worden toegepast:

- Reduceer de kans preventief.
- Reduceer de kans repressief.
- Reduceer het effect preventief.
- Reduceer het effect repressief.

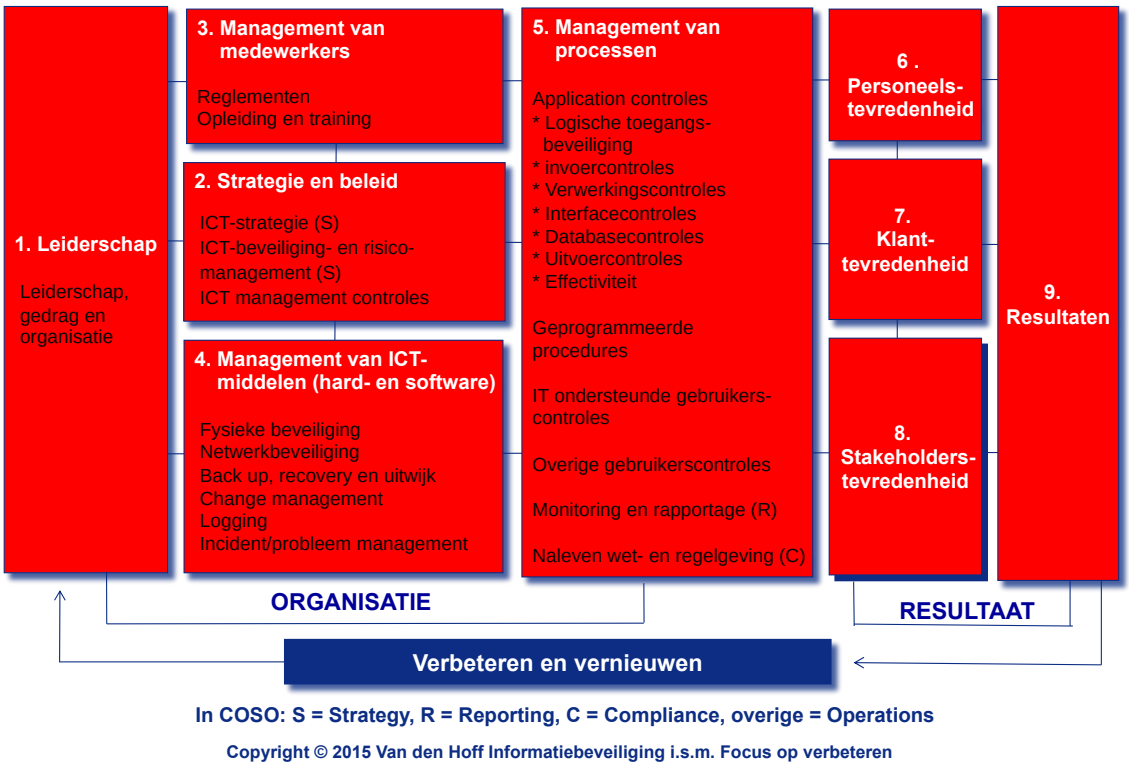
De reductiemaatregelen van de risico's 'Effect hoog/kans laag' en 'Effect laag/kans hoog' zijn normaliter geborgd in de maatregelen van administratieve organisatie en interne controle.

De risico's 'Effect hoog/kans hoog' worden (te) vaak uitsluitend benaderd vanuit het bestaande referentiekader. Toekomstgericht (en out of the box) denken zijn echter essentieel om deze risico's beter te kunnen beheersen.

1.5 INK-model

Het is verstandig om op een gestructureerde wijze naar mogelijke risico's te kijken. Een handzaam manier hiervoor is het INK-model, dat ook eenvoudig aan het veelgebruikte COSO-model te koppelen is en als 'bril' kan worden gebruikt. Organisatie breed ziet dit model er als volgt uit:

Het onderdeel 5 ICT kan daarbij als volgt worden verdiept:



1.6 Verschillen tussen bedrijfsonderdelen

Het is niet per definitie zo dat geïdentificeerde risico's of gedefinieerde beheersmaatregelen integraal van toepassing zijn op alle onderdelen van de organisatie. Er kan sprake zijn van kleinere organisatieonderdelen met afwijkende risico's of waar onvoldoende mogelijkheden voor functiescheiding bestaan, van buitenlandse vestigingen met andere of aanvullende wet- en regelgeving, van verschillen tussen divisies, van afwijkende bedrijfsactiviteiten of een mix hiervan.
In de risicoanalyse dient te worden onderkend welk effect deze afwijkingen hebben op de kwaliteit van de interne controle, en hoe eventueel daaruit voortvloeiende leemten zijn afgedekt. Veelal zal sprake moeten zijn van aanvullende controles, bijvoorbeeld vanuit de centrale leiding.

