COSO vernieuwt

Na twintig jaar heeft COSO met een nieuwe (concept)rapport een nieuwe stap gezet op de weg van beoordeling van de beheersing van organisaties. Een introductie op hoofdlijnen, plus suggesties ter aanscherping. Zo wordt bijvoorbeeld de invloed van IT op functiescheidingen niet besproken.

TEKST: **HENK DEN BOER, REMKO RENES** EN **LUC VAN ZUTPHEN*** | BEELD: **CORBIS**

In 1992 verscheen het zogenaamde COSO-rapport: Internal Control - Integrated Framework (ICIF). Dit rapport had als doelstellingen:

1. Het geven van een algemeen aanvaarde definitie en begrippenkader voor *internal control* in de ogen van verschillende belanghebbenden bij een organisatie.
2. Het management van huishoudingen helpen met het verbeteren van hun *internal control*-systeem.

Het begrip *internal control* werd onder meer gedefinieerd om een standaard te verschaffen waarmee ondernemingen en organisaties hun *internal control*-systeem kunnen beoordelen en waarmee ze kunnen vaststellen hoe het kan worden verbeterd.
In december 2011 publiceerde COSO een geheel nieuw ontwerprapport. Het ligt in de bedoeling om, na het ontvangen van commentaar, in het najaar van 2012 een definitief nieuw COSO-rapport uit te brengen.

ZEVENTIEN PRINCIPES

In het nieuwe rapport is de definitie van *internal control* onveranderd gebleven, evenals de vijf elementen van een internal control-systeem. Een belangrijke wijziging is de vertaling van internal control-concepten in zeventien principes en nadere kenmerken daarvan, die organisaties moeten helpen bij het beoordelen van risico's en de verbetering van prestaties.
Zo kent bijvoorbeeld het element Control Environment in het nieuwe (concept)rapport de volgende vijf principes:

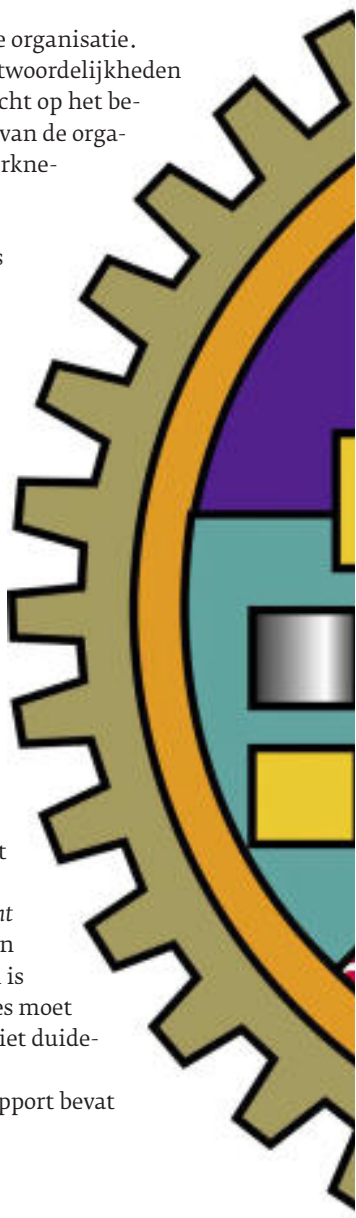
1. De organisatie toont commitment ten aanzien van integriteit en ethische waarden.
2. De board toont onafhankelijkheid ten aanzien van het management en oefent toezicht uit met betrekking tot de ontwikkeling en de werking van internal control.
3. Het management zorgt onder toezicht van de board voor een goede organisatiestructuur, wijze van rapportering en voldoende bevoegdheden en verantwoordelijkheden ten behoeve van het behalen van de doelstellingen.
4. De organisatie toont commitment om mensen te werven en zich blijvend te laten ontwikkelen in lijn met de doelstellingen van de organisatie.
5. De organisatie legt de verantwoordelijkheden voor de internal control gericht op het behalen van de doelstellingen van de organisatie bij de individuele werknemers.

'HET RAPPORT ZOU BETER KUNNEN AANGEVEN OP WELKE WIJZE ORGANISATIES SOFT CONTROLS KUNNEN GEBRUIKEN.'

