Embedded testing is efficiënt en effectief

Het middel tegen

Anders dan velen denken bestaat er wel degelijk een effectieve en efficiënte aanpak voor de audit van interne beheersmaatregelen, zoals vereist onder SOx 404. Ahold hanteert het 'natuurlijke' *embedded testing*. Daarbij kan ook de externe accountant in hoge mate steunen op de werkzaamheden van het management. En de compliance-kosten kunnen met vijftig procent omlaag.

STEPHAN GEUZEBROEK EN CEES KLUMPER*

de interne accountant

Het concept van embedded testing is zeer eenvoudig: het testen van de werking van de interne beheersmaatregelen dient onderdeel te zijn van het al bestaande en natuurlijke proces waarbinnen de beheersmaatregelen worden uitgevoerd. De tests worden vaak al op een natuurlijke wijze uitgevoerd in de vorm van review of verificatie door managers of supervisors. Het is bij embedded testing wel de bedoeling dat de tests goed worden gedocumenteerd en dat eventuele issues tijdig worden opgevolgd. Internal audit zal daarna nog steeds enige werkzaamheden uitvoeren om de kwaliteit van de testwerkzaamheden te beoordelen, maar niet langer het primaire bewijs leveren dat beheersmaatregelen werken.

Fundamenteel

In al zijn eenvoud verschilt embedded testing fundamenteel van wat de meeste SOx-plichtige organisaties tot nu toe hebben gedaan - de 'add-on'-testaanpak. Daarbij wordt het testen uitgevoerd door mensen die geen onderdeel uitmaken van het reguliere proces. Vaak is dit de internal auditafdeling, andere specifieke internal control-specialisten of personen van een andere afdeling binnen de organisatie (*peer review testing*).

Embedded testing heeft belangrijke voordelen:

- het is veel natuurlijker;
- de kosten om compliant te zijn met SOx 404 dalen met de helft;
- er wordt veel meer getest;
- zwakheden in de beheersing (*control weaknesses*) worden geïdentificeerd door de personen die daartoe het best gepositioneerd zijn;
- control weaknesses worden sneller onderkend;
- alleen tests die echt iets toevoegen worden uitgevoerd;
- het control-bewustzijn van managers wordt verder vergroot.

Dubbel werk

Een voorbeeld ter verduidelijking. Als een administratief medewerker een aansluiting maakt tussen sub- en grootboek, wordt dit doorgaans in het reguliere proces gereviewed door zijn supervisor of manager. Met deze review wordt vastgesteld dat:

- de aansluiting is uitgevoerd en gedocumenteerd volgens de overeengekomen richtlijnen;
- aansluitingsverschillen afdoende zijn verklaard;
- eventuele verschillen afdoende zijn opgevolgd.

De supervisor voegt hierbij in feite geen nieuwe informatie toe. Hij controleert - beter gezegd: test - eenvoudig of de persoon die de aansluiting heeft gemaakt zijn werk juist heeft uitgevoerd, daarmee vaststellend dat de beheersmaatregel (de aansluiting) heeft gewerkt. Bij add-on-testing daarentegen test iemand anders (bijvoorbeeld een internal auditor) de aansluiting, en doet in feite het werk van de supervisor nog eens over.

In het pre-SOx-tijdperk waren managers echt niet onwetend.

Onnodig en inefficiënt

Op dit moment hebben veel beheersmaatregelen die voor SOx 404 als key zijn bestempeld een review - of monitoring - karakter. Managers testen de beheersmaatregelen, omdat zij nu eenmaal willen weten of de mensen die aan hun rapporteren hun werk goed uitvoeren, dat de informatie die uit het proces komt betrouwbaar is, dat fouten worden gevonden voordat zij problemen kunnen veroorzaken en dat verbeteringen kunnen worden doorgevoerd om toekomstige fouten te voorkomen.
Dit werd al gedaan lang voor SOx 404, en zal

FOTO'S: SIMONE VAN ES

SOx-blues

Stephen Geuzebroek (rechts) en Cees Klumper:

'Veel organisaties hebben een add-on-testaanpak gekozen omdat de externe accountant dit heeft geadviseerd of zelfs vereist.'

Internal audit zal nog wel de kwaliteit van de testwerkzaamheden beoordelen, maar niet langer het primaire bewijs leveren dat beheersmaatregelen werken.

altijd gedaan blijven worden. Het is onderdeel van de 'natuurlijke' *plan-do-check-act* managementcyclus, en aan deze test zouden de juiste *credits* gegeven moeten worden in het SOx 404-proces.
Op deze manier bekeken is de door een buitenstaander uitgevoerde add-on-test inefficiënt. Sterker, zolang het management de beheersmaatregelen zelf adequaat blijft testen, is een add-on-test volstrekt onnodig. Bijna alle organisaties laten management testing nu wel uitvoeren door andere personen dan het management zelf. Aangezien gemiddeld meer dan de helft van de SOx 404 compliance-kosten opgaan aan add-on testing is dit een kostbare exercitie.

