7

# “Why Update What Works…”

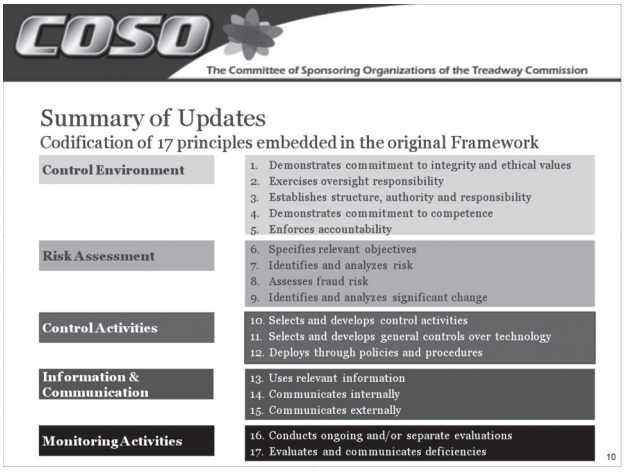
Philip Wallage

Op 19 december jongstleden heeft de COSO[1]-commissie een voorstel uitgebracht om het raamwerk voor het opzetten en evalueren van het systeem van interne beheersing (internal control) aan te passen.

Sinds de financiële debacles in het begin van de 21e eeuw heeft de toepassing van het raamwerk uit 1992 een grote vlucht genomen. Zo verwijzen Sarbanes-Oxley (Sectie 404) en de Nederlandse Corporate Governance Code hiernaar. Ook in de populaire en academische literatuur, inclusief de rubriek Bestuurlijke Informatieverzorging van dit maandblad, is veelvuldig aandacht besteed aan het COSO-raamwerk.

Voldoende reden om in deze column stil te staan bij de voorgestelde wijzigingen. Het meest opmerkelijke is dat door de commissie is besloten om de fundamentele concepten ongewijzigd te laten. Dit zijn de zogenaamde vijf componenten (risicomanagement, beheersingsprocedures, bewaking, beheersingsomgeving en informatie en communicatie) en de drie doelstellingen van interne beheersing (betrouwbaarheid van de financiële rapportages, naleving van wet en regelgeving en effectiviteit van de bedrijfsprocessen). Ook de definitie van interne beheersing en het uitgangspunt dat interne beheersing geen absolute zekerheid biedt dat er geen zaken fout kunnen gaan, blijven ongewijzigd.

Wel stelt COSO een aantal aanpassingen voor om de bruikbaarheid van het raamwerk te vergroten. Zo wordt ingespeeld op recente ontwikkelingen als globalisering, outsourcing en IT en wordt meer nadruk gelegd op belangrijke veranderingen in de bedrijfsomgeving en gerelateerde risico’s. Interessant is de brede focus op de interne beheersingsdoelstellingen operaties, compliance en (niet-) financiële rapportage. Pas medio 2012 volgt een addendum waarin nader wordt ingegaan op interne beheersing betreffende financiële rapportage. Ondanks dat de doelstellingen en componenten ongewijzigd zijn gebleven (gemotiveerd met *‘Why Update What Works’*), zijn de componenten uitgewerkt in de volgende (zeventien) principes:




Bron: COSO, IC – Integrated Framework, december 2011.

Overige aanpassingen van het raamwerk zijn onder andere:

- verdergaande betrokkenheid van toezichthouders (ter verbetering van de governance);
- verbreding van de toepassing (inclusief niet-financiële rapportage);
- verbetering van de kwaliteit van risk-assessment;
- versterking van anti-fraude inspanningen waarbij meer nadruk op ‘soft controls’ (zonder het begrip expliciet te introduceren);
- eenvoudig aanpasbaar zijn van het interne beheersingssysteem vanwege de snelheid van veranderingen en toegenomen complexiteit;
- grotere toepasbaarheid voor verschillende business models.

Ondanks de voorgestelde verbeteringen komt een fundamenteel vraagpunt op. Dit betreft het ontbreken van een antwoord op de vraag in hoeverre het COSO-raamwerk voor en tijdens de financiële crisis[2] effectief is gebleken. Zoals gezegd wordt COSO gebruikt bij het evalueren van de interne beheersing rondom financiële verslaggeving en vormt het raamwerk de basis voor het afgeven van het ‘in-control statement’ (SOX 404). Bij dit ‘in-control statement’ verstrekt de accountant een controleverklaring.

