De IT Dependent Manual Control; een nog te verkennen gebied binnen de auditing

Xander Merkelbach

SAMENVATTING Het fenomeen IT Dependent Manual Control is binnen de accountancy een bestaand, maar beperkt ingevuld begrip. Door de introductie van de Sarbanes-Oxley Act (SOx) in 2002 is de IT Dependent Manual Control meer in de schijnwerpers komen te staan. De internationale auditing standaarden geven echter weinig houvast omtrent deze materie, waardoor ook accountants moeite hebben met dit fenomeen. Dit artikel heeft als doel om te komen tot een verheldering van de begripsvorming en geeft tevens een aanpak om te komen tot de uiteindelijke implementatie van de IT Dependent Manual Control voor SOx.

1 Inleiding

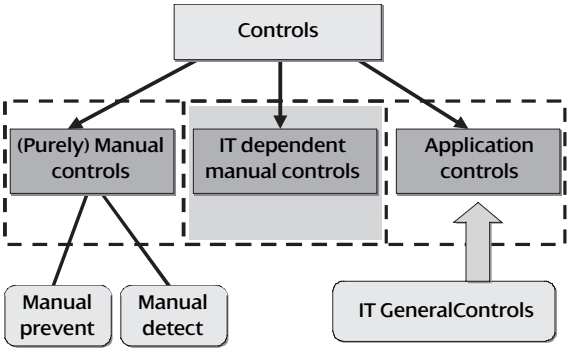
De internationale auditing standaarden voor het vormgeven, inrichten en aantonen van een effectief internal control framework, gaan uit van de standaardonderverdeling van belangrijke bedrijfscontroles in manual en application controls; controls die door mensen worden uitgevoerd of controls die door applicaties worden uitgevoerd in de vorm van een geprogrammeerde procedure. Door de steeds verder toenemende afhankelijkheid en integratie van informatietechnologie (IT) in de bedrijfsvoering van ondernemingen is een vervaging opgetreden in deze standaardtypering van de key controls.
Het standaardonderscheid van manual en automated controls dekt in een steeds verder automatiserende bedrijfsomgeving niet meer de volledige lading. Om dit 'hiaat' te vullen is binnen de accountancy de IT Dependent Manual Control geïntroduceerd. Door de introductie van de Sarbanes-Oxley Act is deze IT Dependent Manual control meer in de schijnwerpers komen te staan. Ondernemingen worden hierdoor door de controlerende accountant verplicht binnen het controleframework invulling te geven aan dit fenomeen. Maar wat is nu een IT Dependent Manual Control precies en hoe moet hier in de praktijk mee om worden gegaan?
Als antwoord op deze vragen wordt in paragraaf 2 het begrip IT Dependent Manual Control geplaatst binnen de standaardcontrole-onderverdeling, wordt in paragraaf 3 het begrip nader gedefinieerd, waarna in de paragrafen die volgen een concrete invulling wordt gegeven over hoe met het fenomeen IT Dependent Manaual Controls in de praktijk kan worden omgegaan.

Drs. A.P.N. Merkelbach is sinds zijn studie Bedrijfskunde aan de Katholieke Universiteit Nijmegen werkzaam in de consultancy. Sinds 2004 werkt hij als Senior Business Consultant bij Atos Consulting.

2 De standaardcontrole-onderverdeling

Waar voorheen manual en application controls 'zwart-wit' genoemd konden worden, is door de voortschrijdende automatisering in toenemende mate sprake van een 'grijs' gebied. Dit grijze gebied wordt gevormd door de manual controls die zich bevinden op de punten waar het handmatige proces en de geautomatiseerde processen elkaar raken en soms in elkaar overgaan. Doordat op deze connectiepunten sprake is van een dusdanige integratie van IT en de uitvoering van de manual controls, zijn beide niet meer los van elkaar te bekijken. Controles waar het hier onder andere om gaat bevinden zich rondom de invoer van data in systemen, reconciliaties van systeemadministraties en het wegwerken van verschillen of uitvallijsten welke door een systeem zijn gegenereerd. Om aan dit onderkende grijze gebied invulling te kunnen geven, is binnen de accountancy het fenomeen IT Dependent Manual Control ofwel ITDMC geïntroduceerd (zie figuur 1).