Elk van de genoemde principes wordt in het desbetreffende hoofdstuk verder uitgewerkt. Voorop staat echter dat het principes zijn en geen lijstjes van punten die kunnen of moeten worden afgevinkt.

COSO EN ERM

Door het uitbrengen van een nieuw (concept) COSO-rapport ontstaat een bijzondere situatie ten aanzien van het in 2004 door de COSO-organisatie gepubliceerde rapport Enterprise Risk Management (ERM). Risk assessment is een van de vijf componenten van het COSO-Framework, maar in het COSO-ERM-rapport wordt gesteld dat *enterprise risk management* veel breder en uitgebreider is en dat *internal control* een onderdeel is van COSO-ERM. Hoe dat precies moet worden gezien, wordt echter niet duidelijk gemaakt.
Het nieuwe (concept) COSO-rapport bevat



een aparte bijlage (D) die aandacht besteedt aan de relatie tussen COSO-ERM en het nieuwe COSO-framework. Ook in die bijlage wordt weer gesteld dat ERM ruimer is dan internal control. COSO-ERM behandelt bijvoorbeeld strategische doelstellingen, terwijl deze buiten het oorspronkelijke COSO-framework vallen. Ja, zelfs expliciet buiten beschouwing worden gelaten. Wij zijn van mening dat het proces om tot de formulering en keuze van strategische doelstellingen te komen wel onderdeel is van het beheersingssysteem van de organisatie. De leiding van de organisatie dient naar onze mening wel te waarborgen dat het proces van strategievorming wordt beheerst. De strategie zelf is overigens geen onderdeel van het beheersingssysteem.
Risico's op de terreinen van operations, rapportering en compliance lijken normaal binnen de reeds bekende onderdelen van het COSO-framework te vallen. Het nieuwe concept-COSO-rapport zou ons inziens wel dieper op de feitelijke relatie tussen het COSO-framework

'WELKE AANDACHT BESTEEDT HET ONTWERPRAPPORT AAN TECHNOLOGISCHE VERANDERINGEN? HET ANTWOORD IS TELEURSTELLEND.'

en COSO-ERM in kunnen gaan om de stelling ten aanzien van COSO-ERM (breder en uitgebreider) meer te onderbouwen en daardoor te verduidelijken.

BEVEILIGING VAN ACTIVA

In 1994 verscheen een Addendum op het gedeelte 'Rapportering aan derden' in het COSO-rapport, en wel in het bijzonder gericht op het aspect 'beveiliging van activa'. Dit werd vooral ingegeven door kritiek van onder meer de Amerikaanse General Accounting Office (Rekenkamer).
Het aspect beveiliging van activa wordt ook internationaal in vele landen apart onderscheiden. In het nieuwe (concept) COSO-rapport komt het echter niet terug in de definitie.

Hoewel het addendum van 1994 was gericht op het onderdeel 'Rapportering aan derden', zou het ons inziens goed zijn geweest om dit aspect wel in het nieuwe rapport mee te nemen. Dit zou aansluiting geven bij een gegroeide internationale kijk op *internal control* en daarmee het nieuwe rapport versterken en breder geaccepteerd maken.

RELATIE MET CORPORATE GOVERNANCE

Sinds de publicatie van het Cadbury-rapport in het Verenigd Koninkrijk in 1992 (The Financial Aspects of Corporate Governance) heeft corporate governance wet- en regelgeving internationaal de aandacht versterkt voor internal control en in het bijzonder voor internal control-verklaringen (*zie kader 'COSO en Cadbury'*). Inmiddels is het COSO-framework de wereldstandaard voor de beoordeling van internal control en ligt het wereldwijd op tafel in menige bestuurskamer.

'DE INVLOED VAN IT OP FUNCTIESCHEIDINGEN WORDT NIET BESPROKEN.'

Het COSO-framework is oorspronkelijk in de Verenigde Staten ontwikkeld om een bijdrage te leveren aan fraudepreventie. Corporate governance omvat daarentegen meer het voorkomen van fraude en frauduleuze financiële verslaggeving. Corporate governance gaat over de rol, verantwoordelijkheid en verdeling van bevoegdheden aan de top van organisaties tussen uitvoerende en toezichthoudende bestuursleden, interne en externe accountants, audit committees en de relaties met externe (publieke) toezichthouders, aandeelhouders en overige belanghebbenden.
Naar onze mening zou de definitieve versie van het COSO-framework nog waardevoller worden wanneer duidelijk aandacht wordt gegeven aan de relatie tussen internal control en corporate governance. Met name gelet op het belang van de in het framework benadrukte *tone at the top*, die vooral de resultante is van bewust en onbewust optreden van de bij governance betrokken hoofdrolspelers.