1.7 Soft controls

De praktijk heeft geleerd dat organisaties, ondanks de aanwezigheid van uitgebreide risicomanagementsystemen, in grote problemen kunnen komen of zelfs failliet gaan.
Daarom is het noodzakelijk om, naast het implementeren van alle formele beheersmaatregelen, ook te sturen op cultuur en waarden en bijbehorende 'soft controls'.

1.8 Beschrijving risicomanagementactiviteiten

Het verdient sterke aanbeveling de risicomanagementactiviteiten van de organisatie, waaronder het gekozen model, de verzekerde risico's, de maatregelen van toekomstgericht denken en de opzet en monitoring op bestaan en werking van de AO/IC beknopt vast te leggen in een 'Interne Controle Raamwerk' (hierna: ICR).

De ervaring leert dat bij het opstellen van een ICR in meerdere of mindere mate altijd risico's of leemten in de AO/IC blijken die tot dan toe onder de radar waren gebleven.

Het opstellen van een ICR heeft een aantal voordelen:

- De opsteller(s) van het ICR worden gedwongen om organisatie breed nog eens na te gaan hoe het ook alweer zat met het risicomanagement en de monitoring daarvan. Het lijkt logisch om de financieel eindverantwoordelijke binnen de organisatie hierbij een belangrijke rol te geven omdat de financiële functie raakvlakken heeft met alle onderdelen van de organisatie en daardoor een goed overzicht heeft.
- Het kennisnemen van het ICR door interne belanghebbenden als bestuurders, MT-leden, sparringpartners en commissarissen/toezichthouders draagt bij aan de bewustwording bij betrokkenen en verbetert daardoor ook de signalering zoals genoemd bij 'Kans hoog, effect hoog'.
- Het ICR kan desgewenst worden gedeeld met externe stakeholders als financiers of partijen waarmee strategisch wordt samengewerkt.
- Door het ICR periodiek (bijvoorbeeld jaarlijks tijdens het begrotingsproces) opnieuw te herijken en vast te stellen ontstaat een levend document dat, nadat het eenmaal is opgesteld, eenvoudig is te onderhouden. Tevens blijft daardoor de kennis binnen het management actueel.

Het ICR moet wel volledig maar niet te uitgebreid zijn en een duidelijke structuur volgen.

De structuur is vormvrij, maar kan er bijvoorbeeld zo uitzien (vrij naar het INK-model):

- Algemeen: generieke omschrijving van de onderneming (missie en visie, kernwaarden, organisatiestructuur, omvang, activiteiten, geografische spreiding).
- Gekozen risicomodel.
- Beschrijving overgedragen risico's (waaronder verzekeringsportefeuille).
- Beschrijving risico's kans en effect hoog (inclusief beheersmaatregelen).
- Beschrijving Administratieve Organisatie en Interne Controle inzake te reduceren risico's:
    - Strategie (businessplan, resultaten van PESTEL-analyse, sterkte/zwakte analyse, BCG-matrix).
    - Personeel (kwaliteit, beschikbaarheid, flexibiliteit).
    - ICT-middelen (management en organisatie van de ICT, logische toegangsbeveiliging, wijzigingsbeheer, incident-/probleemmanagement, fysieke beveiliging, back up en herstel, uitwijk).
    - Overige middelen (huisvesting, machines en installaties, voorraden, financieringsmiddelen).
    - Processen (verkopen, inkopen, productie/primair proces, kwaliteitszorg, innovatie, communicatie).
    - Financiële functie en rapportage.
    - Voldoen aan wet- en regelgeving (governance structuur, ingeregelde bevoegdheden, opmaken en deponeren jaarrekening, fiscale zaken, juridische zaken, contractbeheer, algemene voorwaarden, fraudebeleid e.d.).
    - Personeelstevredenheid.
    - Klanttevredenheid.
    - Stakeholdertevredenheid.
    - Resultaten.

1.9 Periodieke organisatiedoorlichting

Door het hoge tempo van externe ontwikkelingen is het verstandig om de strategie en het verdienmodel minimaal jaarlijks te toetsen met behulp van:

- PESTEL-analyse (Politieke, Economische, Sociale, Technologische, Ecologische en Legal factoren);
- Het vijfkrachtenmodel van Porter;
- BCG-matrix (kwaliteit productportfolio);
- SWOT-analyse;
- Fase in levenscyclus;
- Vlootschouw personeel.