Beste positie

Als embedded testing het al bestaande Ei van Columbus is, waarom besteden organisaties dan toch nog zoveel energie aan add-on-testing? Het antwoord houdt verband met het moment van implementatie van SOx 404. De *guidance* daarbij was destijds sterk gefocused op de externe accountants, die door toezichthouder PCAOB werd opgedragen hun eigen assessment uit te voeren. Nu is een specifieke eigenschap van externe accountants dat zij ... extern zijn! Zij weten op geen enkele wijze uit de eerste hand, op basis van eigen observatie, of de beheersmaatregelen werken zoals beschreven. Zij moeten dus wel add-on-testen. Het management daarentegen *is* in de positie (de *beste* positie) om te weten of maatregelen voldoen, aangezien men de gehele dag aanwezig is en ze ziet werken. Ze worden er voor *betaald* om zeker te stellen dat de beheersmaatregelen werken, en correcties aan te brengen als dat niet zo is.
In het pre-SOx-tijdperk waren managers echt niet onwetend. Met add-on-testing is dat echter precies wat wordt verondersteld: dat zonder iemand van buiten te laten komen, het management werkelijk geen idee heeft of haar beheersmaatregelen werken zoals bedoeld en alleen maar 'hoopt'. Dit is natuurlijk niet het geval. Dus waarom worden dan niet de credits gegeven aan de monitoring-achtige tests die het management toch al uitvoert?

Van impliciet naar expliciet

Er zijn ook andere redenen waarom de meeste organisaties add-on-testing toepassen. Een valide reden is dat organisaties al hun beheersmaatregelen wel *moesten* documenteren en testen om zeker te weten waar hun *control weaknesses* zaten en welke managers hun review-werkzaamheden adequaat uitvoerden. Het meeste daarvan gebeurde namelijk impliciet in plaats van expliciet. Nu alle beheersmaatregelen zijn gedocumenteerd en de werking is getest, is het gehele proces eindelijk expliciet geworden.
Eén van de belangrijke vereisten voor management testing is dat dit afdoende gedocumenteerd moet zijn, ook omdat tests herhaalbaar moeten zijn door derden, zoals de externe accountant. Vóór SOx 404 was zo'n afdoende vastlegging er zelden. Dus om daadwerkelijk gebruik te kunnen maken van tests die al in het reguliere proces worden uitgevoerd, moest eerst worden aangetoond dat ze ook echt plaatsvonden. Na de initiële implementatie van SOx is dat bewijs er. Managers zijn gewend geraakt aan het documenteren van hun controls (inclusief de controls die ook kwalificeren als test) en we kunnen van deze tests gebruik gaan maken. Er is geen reden om ze twee keer te doen, of te blijven testen wat zelf al een test is.

Twee uitzonderingen

Waar de externe accountant altijd een zekere mate van add-on-testing zal moeten uitvoeren, hoeft dat voor een organisatie zelf in beginsel niet. Daarop zijn twee uitzonderingen:

1. Daar waar management testing efficiënter kan worden uitgevoerd door specialisten. Een voorbeeld hiervan is de filiaalcontrolefunctie in de grotere retail-organisaties. Bij zulke organisaties zouden de regionale managers kunnen worden belast met het checken van de belangrijkste controls, maar dit zou niet efficiënt zijn.
2. Daar waar de benodigde kennis dusdanig specialistisch is, is het voor de organisatie efficiënter om deze kennis niet intern te hebben maar de *check* over te laten aan een externe partij. Een voorbeeld zijn de interne actuarissen van verzekeringsmaatschappijen, waarvan het werk van tijd tot tijd wordt geverifieerd door externe specialisten. Of de treasury-afdeling die zich met allerlei exotische strategieën en producten bezighoudt. Ook dan wordt veelal een externe partij gevraagd om dit te verifiëren.

Minder goede reden

Een andere, minder goede reden waarom veel organisaties een add-on-test-aanpak hebben gekozen is eenvoudigweg omdat de externe accountant of adviseur, zich onbewust van een mogelijke andere aanpak, dit heeft geadviseerd of zelfs vereist. Vanuit het perspectief van de externe accountant is dat wel logisch. Voor de organisatie echter is het uitermate kostbaar, tegennatuurlijk en inefficiënt om op deze wijze de benodigde assurance te verkrijgen.
Vaak is ook vanwege de eenvoud gekozen voor de add-on-methode. De gebruikelijke aanpak was 'eerst documenteren, dan testen'. Dus werden eerst alle beheersmaatregelen (ook de

Waarom worden niet de credits gegeven aan de tests die het management toch al uitvoert?

minder relevante) gedocumenteerd. Daarna werden testplannen gemaakt voor elke beheersmaatregel en begon men met testen - vergetend dat veel van de gedocumenteerde beheersmaatregelen zelf al een test waren! Een positief neveneffect was er wel: waar managers hun review onvoldoende documenteerden werd dat geïdentificeerd en hersteld, als onderdeel van het zogenaamde *evidence gap remediation*.

