

# BETERE INTERNE BEHEERSING DANKZIJ INTEGRAAL RISICOMODEL

**De invoering van een geïntegreerd risicomodel leidde tot versterking van de interne beheersing bij Kempen & Co. Een risicomodel waarin risk, compliance en proces integraal worden benaderd, zorgde voor een organisatiebreed gedragen resultaat én kortere doorlooptijden.**

**tekst:** Jeanette Homan, directeur PSO Management

Op het gebied van risicomanagement zijn drie hoofdtrends te onderscheiden:

1. Nederlandse bedrijven hebben hun risicomanagement onvoldoende, inefficiënt en te oppervlakkig georganiseerd. Dit blijkt uit een gezamenlijk onderzoek onder een groot aantal bedrijven uitgevoerd door de Rijksuniversiteit Groningen, Nyenrode Business Universiteit, het Koninklijk Nederlands Instituut van Registeraccountants (Nivra) en PricewaterhouseCoopers.
2. Veel financiële instellingen hebben problemen met de navolging van externe wet- en regelgeving. Naast het inbedden van compliance regelgeving in algemene zin, hebben zij moeite om tegelijkertijd te voldoen aan diverse andere vereisten zoals die gelden voor specifiekere onderdelen als corporate governance/Code Tabaksblat, Basel II, Sarbanes Oxley wetgeving (SOx), Solvency II en SAS 70.
3. Marktonwikkelingen, vernieuwing van producten/diensten en interne strategische organisatie

ontwikkelingen, vragen om procesveranderingen. Daarnaast worden er vanuit de ICT steeds snellere en completere systemen ontwikkeld om deze processen te ondersteunen.

Deze drie hoofdtrends stellen verdergaande eisen aan de interne beheersing van bedrijven. Externe toezicht-houders worden daarnaast veeleisender. De afgelopen periode heeft een aantal incidenten plaatsgevonden, waardoor de regelgevende overheid scherpere criteria is gaan opstellen. En de verwachting is dat het daar niet bij blijft. De vraag is hoe financiële instellingen zich kunnen verzekeren van een goed systeem van risicobeheersing binnen hun organisaties, terwijl ondertussen ook de effectiviteit en efficiency van processen verbetert.

PSO Management ontwikkelde hiervoor een integrale methode. Deze methodiek kenmerkt zich door het integrale karakter waarmee de deelgebieden risico-beheersing, compliance en processen worden benaderd. Aan de hand van de implementatie bij zakenbank Kempen & Co wordt deze benadering toegelicht.

### Duidelijk risk framework

Het integrale model bestaat uit twee elementen. In de eerste plaats wordt gezorgd voor versterking van de interne beheersing van de risico's en compliance issues. Dit betekent dat risico's en compliance issues geïdentificeerd en vastgelegd moeten worden. Vervolgens moeten de aangebrachte controls, ter mitigatie van die risico's, beschreven worden.

In de tweede plaats wordt gekeken naar de risico's en compliance issues die besloten liggen de in de dagelijkse primaire en ondersteunde processen van organisaties, procedures en werkinstructies. Dit betekent dat ook de belangrijkste processen, procedures en meest risicovolle werkinstructies worden vastgelegd. Deze vastlegging kan overigens in de meeste processtools worden gemodelleerd.

De doelstelling van een integrale benadering, zoals het project bij Kempen & Co, is het opstellen van een duidelijk risk framework, waarbij tegelijkertijd risico's, wet- en regelgeving gekoppeld worden aan geactualiseerde processen.

Een belangrijk voordeel van de integrale aanpak is dat de doorlooptijd van het totale project aanzienlijk korter is en daarmee goedkoper, terwijl ondertussen de kwaliteit van de output hoger is aangezien er een geïntegreerde oplossing wordt gepresenteerd. Een ander belangrijk voordeel is de rol van de business. Deze speelt een actieve rol en biedt tegenwicht aan de input van de afdelingen Risk, Compliance en Audit waarmee het eindresultaat een gedragen resultaat is van deze afdelingen. Bij Kempen & Co wordt het totale proces organisatiebreed gedragen. Dit is zeer belangrijk, het versterken van interne beheersing

begint immers bij de top maar moet een breed draagvlak krijgen zodat er daadwerkelijk een mitigatie van operationele risico's kan optreden.

## *'Mitigatie van operationele risico's door versterking interne beheersing moet organisatiebreed worden gedragen'*

Henri-Jan Staal, directeur Riskmanagement  
Kempen & Co

### Waarom een integrale benaderingswijze?

De traditionele modellen die tot op heden gebruikt werden richten zich over het algemeen alleen op (operational) risk. Met het inzetten van het integrale risicomodel wordt getracht de beperkingen van de huidige traditionele modellen op te heffen.

