Het meten van de effectiviteit van internecontrolemaatregelen

A.A. van Dijke, R.A. Jonker RE RA en ir. R. Ossendrijver

Mede door de invoering van de Sarbanes-Oxley Act en de Code Tabaksblat is het belang van het rapporteren over de effectiviteit van internecontrolemaatregelen sterk toegenomen. De afgelopen maanden is in de pers veel gepubliceerd over de implicaties die deze nieuwe regels hebben voor het aantoonbare bestaan en de effectiviteit van het interne risicobeheersings- en controlesysteem. Over de praktische consequenties die de nieuwe regelgeving heeft voor de interne bedrijfsvoering is echter nog betrekkelijk weinig gepubliceerd. In dit artikel zal daarom specifiek worden ingegaan op het meten en beoordelen van de effectiviteit van de internecontrolemaatregelen. Bovendien zal het meetproces geïllustreerd worden met een door KPMG Information Risk Management ontwikkeld softwaretool, de KPMG Business Controls Monitor, die binnen SAP R/3-omgevingen kan worden toegepast.

Inleiding

Als gevolg van de invoering van de Sarbanes-Oxley Act (SOX) voor ondernemingen die in de Verenigde Staten aan de beurs genoteerd zijn en de invoering van de Code Tabaksblat van de Commissie corporate governance is het belang van het rapporteren over de mate waarin de internecontrolemaatregelen effectief zijn geweest in een onderneming sterk toegenomen.

In de Code Tabaksblat staat in de best practice-bepaling II.1.3 het volgende:

> In de vennootschap is een op de vennootschap toegesneden intern risicobeheersings- en controlesysteem aanwezig. Als instrumenten van het interne risicobeheersings- en controlesysteem hanteert de vennootschap in ieder geval:
> a. risicoanalyses van de operationele en financiële doelstellingen van de vennootschap;
> b. een gedragscode die in ieder geval op de website van de vennootschap wordt geplaatst;
> c. handleidingen voor de inrichting van de financiële verslaggeving en de voor de opstelling daarvan te volgen procedures;
> d. een systeem van monitoring en rapportering.
>
> Bron: [Taba01]

A.A. van Dijke
is sinds 1998 werkzaam als consultant bij KPMG Information Risk Management. Hierbij is hij voornamelijk betrokken geweest bij het uitvoeren van technische audits in de SAP R/3-omgevingen (Unix, databases en SAP R/3).

vandijke.ad@kpmg.nl

R.A. Jonker RE RA
is partner bij KPMG Information Risk Management en geeft leiding aan een unit die gespecialiseerd is in Business System Controls audit en advisering.

jonker.ronald@kpmg.nl

Ir. R. Ossendrijver
is sinds 2003 werkzaam als junior consultant bij KPMG Information Risk Management. Hij is werkzaam als technisch auditor en houdt zich onder meer bezig met het ontwikkelen van auditsoftware zoals de KPMG Security Explorer en de KPMG Business Controls Monitor.

ossendrijver.ronald@kpmg.nl

Bovendien staat binnen dezelfde Code Tabaksblat onder de best practice-bepaling II.1.4 het volgende:

> In het jaarverslag verklaart het bestuur dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn en geeft hij een duidelijke onderbouwing hiervan. Het bestuur rapporteert in het jaarverslag over de werking van het interne risicobeheersings- en controlesysteem in het boekjaar.
>
> Bron: [Taba01]

De bepalingen dat er binnen ondernemingen een 'systeem van monitoring en rapportering' moet zijn en dat de 'controlesystemen adequaat en effectief' moeten zijn, maakt dat organisaties niet ontkomen aan de implementatie van een meetsysteem voor de effectiviteit van internecontrolemaatregelen.

In sectie 404 van Sarbanes-Oxley staat het volgende omtrent de verklaring die de CEO en CFO moeten afleggen in de jaarrekening:

> 1. state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
> 2. contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
>
> Bron: [SEC01]

De bepaling dat de CEO en CFO een analyse dienen op te nemen inzake de effectiviteit van internecontrolemaatregelen maakt dat internecontrolemaatregelen periodiek geëvalueerd moeten worden teneinde een betrouwbare uitspraak te kunnen doen of de maatregelen effectief hebben gewerkt in de praktijk.