SOFT CONTROLS

In een audit op basis van het COSO-framework wordt goede effectieve internal control vooral gebaseerd op formele en verifieerbare kenmerken. Het verzamelen van controlebewijs voor zowel management als accountants is gebaseerd op formeel achteraf verifieerbaar bewijs. Dit roept de vraag op welke waarde informele maatregelen en activiteiten hebben voor de effectiviteit van internal control. COSO geeft aan dat informele controls waardevol kunnen zijn voor een specifieke groep (kleinere) organisaties of als *mitigating control* wanneer formele controls tekortschieten.
Gelet op de toenemende aandacht voor soft controls in de laatste jaren, zou het rapport beter kunnen aangeven op welke wijze organisaties soft controls kunnen gebruiken bij de inrichting van hun internal control-systeem en de uitvoering van een internal control audit.

IT-ONTWIKKELINGEN

In het concept-COSO-rapport komen ook de ingrijpende veranderingen op IT-gebied in beeld. In 1992 was er nog geen massaal gebruik van e-mail, internet, smartphones, laptops, tablets, social media, cloud computing et cetera. Nieuwe businessmodellen ontstonden, vaak complex van aard en veelal gefaciliteerd door informatietechnologie om zelfs wereldwijd te kunnen opereren. Welke aandacht besteedt het ontwerprapport aan deze technologische veranderingen? Het antwoord is in structurele en instrumentele zin teleurstellend.
De gekozen opzet - *principles based* aangevuld met *attributes* en *examples* - is ook gevolgd voor de effecten van IT op het control framework. Bij alle control-componenten wordt *technology* als belangrijk aspect gezien. Richtlijnen voor een gestructureerde en praktische uitwerking van IT-governance en control ontbreken echter. Hiervoor is bewust gekozen. Wellicht zal een herziene vijfde editie van COBIT, die later in 2012 zal verschijnen, hierin voorzien.
Met de gekozen benadering hoopt COSO een nieuwe editie van het framework te presenteren die niet al na enkele jaren als gevolg van technologische ontwikkelingen weer moet worden herzien. Een gestructureerde uitwerking in doelstellingen van IT-control, procedurele standards en technieken (hard- en software, manuele controles en dergelijke) treft men derhalve niet aan.

GEVOLGEN IT-EVOLUTIE

Bij de bespreking van alle vijf componenten van een internal control-systeem komen relevante IT-aspecten naar voren. Het meest nadrukkelijk bij de onderwerpen control activities, information and communication en monitoring. Bij de onderdelen control environment en - opvallend genoeg - risk assessment vrij sporadisch.
Eén van de zeventien principles (principle 11 onder control activities) gaat specifiek over *technology* en behandelt de keuze en ontwikkeling van technology general controls in samenhang met transaction controls. Dit zijn aangepaste termen voor het bekendere begrippenpaar general controls en application controls. Begripsmatig zijn er geen verschillen.
Technology controls hebben in het rapport wel een bredere scope. Volgens de glossary en de toelichtingen blijft deze niet beperkt tot geautomatiseerde gegevens-

VOORBEELDEN GEVOLGEN BIJ INTRODUCTIE NIEUWE IT

Control Environment
- **Verbeterde toegang en communicatie van het hogere management tot lagere echelons en bedrijfsprocessen.**
- **Risico van onvoldoende IT-kennis en ervaring binnen het bedrijf.**

Risk assessment
- **Nieuwe of andere risico's.**
- **Ondersteuning risicoanalyses met verbeterde kwaliteit van gegevens en analyses.**
- **Risico's voor continuïteit en leveringszekerheid.**

Control activities
- **Invloed IT op functiescheidingen.**
- **Nieuwe opzet en keuze control-maatregelen vereist.**
- **Verhoging efficiency internal control-systeem.**

Information & communication
- **Toename beschikbare informatie.**
- **Verbreding en verdieping communicatiekanalen.**