De ‘one million dollar question’ luidt vervolgens hoe het kan zijn dat besturen van (financiële) instellingen in 2007

ongeclausuleerd verklaren 'in control' te zijn, terwijl kort daaropvolgend de financiële crisis is ontstaan en instellingen failleren.[3] Als ter beantwoording van deze vragen geen 'root cause analysis' heeft plaatsgevonden, hoe kan de COSO-commissie tot de conclusie komen dat er geen wezenlijke aanpassingen nodig zijn?

Observaties van de werking van risicomanagement gedurende de financiële crisis van de 'Senior Supervisors Group' (SSG) uit maart 2008, wijzen wel degelijk op de noodzaak risicomanagement/interne beheersing diepgaand te evalueren.[4] De SSG concludeert onder meer dat effectieve, ondernemingsbrede risico-identificatie en analyse veelal niet hebben plaatsgevonden en dat de rapportages over risicomanagement en interne beheersing onvoldoende informatief zijn geweest en vervolgactie heeft ontbroken. Opmerkelijk is ook dat sommige financiële instellingen onvoldoende in staat zijn geweest om een aanvaardbaar niveau van risk appetite te bepalen, te meten en te beheersen. Desondanks hebben zij tot het laatste toe verklaard 'in-control' te zijn. Ook is de invloed van beloningspakketten die conflicteren met de interne beheersingsdoelstellingen van de onderneming onvoldoende onderkend. Even schokkend is de constatering dat effectieve identificatie en meting van risico's vaak is belemmerd door gefragmenteerde technologische infrastructuren. Als laatste bevinding van de SSG noem ik institutionele arrangementen die status verleenden aan (te) vergaande risk appetite van besluitvormers ten koste van de invloed van medewerkers van risk management, compliance en audit.[5] Jammer genoeg verschaft het SGG-rapport geen nader inzicht in de onderliggende oorzaken van de ontoereikende (opzet, werking en evaluatie van) interne beheersing.

Fundamenteel is dat menselijk handelen uiteindelijk bepaalt of risico's voldoende worden beheerst en is het systeem van interne beheersing even goed of slecht als haar gebruikers.[6] Een uitgangspunt dat in het raamwerk een centrale plaats zou moeten hebben.

Natuurlijk is de werkelijkheid complex en kunnen crises (per definitie) niet worden voorkomen, maar het is een gemiste kans dat COSO in het voorliggende voorstel niet zichtbaar ingaat op bovengenoemde aspecten. De conclusie dat geen fundamentele wijzigingen nodig zijn, komt hierdoor in een merkwaardig daglicht te staan. Het ontbreken van een goede analyse van oorzaken van de opzet en werking van interne beheersing tijdens de (huidige) financiële crisis, impliceert een 'jumping to conclusions'.[7]

Gegeven de grote autoriteit die het raamwerk wereldwijd heeft, is nader beraad over de aanname *'if it ain't broke, don't fix it'*, beslist nodig.

Prof. dr. Ph. Wallage is hoogleraar Accountantscontrole aan de Vrije Universiteit van Amsterdam en Universiteit van Amsterdam en is tevens als partner werkzaam bij KPMG.

## Noten

1 The Committee of the Sponsoring Organizations of the Treadway Commission. Het Framework voorstel, december 2011, is te downloaden van www.ic.coso.org. De commentaarperiode loopt tot 31 maart 2012.

2 Voor nadere oppositie tegen de voorgestelde (beperkte) wijzigingen zie bijvoorbeeld 'Framework Naysayers Call for Blank Sheet of Paper', Tammy Whitehouse, January 10, 2012, Compliance Week.

3 Voor zover mij bekend heeft de Securities and Exchange Commission zich nog niet publiekelijk geuit over de zorgen die bestaan als gevolg van de (ten tijde van de kredietcrisis) door de CEO/CFOs afgegeven 'in-control statements' waarbij het COSO-raamwerk is gehanteerd.

4 Senior Supervisors Group, Observations on Risk Management Practices during the Recent Market Turbulence, March 6, 2008. De SSG bestaat uit Engelse, Zwitserse, Duitse, Franse en Amerikaanse toezichthouders op de financiële markten onder leiding van William L. Rutledge (Federal Reserve Bank of New York).

5 Risk Management Lessons from the Global Banking Crisis of 2008, October 21, 2009, Senior Supervisors Group, www.sec.gov/news/press/2009/report102109.pdf

6 Zie ook Jules Muis, Disclaimer bij strategisch management, maandag 16 januari 2012, Weblogs, www.accountant.nl.

7 Zie ook Tim J. Leech, The High Cost of 'ERM Herd Mentality', Exposure Draft for Comments, www.riskoversight.ca.