Zowel SOX 404 als de twee genoemde best practice-bepalingen uit de Code Tabaksblat maken dat een implementatie van een meetsysteem voor internal controls essentieel is om aan de regelgeving te kunnen voldoen. Hierbij moet worden opgemerkt dat zowel bij SOX 404 als bij de Code Tabaksblat moet worden uitgegaan van internecontrolemaatregelen die gericht zijn op het waarborgen van de betrouwbaarheid van financiële verslaglegging. In dit artikel zal naast de 'internal controls over financial reporting' ook worden ingegaan op controls die vallen buiten de scope van SOX en de Code Tabaksblat.

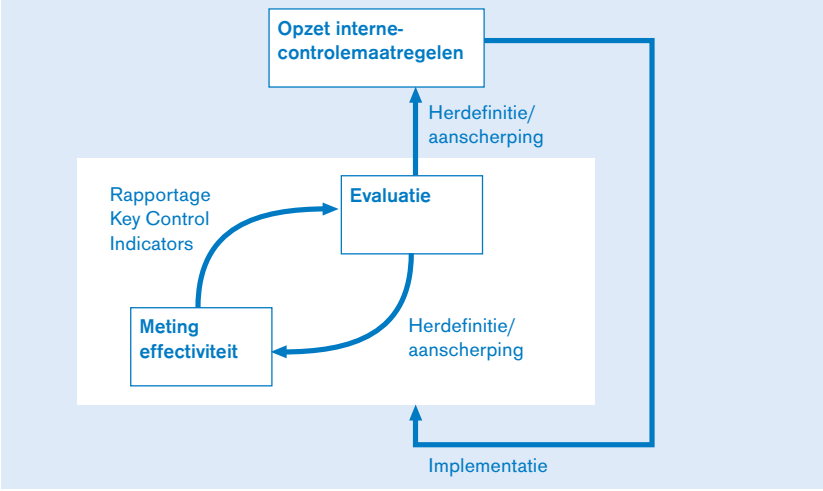
Het in figuur 1 weergegeven model beschrijft het proces van meten van de effectiviteit van de internecontrolemaatregelen. Binnen dit model wordt onder interne controle het volgende verstaan:

'COSO defines internal control as: a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
- Effectiveness and efficiency of operations;
- Reliability of financial reporting;
- Compliance with applicable laws and regulations.' ([Colb01])

Deze definitie gaat verder dan 'internal controls over financial reporting'. Efficiency wordt bij zowel SOX als de Code Tabaksblat niet als uitgangspunt gehanteerd binnen de doelstelling van internal controls.

De eerste fase van het model is de opzet van de internecontrolemaatregelen. Hierin worden de procesdoelstellingen en de bijbehorende risico's geïdentificeerd en ten slotte geanalyseerd. Veel ondernemingen hebben deze fase afgerond of zijn bezig om deze verder uit te werken voor de SOX-regelgeving.
Binnen de eerste fase worden ten slotte de internecontrolemaatregelen gedefinieerd om de onderkende risico's te kunnen beheersen zodanig dat met voldoende zekerheid de vastgelegde doelstellingen kunnen worden bereikt.
Vervolgens kan worden gestart met een iteratief proces van kwantitatieve metingen van de effectiviteit van internecontrolemaatregelen.

De mate waarin wordt voldaan aan de doelstellingen per controlemaatregel wordt kwantitatief uitgedrukt. Enkele voorbeelden hiervan zijn:
- Hoeveel doorbrekingen van kritieke functiescheidingen hebben er in het afgelopen boekjaar plaatsgehad?
- Hoeveel openstaande verkooporders staan na een bepaalde periode nog steeds open?
- Hoeveel verkooporders zijn na de afgesproken leveringsdatum beleverd?
- Hoeveel openstaande posten staan nog op de tussenrekeningen?