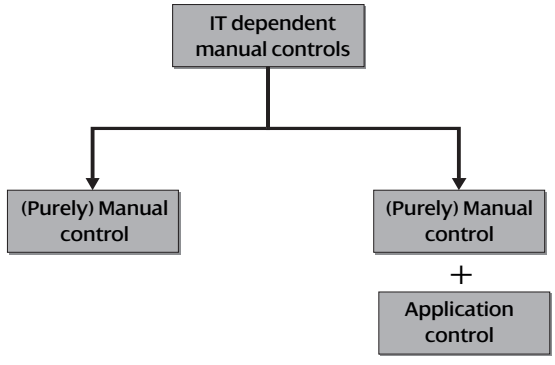
Figuur 1



3 De IT Dependent Manual Control

Ondanks de naamgeving is de IT Dependent Manual Control geen controltypering, maar een tussenstation van waaruit de uiteindelijke control of controls worden bepaald. De essentie hierbij is dat iedere IT Dependent Manual Control op het eindstation opgaat in een of twee relevante controls. Dit kan een pure manual control, ofwel een pure manual control én een application control zijn (zie figuur 2). Op deze wijze wordt de IT Dependent Manual Control dus weer terugherleid naar de basisonderverdeling van manual en application controls.

Figuur 2



Door dit uiteenvallen van de ITDMC in de basiscontroltyperingen hoeft de ITDMC niet zelf te worden beschreven, ingericht en aangetoond. Het eindstation van de ITDMC, alleen een pure manual control of een pure manual en een application control, moet daarentegen wel worden beschreven, ingericht en aangetoond. Hiervoor gelden dan de algemene auditing standaarden voor manual en application controls.
Ondanks het erkennen en introduceren van het begrip ITDMC ontbreekt het tot op heden, binnen de auditing standaarden, aan een formele en eenduidige definitie van dit steeds belangrijker wordende begrip. Om in de praktijk toch met het ITDMC-fenomeen om te kunnen gaan, hebben meerdere partijen, zoals accountantskantoren, een definitie gegeven aan het begrip. Ter illustratie is één van de ITDMC-definities in figuur 3 weergegeven.

Figuur 3

> IT-dependent manual controls are activities performed by an individual, using for instance a system-generated report, e.g. resolution of exceptions by an individual based on a system-generated exception report related to a reconciliation.
>
> Rajamani, B.; Certifying automated information technology controls, Deloitte.

Op grond van de beschikbare definities ontstaat wel een algemeen beeld van wat een IT Dependent Manual Control nu is, maar geheel eenduidig is dit beeld niet. Gemeenschappelijk in de definities is wel dat het bij de ITDMC gaat om een handmatig uitgevoerde controle met een directe afhankelijkheid van IT. Op basis van deze twee kernelementen is de defenitie van een IT Dependent Manual Control als volgt te formuleren.
'Een IT Dependent Manual Control is een handmatig uitgevoerde controle die bij de uitvoering in grote mate afhankelijk is van een door het systeem gegenereerde uiting in de vorm van een lijst of een computerscherm.'

4 ITDMC en de op risico gebaseerde aanpak

Een definitie is noodzakelijk om te komen tot draagvlak omtrent de aanpak. In het geval van de ITDMC gaat het om de punten 'hoe' en 'op basis waarvan' wordt bepaald of een ITDMC uiteenvalt in alleen een manual control of in een manual én een application control. Met andere woorden: op basis van welke criteria wordt bepaald of de betrouwbaarheid van de systeemuiting, die bij de uitvoering van de manual control wordt gebruikt, moet worden aangetoond? Vanuit het controlerend orgaan, de SEC (US Securities en Exchange Commission), is vooralsnog het antwoord op de vragen het gebruik van de breed toepasbare Risk Based Approach (RBA) (zie figuur 4).
Uitgangspunt van deze RBA is om de 'in control' inspanningen vooral te richten op die controls die het

grootste risico vormen. Dit betekent dat de inspanning vooral gericht moet worden op de controls die een dusdanig risicoprofiel hebben dat ze een verhoogde kans hebben op een materiële impact op de financiële verslaglegging.