1.10 Risicomanagement en waardeontwikkeling

De resultante van de strategie zijn de toekomstige kasstromen. De contante waarde hiervan geeft voor commerciële bedrijven de ondernemingswaarde weer. De contante waarde wordt onder meer bepaald door de risico-opslagen in de disconteringsfactor. Door periodiek (bijvoorbeeld om de twee of drie jaar) de ondernemingswaarde uit te rekenen kan de waardecreatie (of waardevernietiging) in de tijd expliciet worden gemaakt.

2. Samenvatting

Het stappenplan voor risicomanagement kan als volgt worden samengevat:

1. Beleg risicomanagement bovenin de organisatie.
2. Introduceer een risicomanagementmodel dat passend is voor uw organisatie.
3. Ontwikkel op een gestructureerde wijze toekomstgericht denken in uw organisatie.
4. Integreer risicomanagement in uw bestaande planning & control cyclus (strategie, begrotingsprocedure, kritische performance indicatoren, managementinformatie, managementoverleg, actie/bijsturing, jaarverantwoording).
5. Evalueer periodiek uw verzekeringsportefeuille.
6. Beschrijf het Interne Controle Raamwerk, actualiseer dit periodiek en neem gestructureerd actie op gesignaleerde leemten.
7. Besteed in het Interne Controle Raamwerk specifiek aandacht aan afwijkende organisatie-onderdelen.
8. Zorg voor goede “soft controls”.
9. Toets jaarlijks de actualiteit van de strategie en het verdienmodel.
10. Laat om de twee à drie jaar een waardebepaling uitvoeren om de waardeontwikkeling van de onderneming te monitoren.

3. Bronnen en relevante literatuur

- Corporate Governance in Nederland – De Veertig Aanbevelingen, Commissie Peters 1997
- COSO Enterprise Risk Management Framework - Committee of Sponsoring Organisations of the Treadway Commission, 2004
- Een continue afweging van risico's tegen genoegens – Koster en Snijders, Tac, 1997
- Guidelines for Internal Control Standards for the Public Sector - International Organization of Supreme Audit Institutions, 2004
- ISO guide 73 – International Organization for Standardization, 2009
- M_o_R® (2007) - Office of Government Commerce, 2007
- Risicomanagementmodel (par.1.3) – www.bedrijfsvitaliteit.nl, drs. G.E. van Heeswijk MFSME
- www.hm-treasury.gov.uk
- www.wikipedia.nl

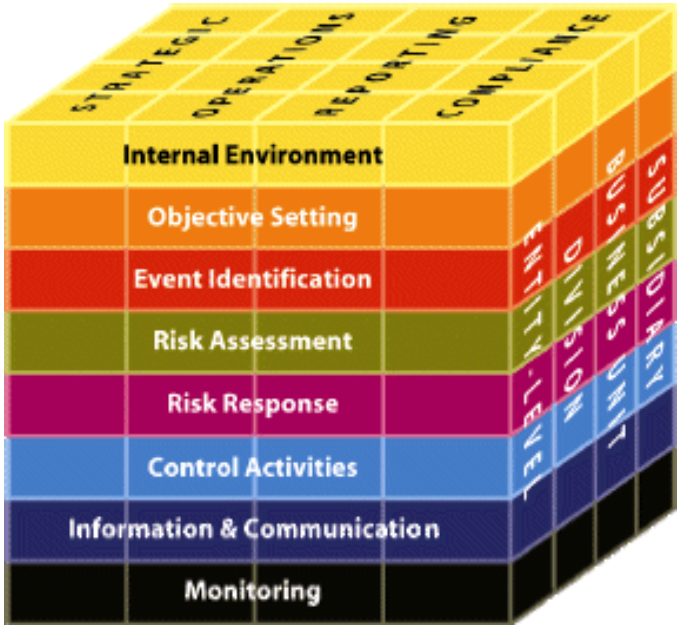
Bijlage 1. COSO Enterprise Risk Management Framework (COSO ERM)

COSO is één van de meest gebruikte management modellen ter wereld en is ontwikkeld door The Committee of Sponsoring Organizations of the Treadway Commission (COSO).
Dit comité, bestaande uit een aantal private organisaties, heeft in 2002 naar aanleiding van een aantal boekhoudschandalen en fraudegevallen bij Amerikaanse bedrijven aanbevelingen gedaan en richtlijnen aangegeven ten aanzien van interne controle en interne beheersing.
Dit rapport is bedoeld om aan organisaties een uniform en gemeenschappelijk referentiekader voor interne controle te bieden en om het management te ondersteunen bij de verbetering van het interne controlesysteem.
In 2004 werd het model geactualiseerd, en werden er elementen toegevoegd en aangepast.
Dit geactualiseerde model richt zich niet meer alleen op interne controle maar op het gehele interne beheersingssysteem en staat bekend als *COSO II* of *Enterprise Risk Management Framework* (ERMF).

