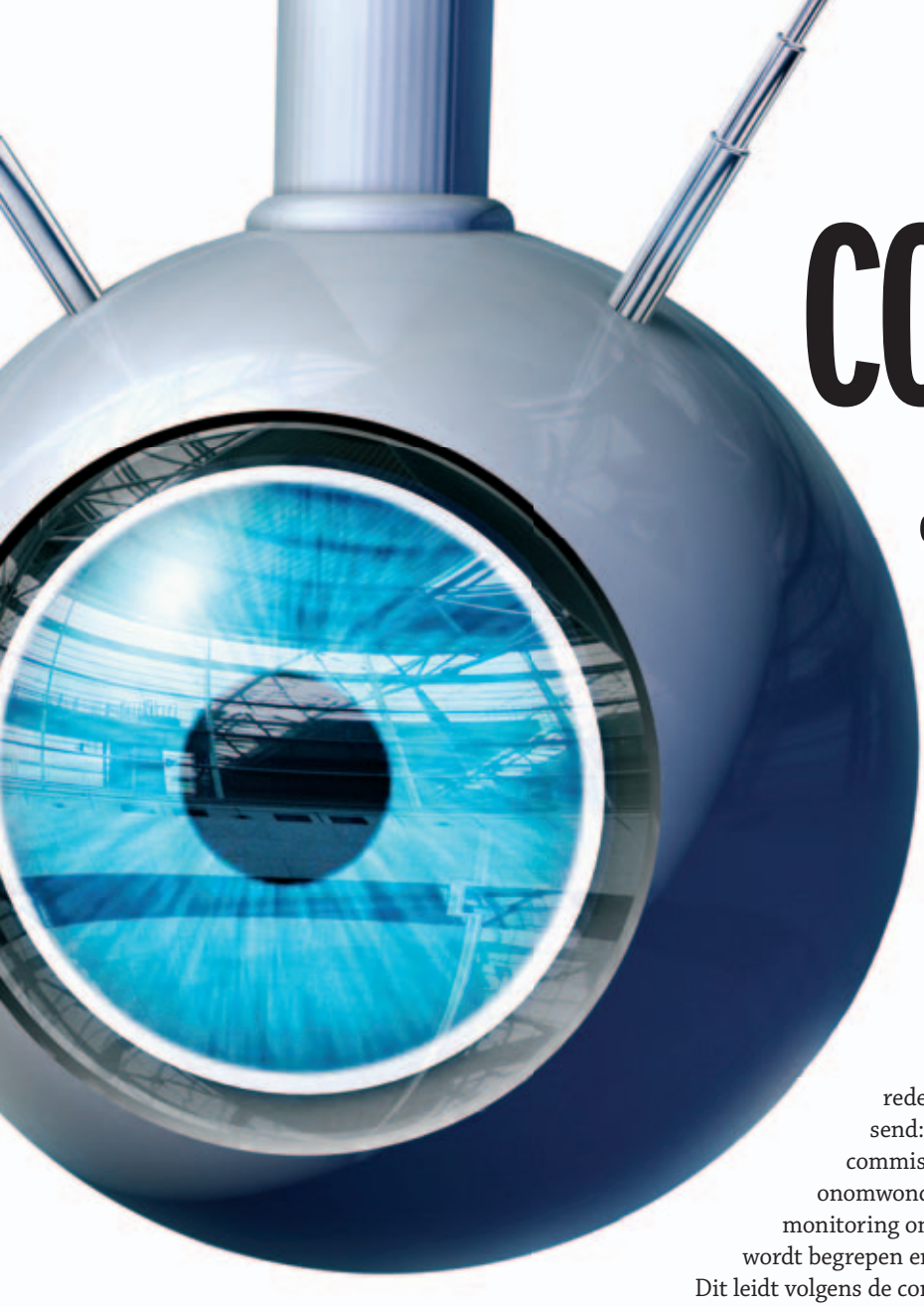

COSO over mo

Op 4 juni 2008 publiceerde het Committee of Sponsoring Organizations nieuwe conceptrichtlijnen over de monitoring-component van het COSO-raamwerk voor interne beheersing. De hoofdlijnen.

TEKST **CEES KLUMPER*** | BEELD **CORBIS**

Monitoring ziet er kort gezegd op toe dat de interne beheersing binnen een organisatie effectief is en blijft: het stelt vast of de interne beheersingsmaatregelen werken zoals ze zijn bedoeld, en worden aangepast zodra daar aanleiding toe is. Waar *controls* ten doel hebben om **tekortkomingen in processen** te voorkomen of op te sporen hebben monitoring-activiteiten ten doel om **hiaten in de werking van controls** te voorkomen of te detecteren. Een wezenlijk andere doelstelling dus.

LAGERE KOSTEN

Monitoring is al goed beschreven in het oorspronkelijke COSO-raamwerk uit 1992. Toch is dit de eerste keer dat COSO specifieke *guidance* geeft voor één van de vijf interne beheersingscomponenten. De reden is verrassend: de commissie stelt onomwonden vast dat monitoring onvoldoende wordt begrepen en toegepast.

Dit leidt volgens de commissie in de praktijk tot vaak overbodige en weinig effectieve interne beheersingsmaatregelen.

COSO verwacht dan ook dat juiste toepassing van monitoring een grote bijdrage kan leveren aan het zowel beter beheersen van risico's als het verlagen van de kosten voor het *in control* zijn van organisaties. Hogere kwaliteit van interne beheersing tegen lagere kosten dus.

> 'Coso stelt onomwonden vast dat monitoring onvoldoende wordt begrepen en toegepast.'