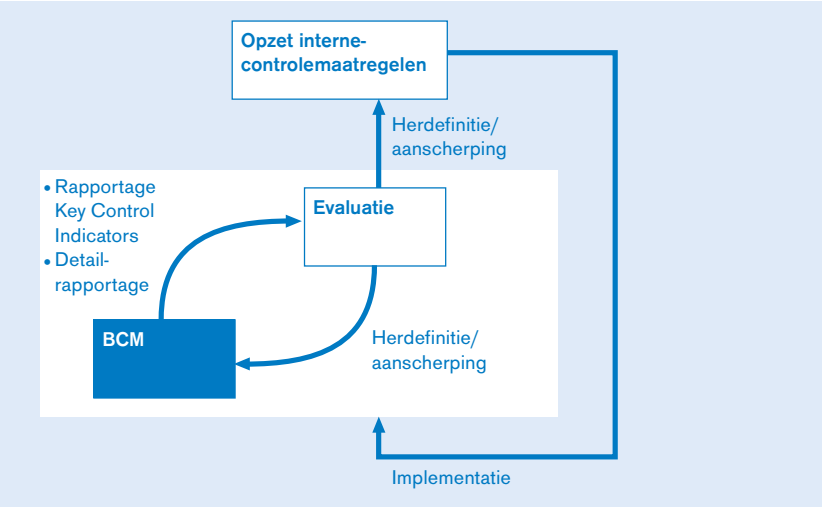
Figuur 1. Model voor de beoordeling van de effectiviteit van internecontrolemaatregelen.

De verzameling van al deze cijfers wordt in het model aangeduid als Key Control Indicators. Hiermee worden kwantitatief meetbare indicatoren bedoeld die essentieel zijn binnen de onderneming, gegeven de bovengenoemde definitie van internecontrolemaatregelen.

De kernvraag die moet worden beantwoord, is of de internecontrolemaatregelen in voldoende mate effectief zijn gebleken

Na de meting kan er een evaluatie van de Key Control Indicators worden uitgevoerd door het management van de onderneming. De kernvraag die moet worden beantwoord, is of de internecontrolemaatregelen in voldoende mate effectief zijn gebleken. Dit beoordelingsproces kan efficiënt plaatsvinden aangezien de informatie zowel volledig als kwantitatief van aard is. De complexiteit van de evaluatie is hierdoor beperkt. Echter, als blijkt dat er op punten tekort wordt geschoten, dient het management te besluiten of een aanscherping van de internecontrolemaatregelen ofwel een aanpassing van de Key Control Indicator noodzakelijk is.
Een voorbeeld hiervan is wanneer het management een controledoelstelling heeft gedefinieerd die het risico moet beperken dat de verkoopafdeling ongeautoriseerde kortingen buiten een vastgestelde bandbreedte kan verlenen aan klanten.
Als blijkt dat er té veel ongeautoriseerde kortingen worden verleend aan klanten, kan het ofwel zijn dat de autorisaties/configuratie van het systeem aangepast moet(en) worden ofwel dat de kortingsnorm aangepast moet worden, met andere woorden: de doelstelling wordt aangepast.

Figuur 2. De Business Controls Monitor opgenomen in het beoordelingsmodel.



Als blijkt dat de opzet in orde is, zal met een aanscherping van de internecontrolemaatregelen volstaan kunnen worden. Hierdoor zal er een aanscherping van de configuratiecontroles, rapportagecontroles of autorisaties moeten plaatsvinden.

Naarmate het iteratief meetproces vaker wordt doorlopen, bestaat de mogelijkheid om de opzet van de internecontrolemaatregelen alsmede de bijbehorende Key Control Indicators uit te breiden. Zo kunnen de bedrijfsprocessen die onderdeel uitmaken van het model incrementeel worden uitgebreid.