De werking van COSO

Als een organisatie haar doelstellingen wil bereiken dan moet ze omgaan met risico's en moet ze deze risico's proberen te beheersen. COSO beschrijft en definieert hiervoor de verschillende elementen van een intern beheersingssysteem. Het model geeft in de COSO-kubus de directe relatie weer tussen:

- de doelstellingen van een organisatie(bovenvlak);
- de controlecomponenten(voorvlak);
- de activiteiten/eenheden waarvoor de interne controle benodigd is (zijvlak).



Figuur 1: COSO ERM.

Organisatiedoelstellingen

COSO identificeert de relaties tussen de ondernemingsrisico's en het interne beheersingssysteem. COSO hanteert hierbij de gedachten dat interne beheersing een proces is dat gericht is op het verkrijgen van een redelijke mate van zekerheid omtrent het bereiken van doelstellingen in de categorieën:

- Bereiken van de strategische doelstellingen (Strategic);
- Effectiviteit en efficiëntie van bedrijfsprocessen (Operations);
- Betrouwbaarheid van de (financiële) informatieverzorging (Reporting);
- Naleving van relevante wet- en regelgeving (Compliance).

Controlecomponenten

Vervolgens definieert het model de controlecomponenten van een organisatie als:

- Interne omgeving (de mate waarin risico's worden genomen (de risicobereidheid van een organisatie wordt hierin gedefinieerd, ook wel risk appetite genoemd);
- Bepaling van doelstellingen (objective setting);
- Identificatie van de gebeurtenissen (kansen/risico's die een positieve of negatieve invloed kunnen hebben op het behalen van de doelstellingen);
- De risico-inschatting of de beoordeling van de geïdentificeerde risico's (waarschijnlijkheid dat risico zich zal voordoen en de gevolgen indien het zich voordoet);
- De risicobeheersingsmaatregelen (risk response) - (risico's vermijden, aanvaarden, delen of verminderen);
- Controleactiviteiten (bijvoorbeeld functiescheiding);
- Informatie en communicatie;
- Monitoring.

Activiteiten

Tenslotte worden de activiteiten weergegeven waarvoor interne controle benodigd is en deze worden onderscheiden in vier niveaus op basis van de geldende organisatiestructuur.

Al deze componenten vormen samen een geïntegreerd systeem dat aan de veranderende omstandigheden kan worden aangepast.

Sterke punten

Het voordeel van de COSO-aanpak is dat het een internationaal geaccepteerde standaard is, die in Nederland met name door de beursgenoteerde bedrijven gebruikt wordt. Het feit dat in governance codes (zoals Sarbanes Oxley en Tabaksblat) expliciet naar COSO wordt verwezen maakt het model algemeen en ook door accountants geaccepteerd. Door aan te haken bij COSO geeft een organisatie een helder signaal dat zij risicomanagement serieus neemt. Zeer sterk is de beschrijving van de eerste stap van het proces, het vaststellen van de interne control. De componenten zijn goed uitgelegd.

COSO 2 maakt een helder onderscheid tussen de verschillende doelstellingen welke door vele organisaties is gebruikt om risico's te clusteren:

- Strategisch: betreft globale doelen en is afgestemd op de missie;
- Operationeel: betreft effectief en efficiënt gebruik van de middelen;
- Rapportage: betreft betrouwbaarheid van verslaggeving;
- Toezicht: betreft naleving van wet- en regelgeving.

De eerste twee doelstellingen gaan meer uit van ondernemingsrisico's, waarbij externe risico's die niet altijd beïnvloedbaar zijn door de organisatie op een efficiënte en effectieve wijze moeten worden gemanaged. Van belang zijn:
a) transparantie naar bestuur en toezichthouders over in welke mate men met deze risico's omgaat, en
b) in welke mate de organisatie zich beweegt richting het realiseren van de doelstellingen.

De laatste twee doelstellingen rondom toezicht en rapportage zijn de verplichte nummers, hieraan moet de organisatie gewoon voldoen.
Het hoofdstuk 'taken en verantwoordelijkheden' is bruikbaar om de juiste rolverdeling te bepalen, met name omdat de rollen van externe partijen – accountant, toeleveranciers en zelfs de financieel analisten en de media – worden omschreven. Al met al is COSO een goed model om vast te stellen wat er van een organisatie verwacht wordt ten aanzien van risicomanagement.