1. Er is sprake van een koppeling met compliance. In de traditionele modellen was deze koppeling niet aanwezig. Dit had tot gevolg dat bij veranderende wet- en regelgeving de inrichting van de riskstructuur niet meer afdoende was. In veel gevallen werd dit echter niet als zodanig geconstateerd, laat staan aangepast of verwerkt in de riskstructuur. Binnen het integrale model leidt iedere aanpassing van wet- en regelgeving automatisch en direct tot een aanpassing van het riskkader. Er is een continue interactie waardoor een dynamisch in plaats van een statisch en passief risk kader ontstaat.

2. Er is sprake van een integrale koppeling tussen risk, compliance én processen. In de traditionele modellen was ook deze koppeling niet aanwezig. Waar risk evenals compliance autonoom werd benaderd, was de koppeling van beide velden met de werkprocessen zoals die gehanteerd werden, niet gestructureerd ingericht. Met toepassing van het integrale model worden niet alleen risk en compliance gekoppeld, maar worden ook automatisch de werkprocessen geactualiseerd.

3. Er is sprake van een gedragen risicomodel in plaats van een opgelegde werkwijze. Onder toepassing van het geïntegreerde model zal de samenwerking met de medewerkers in commerciële en ondersteunende functies (hierna: de business) anders worden. Zij zullen nu éénmaal worden benaderd voor informatievragen, terwijl het voorheen gebruikelijk was dat risk, compliance, audit en de afdeling administratieve organisatie keer op keer bij dezelfde personen aanklopten om de processen te beschrijven.

In het integrale model is de inzet van zowel de afdelingen risk en compliance als de business zelf

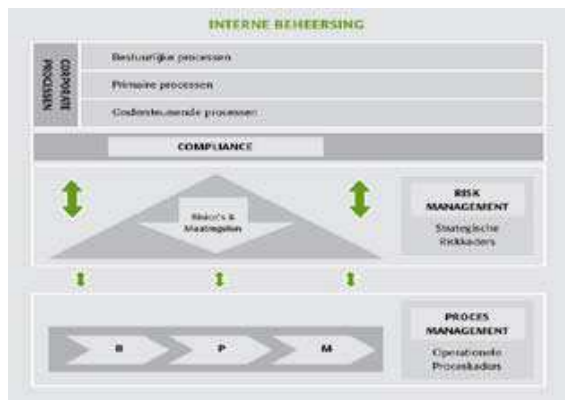
gewenst. Gezamenlijk worden de kaders bekeken, aangepast, bepaald en wordt een manier uitgewerkt om de risico's te evalueren (toetsmethodiek), een en ander in samenwerking met audit. De uitkomst, een nieuw risicomodel, is door beide 'partijen' ontwikkeld en wordt daarmee beter gedragen dan de modellen/werkwijzen uit het verleden die min of meer werden opgelegd.

### *'Door de centrale rol van de business is er meer betrokkenheid en enthousiasme'*

Marlies Dorenbosch-Kolle, medewerker projectdesk Kempen Capital Management

Het managen van risico's maakt deel uit van het beheersen van de organisatie. Als zodanig behoort dit tot de dagelijkse werkzaamheden van managers. Zij kennen immers de risico's binnen de organisatie en kunnen daar invloed op uitoefenen. Door de centrale rol van de business is er meer betrokkenheid en enthousiasme. Dat is ook nodig omdat het een zeer intensief traject is dat niet onderschat moet worden.

4. Er is sprake van een uniforme basis voor procesinrichting in plaats van verschillende afwijkende inrichtingen. Voorheen werd voor iedere nieuwe wet- of regelgeving een apart handboek opgesteld waarin de (nieuwe) processtructuur en aanpassingen van bestaande processen was uitgeschreven. In het integrale model wordt gewerkt vanuit een uniforme basis voor procesinrichting. Aan iedere wet of regel die wordt uitgevaardigd kan vanuit die uniforme basis worden voldaan. Vanuit de basis procesketen met daarin de onderverdeling van bestuurlijke, primaire en ondersteunende processen,



Figuur 1. Integrated Risk, Compliance & Process model. © PSO Management

worden risico's benoemd en verbonden met compliance issues. Niet alleen bij wetwijzigingen, maar ook bij Risk Self Assessments (RSA's), SAS70 certificeringen, 'In control statements' en systeem-en/of organisatiewijzigingen kan gebruik worden gemaakt van een en dezelfde basis procesinrichting. De basis procesinrichting krijgt hierbij een 'multi user' karakter. Dit leidt tot meer rust in de procesorganisatie en meer snelheid in het verwerken van de effecten van wet en regelgeving. Hierbij blijven de risico's bij iedere aanpassing aangesloten.