Figuur 4

Risk Based Approach
The desired approach should devote resources to the areas of greatest risk and avoid giving all significant accounts and related controls equal attention without regard to risk.
The assessment of internal control over financial reporting will be more effective if it focuses on controls related to those processes and classes of transactions for financial statement accounts and disclosures that are most likely to have a material impact on the company's financial statements.

US Security and Exchange Commission, Staff Statement on Management's Report on Internal Control Over Financial Reporting (May 16, 2005).

Wanneer de SEC-omschrijving van de Risk Based Approach nader wordt bestudeerd, blijkt dat de RBA wel richting geeft aan een aanpak, maar dat het inhoudelijk niet voldoende concreet is. De centrale vragen: 'Wat doe je precies?' en 'Op basis waarvan?' blijven hier namelijk onbeantwoord. Dit heeft voor de ITDMC-problematiek tot gevolg dat het ook voor de accountants lastig is om tot een eenduidige aanpak te komen (zie figuur 5).

Figuur 5

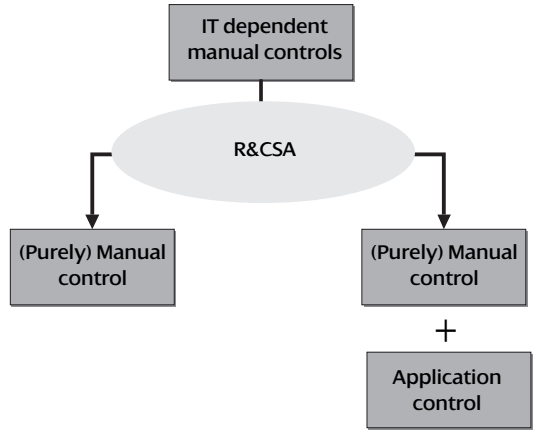
The challenge arises when organizations begin to consider whether they must document and test the automated control as well as the manual control, or whether they can simply confine their reviews to the manual controls.

Rajamani, B.; Certifying automated information technology controls, Deloitte

Nu binnen de accountancy de definitie van de ITDMC niet geheel eenduidig is en de ITDMC-problematiek ook vanuit de RBA aanpak geen concrete invulling krijgt, ontstaat op het ITDMC-gebied een soort status quo. Aan de ene kant moeten ondernemingen iets met het begrip ITDMC, maar door het huidige gebrek aan duidelijkheid worden door deze zelfde ondernemingen op dit gebied geen of te weinig organisatiebrede stappen ondernomen. Het invullen van de ITDMC-problematiek wordt hierdoor regelmatig gereduceerd tot lokale initiatieven.

Een manier om toch tot een concrete en organisatiebrede aanpak binnen de Risk Based Approach te komen, die gefundeerd de IT Dependent Manual Control opsplitst in alleen een pure manual control of een pure manual én een application control, is het toepassen van de erkende Risk and Control Self Assessment (R&CSA) (zie figuur 6).
De R&CSA is een interactieve methodiek die in toenemende mate door het bedrijfsleven wordt erkend als een krachtige methodiek die het management, de accountant en andere betrokkenen in staat stelt om bedrijfsprocessen en de effectiviteit van de hierin voorkomende controls te beoordelen. De essentie van de methodiek is om vanuit verschillende invalshoeken tot een oordeel te komen over het risicoprofiel. Dit risicoprofiel kan betrekking hebben op een proces, een systeem maar ook op een control. Door het toepassen van de methodiek krijgen de diverse participanten inzicht in de relevante risico's en kan het meest effectieve design van de control(s) worden bepaald.
Ondanks de bruikbaarheid van de Risk and Control Self Assessment, is een standaardmethodiek, zoals de R&CSA die hanteert, niet direct toepasbaar in de situatie van de IT Dependent Manual Control. De methodiek, die haar oorsprong heeft in het operationele risicomanagement, moet eerst ITDMC-specifiek worden gemaakt, zodat een onderneming in staat is om per ITDMC vast te stellen wat het risicoprofiel is. De essentie hierbij is dat de methodiek wordt aangepast van het vaststellen van een profiel van een operationeel risico naar het vaststellen van het risicoprofiel van een controle. Op basis van dit vastgestelde profiel kan vervolgens de consequentie voor de betreffende IT Dependent Manual Control worden vastgesteld. Kortom, een R&CSA