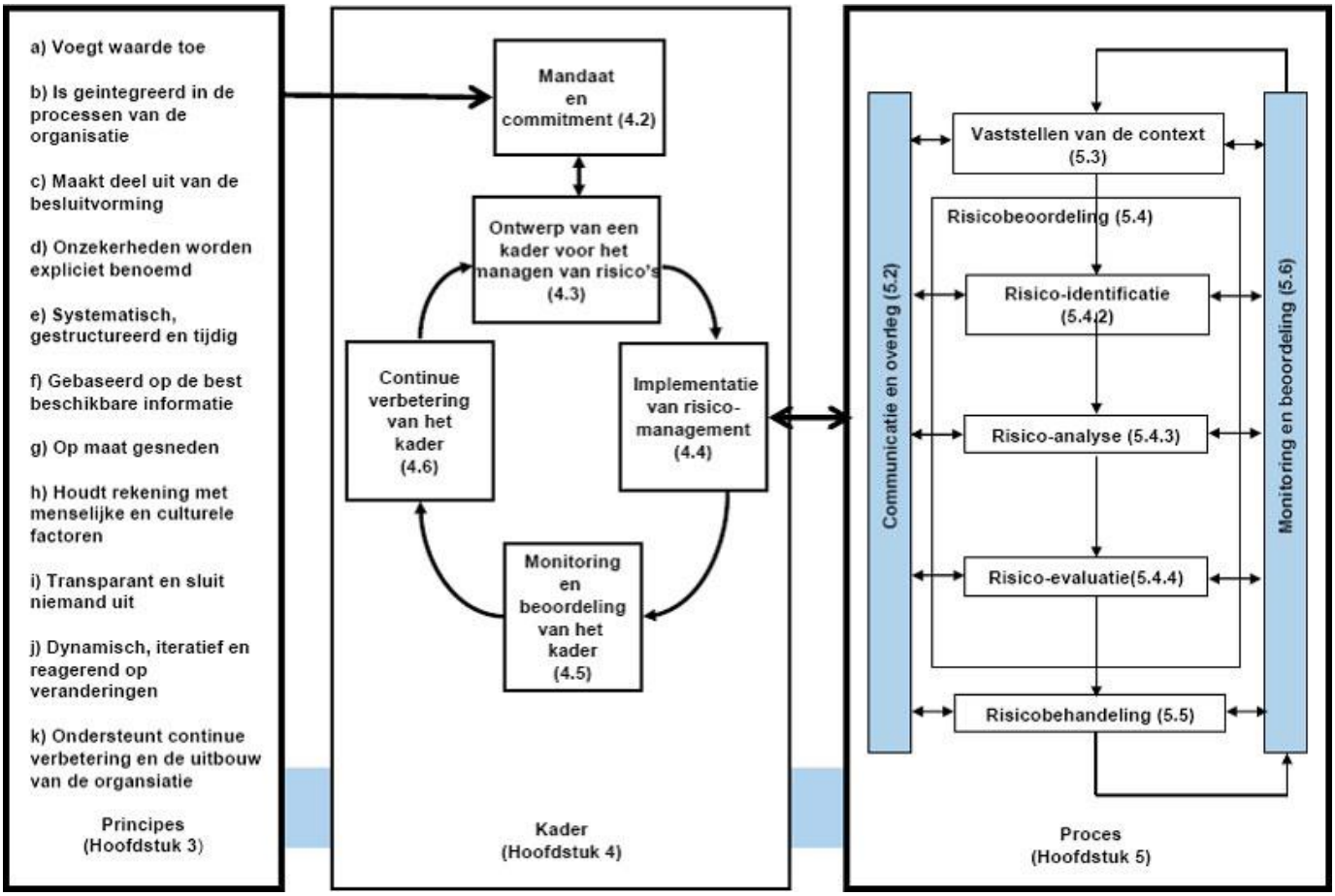
Bijlage 2. ISO 31000

In 2005 stelden Japan en Australië samen voor om een algemene ISO-richtlijn voor de principes en implementatie van risicomanagement te ontwikkelen. Bij gebrek aan beter bleken veel organisaties hun toevlucht te nemen tot de Australisch-Nieuw-Zeelandse norm AZ/NZS 4360.
De doelstelling die men met de nieuwe norm wilde bereiken was tweeledig. Ten eerste om een algemeen kader (best practice-model) te bieden voor organisaties die risicomanagement in de meest brede zin in de praktijk willen brengen. Ten tweede om als paraplu te dienen voor allerlei sector- en onderwerpspecifieke ISO-normen op het gebied van risicomanagement.