Drie belangrijke voorwaarden

Een eerste belangrijke voorwaarde voor embedded testing is dat de interne auditfunctie verifieert of het management haar tests adequaat uitvoert en documenteert. Dit zal zij doen door de uitgevoerde tests op *sample* basis te beoordelen. Internal audit zal dus niet zelf de beheersmaatregelen nogmaals gaan testen!
Een tweede vereiste is dat managers continu worden ondersteund bij het definiëren van de juiste testactiviteiten (inclusief reikwijdte, vereiste documentatie etc.) en bij het interpreteren van de testresultaten. Deze ondersteuning zou kunnen worden gedaan door dezelfde personen die belast zijn met de andere SOx 404-activiteiten (*scoping*, *risk assessment*, control-documentatie etc.).
Een derde voorwaarde is dat het vastleggen van de testuitkomsten voor het management zo makkelijk mogelijk moet worden gemaakt. Daarbij is een effectieve software tool, die de organisatie ook in staat stelt om de voortgang te monitoren, onontbeerlijk. Waar organisaties met een add-on-testaanpak vaak nog wegkomen zonder zo'n *tool* - vooral omdat slechts een kleine groep 'experts' de tests uitvoert - zal dit veranderen in de embedded testing-aanpak, waarbij vele managers betrokken zijn.
De investeringen (tijd en geld) die deze drie voorwaarden vergen, zullen echter maar een fractie zijn van hetgeen wordt bespaard.

Als een manager niet objectief de prestaties van zijn medewerkers kan beoordelen, zou hij geen manager moeten zijn in die positie.

Hoe maak ik deze draai?

Het aanpassen van het SOx 404-proces is niet makkelijk. Het betekent een her-evaluatie van het gehele control framework, vanuit een ander perspectief. Het onderscheid tussen beheersmaatregelen, *key*-beheersmaatregelen en tests moet worden geherdefinieerd.
Beheersmaatregelen die nu niet worden gereviewed in het normale business-proces, moeten opnieuw worden bekeken: waarom voert de betrokken manager nog geen review uit op adequate werking? Als blijkt dat management review de eerste en enige manier was om assurance te krijgen, zullen nieuwe beheersmaatregelen moeten worden geïmplementeerd.
Maar het is het allemaal meer dan waard!

Een Engelstalige versie van dit artikel is in januari 2007 aan de SEC gezonden, als bijlage bij een comment letter van Cees Klumper en Matt Shepherd (Amerikaanse CPA) op de voorgestelde nieuwe richtlijnen voor SOx 404. In de comment letter werden enkele wijzigingen voorgesteld om de nieuwe richtlijnen beter te laten aansluiten op de embedded testing-aanpak. Op uitnodiging hebben Klumper en Shepherd vervolgens op 9 februari 2007 ten kantore van de SEC een nadere toelichting gegeven, tijdens een meeting met zes betrokken medewerkers. ■

SEC en PCAOB over embedded testing

Met betrekking tot de testaanpak heeft de Securities and Exchange Commission in zijn voorgestelde nieuwe *guidance* voor management een fundamenteel punt opgenomen dat erkenning geeft aan het belang van embedded testing binnen het SOx 404-compliance-proces.
De nieuwe *guidance* van de Public Company Accounting Oversight Board bevat daarentegen een bepaling die enigzins in tegenspraak lijkt met wat de SEC voorstelt: de PCAOB geeft namelijk aan dat de externe accountant geen gebruik kan maken van testactiviteiten van managers die verantwoordelijk zijn voor het gebied waarvan de geteste control deel uitmaakt. In onze ogen is dit een onnodige bepaling, die een (mogelijk onbedoeld) belemmerend effect op de efficiency van het SOx 404-proces heeft.

Objectiviteit en competentie

Kan een manager zowel objectief als competent zijn? Het antwoord is 'ja'. Dit is het fundamentele principe van functiescheiding. Waarom zou nog een *supervisory review* uitgevoerd moeten worden als deze persoon niet als objectief kan worden gezien ten opzichte van degene die de beheersmaatregel uitvoert? Als een manager niet objectief is tegenover degenen die hij in dienst heeft genomen en niet objectief de prestaties van zijn medewerkers kan beoordelen, zou hij geen manager moeten zijn in die positie. Hetzelfde geldt voor competentie. De directe lijnmanager zou de meest competente persoon moeten zijn om het werk van de medewerkers te beoordelen. En zeker minstens zo competent als iemand van buiten die add-on-testing komt doen. Om de kwaliteit van de tests door het management te waarborgen, zal internal audit deze steekproefsgewijs moeten beoordelen.

Noot

* Stephan Geuzebroek en Cees Klumper zijn respectievelijk director en vice president Internal control bij Ahold.