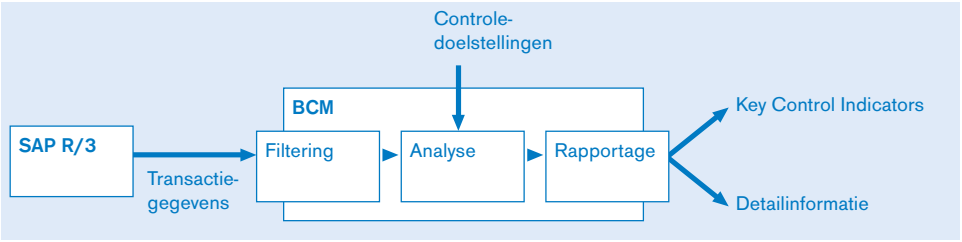
Om een betrouwbare uitspraak over de effectiviteit van internecontrolemaatregelen te kunnen formuleren, is een meetmethode nodig die werkt met grote gegevensverzamelingen afkomstig uit het bedrijfsproces waar de te analyseren controlemaatregelen gelden. Een volledige analyse van de controlemaatregelen omtrent het beheer van stamgegevens zoals klantgegevens vereist het doorzoeken van alle klantgegevens op overtredingen van die controlemaatregelen. Dit is alleen praktisch realiseerbaar door gebruik te maken van geautomatiseerde bestandsanalyses.
Het meten van de effectiviteit van controlemaatregelen binnen een geautomatiseerd systeem is effectief te automatiseren doordat gewerkt kan worden met geformaliseerde gegevens: gegevens uit het geautomatiseerde systeem, formele internecontrolemaatregelen en formele controledoelstellingen. De benodigde gegevens zijn eenduidig definieerbaar en kwantitatief van aard.

Geautomatiseerd meten met de KPMG Business Controls Monitor

Voor ondernemingen die hun bedrijfsprocessen ondersteunen met de *Enterprise Resource Planning* software SAP R/3 heeft KPMG IRM een tool ontwikkeld: de Business Controls Monitor. De Business Controls Monitor meet de effectiviteit van internecontrolemaatregelen in SAP R/3 en past daardoor in het eerder gepresenteerde model op de in figuur 2 geschetste wijze.

Figuur 3 toont de inbedding van de Business Controls Monitor in meer detail. Transacties worden direct ingelezen vanuit het SAP R/3-systeem waardoor de gegevens up-to-date en volledig zijn. Ten behoeve van de performance van het inleesproces vindt filtering plaats: alleen de gegevens die van belang zijn voor de op te leveren Key Control Indicators worden ingelezen. Deze filtering vindt plaats op basis van selectiecriteria zoals ‘te onderzoeken periode’ of ‘te onderzoeken organisatie-eenheden’. De Business Controls Monitor leest zaken als de aanwezige organisatie-eenheden en beschikbare documenttypen in uit SAP, waardoor de gebruiker eenvoudig een selectie kan maken.

Op basis van de uit SAP ingelezen transactiegegevens voert de Business Controls Monitor een analyse uit waarvan de uitkomsten worden vergeleken met de controledoelstellingen. Het resultaat van deze vergelijking wordt gerapporteerd zodat een evaluatie van de effectiviteit van de internecontrolemaatregelen kan plaatsvinden.



Figuur 3. De inbedding van de Business Controls Monitor in meer detail.

De in figuur 4 afgebeelde screenshot toont een overzicht van de mate waarin een onderneming voldoet aan haar controledoelstellingen. Standaard wordt de Business Controls Monitor uitgeleverd met ongeveer vijftig best practice Key Control Indicators.
Naast Key Control Indicators wordt ook detailinformatie gerapporteerd. In deze detailinformatie is nauwkeurig na te lezen welke afwijkingen van doelstellingen van de controlemaatregelen hebben plaatsgevonden. In het geval van '500 te lang openstaande klantfacturen' (de KCI) toont de detailrapportage de feitelijke klantfacturen die te lang openstaan. Deze informatie wordt gebruikt om follow-up actie te nemen op individuele items.

Binnen de Business Controls Monitor worden de rapportages op twee manieren ingedeeld: zowel op basis van de SAP-module als op basis van het kwaliteitsaspect van de controlemaatregelen. Tabel 1 geeft per combinatie een voorbeeldrapportage weer.