NEDERLAND

Deze conclusie werd in april 2007 ook al getrokken in het artikel *Embedded testing is efficiënt en effectief: Het middel tegen SOx-blues* in 'de Accountant'. Daarin werd beschreven hoe de werking van interne beheersingsmaatregelen kon worden vastgesteld op een veel effectievere en efficiëntere manier dan door nagenoeg alle *SOx-compliant*-bedrijven werd (en nog steeds wordt) gedaan. De Amerikaanse Securities and Exchange Commission en Public Company Accounting Oversight Board bevelen deze testaanpak inmiddels aan.

In het in december 2007 gepubliceerde rapport van de Nederlandse Monitoring Commissie Corporate Governance Code wordt, ten aanzien van interne beheersing uitsluitend naar één van de twee huidige COSO-modellen ('basis-COSO' of het ERM-model) verwezen. COSO speelt dus ook in Nederland een belangrijke rol bij interne beheersing.

ZES PUNTEN

De belangrijkste punten in de conceptrichtlijnen zijn de volgende:

nitoring

- Effectieve monitoring begint bij een goede *tone from the top*, een adequate organisatorische inrichting en een goede initiële nulmeting (*baseline*) van de werking van de belangrijkste beheersmaatregelen.
- Zoals interne beheersmaatregelen het antwoord zijn op risico's in processen, moet monitoring het antwoord zijn op het risico dat beheersmaatregelen niet effectief zijn. Daarom is een gedegen risico-inschatting noodzakelijk om de juiste monitoring-activiteiten te kunnen definiëren: wie voert de monitoring uit (deskundigheid en onafhankelijkheid), wat houdt de monitoring precies in en wat is de juiste frequentie. De conceptrichtlijnen besteden relatief veel aandacht aan de vraag welke informatie hierbij van belang is.
- Objectiviteit is niet zwart-wit: iemand kan aangaande de uitvoering van een bepaalde beheersmaatregel niet tot volledig (zoals internal auditors of operational risk managers) objectief zijn en alles daartussenin. Waar het om gaat is dat de persoon die belast is met een bepaalde monitoring-activiteit *voldoende* objectief is.
- Aangezien interne en externe risico's veranderen in de tijd, moet de organisatie op gestructureerde wijze tijdig inspelen op deze veranderingen door aanpassing van beheersmaatregelen en de bijbehorende monitoring-activiteiten.
- Monitoring bestaat uit twee verschillende onderdelen: continue (*ongoing*) monitoring, die in de reguliere procedures en processen is ingebed, en monitoring als een *add-on* bovenop het dagelijkse proces (*separate evaluations*). Feitelijk zijn dit communicerende vaten: hoe beter de continue monitoring, des te minder de noodzaak voor - relatief kostbare - add-on-activiteiten.

COSO concludeert dat continue monitoring meestal beter (effectiever en efficiënter) kan worden ingericht dan add-on, dat mede daarom tot een minimum moet worden beperkt.

- De resultaten van de gecombineerde monitoring moeten aan de juiste personen worden gecommuniceerd: doorgaans de functionaris die verantwoordelijk is voor het adequaat functioneren van de desbetreffende beheersmaatregelen én degene ten minste één niveau hoger.

AANBEVELINGEN

Monitoring is een wezenlijke component van ieder systeem van interne beheersing maar is, zoals de commissie concludeert, tot nu toe in verreweg de meeste organisaties onderbelicht gebleven. Dat is zonde, want er is veel winst te behalen. Concreet zouden organisaties het volgende moeten doen:

> 'Voor wie de principes echt toepast is er veel winst te behalen.'

- Lees om te beginnen de Executive Summary van de exposure draft door; deze beslaat nog geen twintig pagina's en bevat een schat aan informatie.
- Ga na of de binnen de processen altijd aanwezige monitoring-activiteiten separaat zijn onderkend. Dit is bijna nooit het geval. Zelfs organisaties die voldoen aan Sarbanes-Oxley 404 , en daarvoor hun interne beheersmaatregelen rond de externe financiële verslaggeving tot in detail documenteren, behandelen zelden of nooit de monitoring-component zoals COSO dit omschrijft. Laat staan voor andere doeleinden, waarvoor nauwelijks richtlijnen bestaan.

COSO-document

Het in dit artikel beschreven document bestaat uit drie delen: een management samenvatting, de gedetailleerde richtlijnen zelf en een verzameling van 43 concrete voorbeelden. Het telt circa 190 pagina's. Commentaar op het concept kon tot 15 augustus 2008 worden ingediend.
Het artikel is te downloaden via www.coso.org.

- Beoordeel of de door COSO omschreven nulmeting is (of kan worden) gemaakt op basis van de beschikbare informatie. Bestaat er een mechanisme om veranderingen in de risico's adequaat te vertalen naar aanpassingen in beheersmaatregelen en monitoring-activiteiten? Worden geïdentificeerde tekortkomingen in interne beheersmaatregelen adequaat gecommuniceerd binnen de organisatie? Het antwoord op deze vragen zal in de meeste gevallen hoogstwaarschijnlijk 'nee' zijn.
- Selecteer bij wijze van een pilot een willekeurig proces of willekeurige afdeling, maak de daar aanwezige monitoring-activiteiten zichtbaar en evalueer ze op de door COSO onderscheiden criteria. Bepaal vervolgens of continue en add-on monitoring-activiteiten goed op elkaar zijn afgestemd - niet meer maar ook niet minder dan nodig op basis van de onderkende risico's.

Voor wie de principes zoals door COSO in deze exposure draft uiteengezet echt toepast is er veel winst te behalen. En ook inhoudelijk is het zeer stimulerend.

NOOT

* Cees Klumper is partner Management Assurance Services KPMG.