Monitoring
- **Nieuwe methoden monitoring overwegen.**

Bron: Conceptrapport COSO

verwerking, maar behoren ook koppelingen met meet- en regelsystemen, netwerken, productierobots, productie managementsystemen en dergelijke tot het aandachtsveld.
Moderne informatietechnologie biedt bedrijven steeds weer nieuwe toepassingsmogelijkheden, maar:
- confronteert het bedrijf ook met nieuwe of andere risico's;
- bevordert effectiviteit en efficiency;
- betekent vaak toename complexiteit van beheersingssystemen; en
- beïnvloedt het tempo van verandering.

In het rapport komen deze en andere gevolgen van de continue evolutie van IT in vele voorbeelden aan de orde (*zie kader*).

IT EN FUNCTIESCHEIDINGEN

De invloed van IT op functiescheidingen wordt in het ontwerp echter niet besproken. Dat is jammer, want juist deze maatregel van control vormt een krachtig middel om misbruik (fraude, fouten, hacking etc.) te bestrijden. Control-activiteiten en IT zijn nauw gerelateerd.
Wanneer nieuwe IT in het productieproces of de dienstverlening wordt geïntegreerd, zullen de ondersteunende informatiesystemen en control-activiteiten worden aangepast. Zo vereist de introductie van nieuwe verkoopkanalen via mobiele apparatuur zoals smartphones, laptops en tablets bij deze technologie passende controles op toegang en communicatie en wijziging van de controls in de logistieke sfeer.
De mate van afhankelijkheid van IT in bedrijfsprocessen kan een indicatie zijn voor een grotere steun op IT, ook voor controls. Het management dient zich hiervan bewust te zijn en zal een gemotiveerde keuze moeten maken voor de mix: technology general controls/transaction controls, preventive/detective controls, manual/automated controls.
Ook de keuze van het niveau in de organisatie waarop de control-activiteiten worden uitgevoerd, en de timing ervan (realtime/periodiek), hangen hier nauw mee samen.

COSO EN CADBURY

Het COSO-rapport heeft in de afgelopen twintig jaar een belangrijke invloed gehad op het kijken naar de beheersing van organisaties, mede doordat in 1992 in het Verenigd Koninkrijk het Cadbury-rapport over corporate governance verscheen, waar bij latere uitwerking van het begrip *internal control* feitelijk werd gekozen voor de benadering van en de benamingen uit het COSO-framework. De combinatie van de twee rapporten (COSO en Cadbury) is van groot belang geweest voor het denken over governance.
Ook elders in de wereld is de invloed van het COSO-rapport merkbaar, zoals bijvoorbeeld in de wereldwijd aanvaarde International Standards on Auditing (ISA's). Ook in de vele corporate governance codes wordt expliciet of impliciet verwezen naar het COSO-framework. Ten slotte is COSO in verschillende landen verankerd in wetgeving, zoals de Amerikaanse Sarbanes-Oxley wet, maar ook recenter in Indonesië (Government Regulation no. 60/2008) waarin aan overheidsorganisaties verplicht een Internal Control Systeem wordt opgelegd volgens de principes van het COSO-rapport.

EÉN TAAL

Het internationaal spreken van één taal bij de beoordeling van de beheersing van organisaties is van belang voor het begrip tussen landen, volken en organisaties. Het COSO-rapport van 1992 heeft hierop een grote invloed gehad. Als het COSO-committee zich nog meer bewust is van die invloed, zou dat wellicht leiden tot nog enkele aanpassingen, die op hun beurt de invloed van het nieuwe (concept) rapport zullen vergroten en recht doen aan de internationale brede navolging tot op heden. Eind van dit jaar zullen we naar verwachting het antwoord zien. □

Noot

* *Henk den Boer is directeur van Fermera Accountancy en Advies BV en oud-universitair docent corporate governance bij Nyenrode Business Universiteit. Remko Renes is universitair docent corporate governance bij Nyenrode Business Universiteit. Luc van Zutphen is emeritus hoogleraar Vrije Universiteit Amsterdam.*
De auteurs hebben eind maart 2012 een comment letter *verstuurd naar COSO waarvan de essentie in deze bijdrage is opgenomen.*

Zie ook Accountant.nl/ Vaktechniek