De werking van ISO31000

ISO 31000 bestaat uit de volgende 3 hoofdonderdelen (zie ook figuur 2 op de volgende bladzijde):

- Principes voor risicomanagement
  De principes vormen het fundament waarop risicomanagement moet zijn gebaseerd, wil het een positieve bijdrage leveren aan het functioneren van een organisatie.
  Kader
  Dit omvat de beleidscyclus (draagvlak, risicobeleid, contextanalyse, implementatie, monitoring, review en verbetering), waarin de bekende PDCA-cyclus is te herkennen. Het raamwerk vormt het kader voor aansturing van alle risicomanagementprocessen in de organisatie. Die processen moeten passen in het risicobeleid en leiden tot relevante informatie die besluitvorming binnen de organisatie voor allerlei onderwerpen en op allerlei niveaus ondersteunt.
- Proces
  De zijn de bekende stappen van identificatie, analyse, evaluatie en beheersing van risico's, met daarnaast aandacht voor consultatie & communicatie (rapportages) en monitoring & review. Die aanvullende elementen zorgen voor de aansluiting met het raamwerk.



Figuur 2: ISO 31000.

Sterke punten

Van ISO 31000 is het prettig dat het minder dan dertig pagina's telt en dat de hoofdstructuur zeer helder is. Daarnaast is het sterk dat principes expliciet worden gepositioneerd en dat er een aansluiting is met stap één uit het raamwerk; het verkrijgen van mandaat en draagvlak.

Door het gebruik van de juiste principes is de kans groter dat risicomanagement uit de puur financiële-/controlhoek wordt gehaald en iets van de individuele manager wordt.
De principes ('tegeltjeswijsheden') moeten zo concreet mogelijk gemaakt worden en aansluiten bij de organisatie. Daarnaast geeft het raamwerk de basis voor het verankeren van risicomanagement in de organisatie, op alle niveaus. Dit raamwerk vormt het beleidskader en daarmee het mandaat voor de aansturing van alle risicomanagementprocessen in de organisatie (zie figuur 3).

Figuur 3: Risicomanagement raamwerk.

Het raamwerk is ontwikkeld om risicomanagement te integreren in bestaande managementsystemen van organisaties en te vermijden dat er een systeem wordt ingevoerd dat los staat van de gewone bedrijfsvoering. Daarom is het als organisatie noodzakelijk om de onderdelen van het raamwerk aan te passen aan de bestaande procedures en richtlijnen. ISO is natuurlijk ook een bekende naam. Hoewel de 31000-norm een best practice-model is en niet voor certificatie is bedoeld, helpt dat wel. De aanpak van ISO 31000 sluit goed aan bij de door veel organisaties toegepaste ISO-normen voor kwaliteits- en milieumanagement.

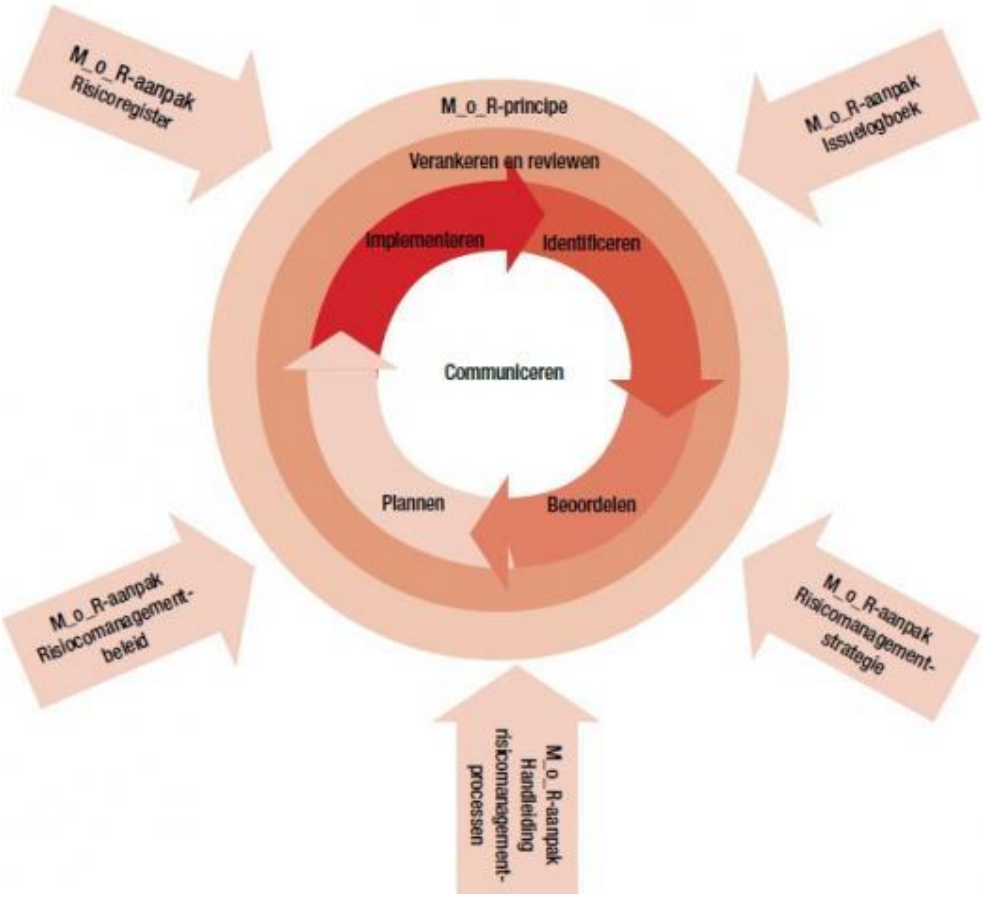
Bijlage 3. M_o_R® (2007)