### Continue verandering van risico's

Het mag duidelijk zijn dat eenzijdige benaderingsmodellen op het gebied van risicomangement en compliance niet meer voldoen aan de huidige omstandigheden. In het risicobeheersingsproces blijft de basis hetzelfde: het bepalen en inschatten van risico's, het treffen van passende maatregelen en het monitoren van de effectiviteit van de maatregelen. Daarnaast moeten controles benoemd worden om zeker te zijn dat de risico's in voldoende mate worden beperkt zoals vooraf is bedacht ten aanzien van de effectiviteit van de maatregelen.

Veranderende diensten/producten brengen andere risico's met zich mee. Processen wijzigen. Ook de wijziging van wet- en regelgeving noopt tot aanpassing van processen. Daarnaast hebben bedrijven te maken met 'reguliere' veranderingen in de processen door nieuwe diensten/producten en/of systeemwijzigingen. Het gevolg hiervan is risico's continu veranderen. Integratie van risk, compliance en processen is in deze tijd van cruciaal belang om de gevolgen van de continue veranderingen op een goede wijze te beheersen.

Het managen van risicomangement, compliance en procesinrichting is een doorlopend proces. De enige manier om de business in control te krijgen en te houden is om op alle fronten onderdelen met elkaar te laten integreren. Dit vergt een duidelijke structurering van strategische en operationele kaders. En met de toenemende dynamiek op markten is een integraal én transparant riskmodel van groot belang. Met het toepassen van de integrale methodiek komt dit model in zicht. Deze integrale aanpak is erop gericht om – naast het verhogen van het risicobewustzijn – juist de risico's effectief te kunnen managen en de risico's van de business units transparanter te maken. Vanuit procesbeheer zijn er vervolgens meerdere opties mogelijk waar bedrijven hun voordeel mee kunnen doen.

### Hoe werkt dit in de praktijk?

Kempen & Co zag zich ook met de vraag geconfronteerd hoe de interne beheersing te versterken. Na een brede afweging koos de bank voor de integrale methode van PSO Management.

In het project bij Kempen & Co is gekozen voor een



Van links naar rechts: Marlies Dorenbosch-Kolle, Henri-Jan Staal, Rob Schouten, Jeannette Homan en Jon Lindeboom.

duidelijke projectfasering door een analyse per business unit uit te voeren.

#### *Fase 1. Scan*

In de eerste fase zijn interviews gehouden met proces-eigenaren. Doel is te bepalen of risico's geïdentificeerd en beschreven worden en of processen zijn vastgelegd. Dit betreft zowel primaire, ondersteunende als ook corporate processen. Daarnaast zijn interviews gehouden met de afdelingen Risk management, Compliance en Audit. Met hen is afgestemd in hoeverre zij in staat zijn de beschikbare risicoanalyses en procesbeschrijvingen te monitoren. Met deze uitkomsten werd al snel duidelijk waar aandachtspunten lagen en welke prioritering gehanteerd moest worden. Vanuit de bovenstaande analysefase is met een duidelijk afgebakende probleemstelling en met duidelijke aandachtspunten en prioritering het project gestart.

#### *Fase 2. Analyse*

Bij het in kaart brengen van de bestaande risico- en procesmanagementkaders en procedurebeschrijvingen, is maximaal gebruik gemaakt van de reeds binnen de organisatie aanwezige informatie. In veel gevallen is deze informatie over risico's, procedures en beheersingsmaat-

regelen aanwezig en zeer goed bruikbaar. Er hoefden geen aparte inventarisatie- en analysewerkzaamheden opgestart te worden, wat leidde tot een aanmerkelijke versnelling van het project.

#### *Risk (self assessment) template*

Door Risk management is in samenwerking met vertegenwoordigers vanuit de hele organisatie een eerste risk (self assessment) template gemaakt aan de hand van de geïnventariseerde processen.

#### *Compliance template*

Vanuit wet- en regelgeving zijn alle bestaande procedures geïnventariseerd en gekoppeld aan 'clusters van wetgeving' in de Wet op het financieel toezicht (intern bij Kempen 'buckets' van wetgeving genoemd). Door deze koppeling worden bestaande procedures gestructureerd en is het makkelijker om compliance issues en procedures op een juiste wijze te vertalen naar processen. Vanwege de gemaakte koppeling tussen procedures en de wet- en regelgeving is het voor Kempen eenvoudig geworden om wijzigingen in de wetgeving te vertalen naar wijzigingen in processen. De vertaling en de implementatie richting de business kan zodoende beter voorbereid en uitgevoerd

worden. Interpretatie, implementatie en toetsing van compliance issues is hiermee vereenvoudigd.