Return on investment

De Business Controls Monitor kan ondersteunen bij het ten uitvoer brengen van de nieuwe SOX-regelgeving alsmede de Code Tabaksblat. De periodieke toepassing van de Business Controls Monitor heeft met name de volgende voordelen:
- tijdsbesparing in het beoordelen van de effectiviteit van de internecontrolemaatregelen;
- inbedding van monitoring van de effectiviteit van internecontrolemaatregelen in de reguliere managementcyclus;
- reductie van licentiekosten doordat bijvoorbeeld gebruikers die nauwelijks of geen gebruik maken van SAP beter opgespoord kunnen worden.

Een verbeterde monitoring van de effectiviteit van internecontrolemaatregelen biedt onder meer de volgende voordelen:
- tijdsbesparing bij de gegevensinvoer door gebruikers doordat stamgegevens minder vervuild zijn;
- hogere interestopbrengsten doordat er een betere controle plaatsvindt op de tijdigheid van betalen door klanten;
- hogere opbrengsten doordat er een betere controle plaatsvindt op het verlenen van ongeautoriseerde kortingen;
- lagere inkoopkosten doordat er een betere leveranciersbeoordeling kan plaatsvinden.

Figuur 4. Screenshot van een deel van de Key Control Indicators.

Key Control Indicator Report - Microsoft Internet Explorer provided by KPMG

status of key control indicators

key control indicator	value	goal	alarm
Open customer invoices	87	50	30%
Incomplete sales documents	25	50	30%
Pending goods issues for outbound deliveries	2	200	30%
Customer invoices paid before or after due date	991	50	30%
Differences between PO and GR quantities	0	50	30%
Duplicate vendor invoices	0	50	30%
Idle Customers	113	50	30%
Incompleteness master data vendors	64	50	30%
Open items on Goods receipt Invoice receipt GL account	8929	50	30%
Open sales orders	52	50	30%
Open vendor invoices	677	50	30%
Users who breached the segregations of duties	21	50	30%

Module	Tijdigheid	Volledigheid	Juistheid	Efficiëntie	Exclusiviteit
Financiële boekhouding	Openstaande facturen	Onvolledige stam-gegevens crediteuren	Dubbele facturen	Niet-gebruikte grootboek-rekeningen	Wijzigingen in bankrekeningen van crediteuren
Inkoop	Openstaande bestellingen	Onvolledige stam-gegevens artikelen	Handmatig overschreven prijzen in bestellingen	Niet-gebruikte inkoop-artikelen	Wijzigingen in bestellingen
Verkoop en distributie	Openstaande verkoop-orders	Onvolledige verkoop-documenten	Handmatig overschreven prijzen in bestellingen	Niet-gebruikte verkoop-artikelen	Wijzigingen in klantcondities
Productieplanning	Niet-bevestigde productieorders	–	Verschillen tussen geplande en werkelijke productieorder-hoeveelheden	–	Wijzigingen in stuklijsten
Projectadministratie	Openstaande projecten	Onvolledige projecten	–	–	–
Autorisaties	–	–	–	Ongebruikte autorisaties	Gebruikers die de functiescheiding hebben doorbroken

Tabel 1. Voorbeelden van rapportages in de Business Controls Monitor per kwaliteitsaspect.

Conclusie

De invoering van SOX en de Code Tabaksblat levert voor ondernemingen veel praktische implicaties op ten aanzien van de implementatieaspecten. Het meten van de effectiviteit van de internecontrolemaatregelen kan alleen efficiënt worden uitgevoerd met een geautomatiseerd tool, zoals de KPMG Business Controls Monitor.

Literatuur

[Colb01] J.L. Colbert and P.L. Bowen, *A Comparison of Internal Controls*, 2001.

[SEC01] *Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports*, June 2003.

[Taba01] Tabaksblat, *De Nederlandse corporate governance code; Beginselen van deugdelijk ondernemingsbestuur en best practice bepalingen*, december 2003.