M_o_R is ontstaan als reactie op het Turnbull report (1998) – de Engelse tegenhanger van de commissie Peters en Tabaksblat –, waarbij risicomanagement vanaf het begin zeer sterk aan behoorlijk bestuur werd gekoppeld. Het is ontwikkeld door dezelfde organisatie als PRINCE2®: de Office of Government Commerce (OGC). De richtlijn is begin 2010 in het Nederlands op de markt gekomen. Het stelde organisaties in staat te voldoen aan op dat moment geldende regelgeving en gaf aan welke essentiële zaken ontwikkeld moeten worden om risicomanagement als bedrijfsproces in te kunnen bedden in de organisatie en de bedrijfsprocessen. Het is bewust niet verplichtend, maar een brancheonafhankelijk best practice-model. Het betrekt alle medewerkers in een organisatie, vervangt niet, maar voorziet in een structuur, kaders en een communicatieomgeving.

Werking van M_o_R

Het doel van risicomanagement volgens M_o_R is het ondersteunen van besluitvorming door een goed zicht op de risico's en hun waarschijnlijke impact. Het model onderscheidt vier kernconcepten (zie ook figuur 4 op de volgende bladzijde):

- Principes
  De principes zijn essentieel voor een ontwikkeling van volwassen risicomanagement. Zij zijn afgeleid van corporate governance principes met de erkenning dat risicomanagement onderdeel is van de interne controle van organisaties.
- Aanpak
  Elke organisatie dient de principes aan te passen en accepteren. Deze afspraken worden vervolgens vastgelegd in beleid, een proceshandleiding en strategiedocumenten en worden ondersteund door risicoregisters en incidentenregistratie.
- Proces
  Het risicomanagementproces onderscheidt vier hoofdstappen om risico's te identificeren, beoordelen en beheersen.
- Verankeren en reviewen
  Als aan bovenstaande onderdelen is voldaan dient de organisatie ervoor te zorgen dat iedereen zich houdt aan de afspraken en dat verbeteringen worden doorgevoerd op alle niveaus.



Figuur 4: Het raamwerk van M_o_R.

Sterke punten

M_o_R omschrijft zeer uitgebreid en met handige checklists alle stappen rondom risicomanagement, inclusief de mogelijke belemmeringen. Zo wordt onder meer ingegaan op het volwassenheidsmodel risicomanagement, of de selectie van risicomanagementsoftware. Het model is in combinatie met de ISO-norm goed bruikbaar.

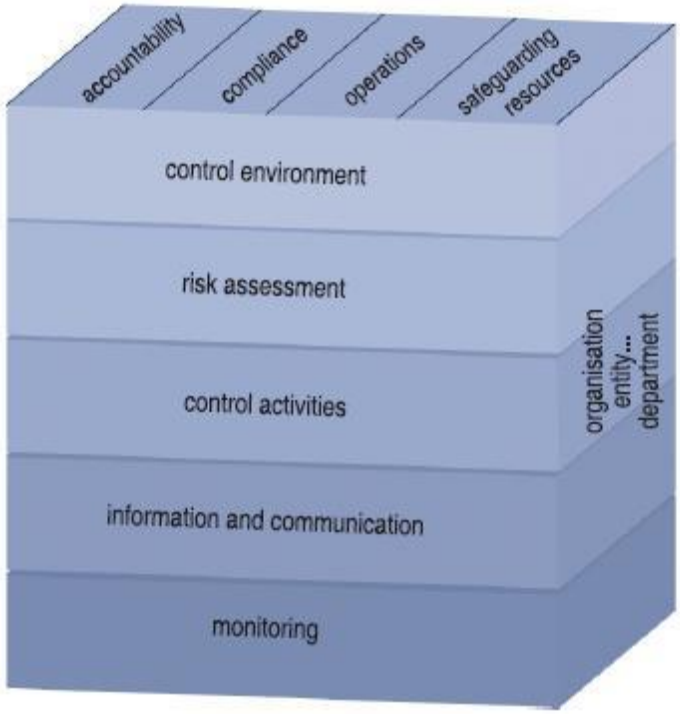
Het M_o_R-model maakt helder welke informatie nodig is om risicomanagement door te voeren. De bijbehorende documenten beschrijven op begrijpelijke wijze hoe de invoer van risicomanagement moet worden aangepakt – en in de loop der tijd geïntegreerd kan worden in de organisatiecultuur.