#### *Fase 3. Toetsing*

De uitkomst van fase 2 is een geïntegreerde template waarin alle risico's en werkelijke aanwezige beheersmaatregelen staan vermeld. Deze template is besproken met de vertegenwoordigers van de business. De resultaten van

### ***‘De interpretatie, implementatie en toetsing van compliance issues is vereenvoudigd’***

Jon Lindeboom, directeur  
Juridische Zaken en Compliance Kempen & Co

deze gesprekken zijn gebruikt om de procesbeschrijvingen te actualiseren. Deze worden ondergebracht in een process template. Vervolgens is de template besproken met de afdelingen Risk management, Compliance en Audit en door hen getoetst op volledigheid en juistheid. Uiteindelijk heeft de CFO de template als geheel beoordeeld.

#### *Fase 4. Risk self assessment*

Na de toetsing in fase 3 is een risk self assessment (RSA) ingepland waarin mensen van de business zelf aan de door hen aangegeven risico's een kans en een impactwaarde verbinden. De deelnemende mensen uit de business zijn proceseigenaren afkomstig uit verschillende disciplines.

Daarnaast is er aan de RSA deelgenomen door vertegenwoordigers van Risk management, Compliance en Audit. De deelnemers hebben – op grond van hun individuele inbreng – per punt in de risicoanalyse gezamenlijk afgestemd wat de kans op de gebeurtenis is en wat de daaraan gekoppelde impact is.

Een positief bijeffect van de gezamenlijke participatie in de RSA is geweest, dat er issues boven tafel komen die voorheen niet nadrukkelijk benoemd waren geweest en die meteen gezamenlijk geanalyseerd en opgelost kunnen worden. Dit is het direct gevolg van de multidisciplinaire participatie van verantwoordelijken uit de business, Risk & Compliance officers en Audit.

#### *Fase 5. Implementatie*

De laatste stap betreft de implementatie van de template. De in de kaart gebrachte risico's en compliance issues worden gekoppeld aan de in fase 3 geactualiseerde processen. Door deze koppeling zijn risico's en maatregelen vertaald naar de dagelijkse operatie. Voorts zijn de geactualiseerde procesbeschrijvingen inclusief aangescherpte beheersingsmaatregelen om de risico's te beperken geüpload vanuit de templates naar een procesmodelleringstool.

#### *Fase 6. Audit & beheer*

In de samenwerking met business, Risk management, Compliance en Audit vervulde Audit een proactieve rol, waarbij zij gedurende het gehele traject aanbevelingen gaf. Zij toetste hierbij vooral de gehele uitgevoerde risicoanalyses, inclusief de compliance risico's. Door de multidisciplinaire participatie is er vooraf discussie ontstaan tussen Compliance en Risk management waardoor er een veel beter gezamenlijk beeld van de issues ontstaan is. Vervolgens is men in staat om proactief maatregelen te treffen, waar voorheen reactief moest worden opgetreden omdat de gezamenlijke relevante issues niet bekend waren.

Vanuit Audit is het ook belangrijk geweest om een borging te kunnen garanderen van de risk en compliance issues door het inzetten van een incidentenmethodiek (action-tracking), die momenteel gebruikt wordt door business, risk, compliance en audit. Bij Kempen ligt de beheerfunctionaliteit van risico's, compliance en processen bij Operational Risk in combinatie met de business en Compliance.

#### **Naast transparantie ook meer efficiency**

Kempen & Co is er in geslaagd de bedrijfsvoering nog transparanter en efficiënter te maken. Door de goede samenwerking van de business en Risk management, Compliance en Audit heeft de bank een goede inbedding van processen in de organisatie kunnen realiseren. Het brede palet van risico's, compliance issues en processen is gekoppeld en daarmee integraal en dynamisch onder controle. Mutaties op het gebied van risico's, maatregelen en wet- en regelgeving zijn daardoor eenvoudig te operationaliseren en – nog belangrijker – te mitigeren.

### ***‘Door een integrale toepassing meer discussie vooraf, waardoor je vanuit Audit meer proactief kan handelen’***

Rob Schouten, directeur Audit Kempen & Co

Op deze wijze is de business verzekerd van goed beheerste risico's binnen de organisatie onderdelen en zijn tevens de processen zodanig ingericht dat zij voldoen aan actuele wetgeving. Ondertussen kan ook de effectiviteit en efficiency van processen verbeterd worden hetgeen van primair belang is voor de organisatie. Daarmee kan de kwaliteit van de interne beheersing ook in de toekomst goed geborgd blijven, ook in geval van nieuwe systeemimplementaties of nieuwe productdifferentiaties.

De Kempen organisatie is klaar voor de toekomst, zowel aan de voorzijde maar zeker en vooral ook aan de achterzijde. «