De activiteiten die ondernomen worden, de volgorde waarin ze worden ondernomen en de rollen en verantwoordelijkheden die nodig zijn voor deze uitvoering worden beschreven:

- Risicomanagementbeleid: communiceert hoe risicomanagement door een hele organisatie heen (of in een deel van een organisatie) wordt geïmplementeerd om het realiseren van haar strategische doelstellingen te ondersteunen.
- Handleiding risicomanagementprocessen: beschrijft de reeks stappen (van Context tot en met Implementeren) en hun respectievelijke verbonden activiteiten, die noodzakelijk zijn voor de uitvoering van risicomanagement.
- Risicomanagementstrategie: beschrijft de risicomanagementactiviteiten die voor een bepaalde organisatieactiviteit worden ondernomen.
- Risicoregister: legt vast en onderhoudt informatie over alle geïdentificeerde bedreigingen en kansen die gerelateerd zijn aan een specifieke organisatieactiviteit.
- Issuelogboek: legt informatie vast over alle geïdentificeerde issues die al hebben plaatsgevonden en actie vereisen, op een consistente en gestructureerde manier, en onderhoudt deze. Tot deze issues kunnen risico's behoren die werkelijkheid zijn geworden en zijn veranderd van mogelijke gebeurtenissen in werkelijke gebeurtenissen.

Bijlage 4. INTOSAI

In 2004 heeft de INTOSAI (International Organization of Supreme Audit Institutions), de wereldwijde koepelorganisatie van nationale rekenkamers, de Guidelines for Internal Control Standards for the Public Sector gepubliceerd. Dit model is gebaseerd op de principes van COSO, maar aangepast voor de publieke sector. In onderstaande figuur is het model weergegeven:



Figuur 5: INTOSAI.

De elementen in de kubus hebben een directe relatie. Er zijn vier doelstellingen te onderkennen, namelijk:

- Verantwoordelijkheid;
- Naleving van wet- en regelgeving;
- Operationeel (degelijk, ethisch, economisch, efficiënt en effectief);
- Bewaking van activa.

Elke onderdeel van de interne beheersing (beheersomgeving, risicobeoordeling, beheersactiviteiten, informatie & communicatie en monitoring) is van toepassing voor de te behalen doelstellingen.

In vergelijking met COSO besteedt INTOSAI meer aandacht aan:

- ethisch gedrag;
- het voorkomen en opsporen van fraude en corruptie in overheidsinstellingen;
- het vrijwaren van middelen in de overheidssector;
- de controle op het gebruik van informatiesystemen.

Belangrijkste afwijking van COSO is dat in dit model het aspect ethiek is toegevoegd. Dit is met name ingegeven doordat in de publieke sector integriteit een belangrijke rol speelt en het ontdekken en voorkomen van fraude in de publieke sector vanaf de jaren 90 steeds meer benadrukt is.
De verwachtingen van het maatschappelijk verkeer zijn voor de publieke sector vaak anders dan voor de private sector.

Van de publieke sector verwacht het maatschappelijk verkeer dat deze organisatie het algemeen belang behartigt. Daarnaast zijn deze organisaties grotendeels gefinancierd met publieke middelen, waarvan verwacht mag worden dat ze op een doeltreffende en doelmatige manier worden ingezet voor het algemeen belang.

Het doel van INTOSAI is om met dit model een richtlijn te geven voor het opzetten en uitvoeren van een goed interne beheersingssysteem binnen publieke organisaties. INTOSAI geeft aan dit model in samenhang met de volgende specifieke kenmerken van de publieke sector te bezien:

- De focus van publieke organisaties om politieke en sociale doelstellingen te behalen.
- Het gebruik van publieke gelden.
- De voorname rol van de budgetcyclus.
- De complexiteit van de instelling (dit vraagt om het vinden van een balans tussen de traditionele waarde als wettigheid, integriteit en transparantie aan de ene kant en effectiviteit en efficiency aan de andere kant).
- Brede maatschappelijke verantwoordelijkheid.