Figuur 6



aanpak voor de IT Dependent Manual Control moet inzicht geven in de noodzaak om de betrouwbaarheid van de bij de manual control gehanteerde systeemuiting aan te tonen. Dit aantonen vindt dan plaats door het, conform de standaard auditing richtlijnen, beschrijven en testen van een application control omtrent de betrouwbaarheid van de betreffende systeemuiting.

5 De ITDMC R&CSA

De kernvragen die binnen de aangepaste ITDMC R&CSA aan de orde moeten komen, spitsen zich toe op het risicoprofiel van de control en van de systeemuiting of uitingen die hierin centraal staat / staan.
Belangrijke aspecten hierbij zijn:

- Analyseren van de functionaliteit achter de systeemuiting.
- Vaststellen van het belang van de systeemuiting in de uitvoering van de manual control.
- Bepalen van de noodzaak om de betrouwbaarheid van de systeemuiting aanvullend aan te tonen.
- Vaststellen van de mogelijkheid op een materiële fout bij de uitvoering van de manual control wanneer de systeemuiting niet juist en volledig is.

Het analyseren van de functionaliteit van de systeemuiting is gericht op het inzicht krijgen in de aard en de complexiteit van de systeemuiting. Vastgesteld dient bijvoorbeeld te worden of ten behoeve van de systeemuiting door het systeem data worden bewerkt of dat de systeemuiting betrekking heeft op meerdere posten. Doel hierbij is om een stuk risicobepaling rondom de systeemuiting uit te voeren. De centrale uitgangspunten hierbij zijn dat een systeemuiting die op basis van complexe functionaliteit tot stand is gekomen, zoals een systeem uitvallijst, een verhoogd risico heeft en dat de systeemuiting die is gebaseerd op een eenvoudige functionaliteit, zoals het weergeven van een vast databasegegeven (bijvoorbeeld een gescande handtekening) een laag risicoprofiel heeft. In andere woorden, de complexiteit van de bewerkingsfunctionaliteit en daarmee de gevoeligheid hiervan bepalen de hoogte van het risicoprofiel van de systeemuiting.
Bij het bepalen van het belang van de systeemuiting is risicobepaling eveneens het uitgangspunt. Het risico wordt hierbij bepaald op basis van het belang van de systeemuiting ten opzichte van de uitvoering van de manual control. De centrale vraag die hier speelt is of de systeemuiting als norm wordt gehanteerd bij het uitvoeren van de manual control of dat de systeemuiting de standaard is op basis waarvan getoetst wordt. Indien blijkt dat de systeemuiting als norm wordt gehanteerd, dan is de betrouwbaarheid van de systeemuiting direct bepalend voor de uitkomst van de manual control. Een voorbeeld hiervan is een door het systeem ondersteunde controle op handtekening. Bij deze vorm van controle wordt de geverifieerde en gescande handtekening in het systeem vergeleken met de handtekening op bijvoorbeeld het opdrachtformulier. De handtekening die door het systeem wordt getoond is hierbij de norm voor de uit te voeren manual control. Voor de effectieve werking van de manual control is het in dit voorbeeld van groot belang dat de handtekening in het systeem betrouwbaar is. Het risicoprofiel van de systeemuiting is hierdoor hoog. Indien de norm van de uitvoering van de manual control buiten het systeem of de systeemuiting ligt, is sprake van een laag risicoprofiel. Een voorbeeld hiervan is de aansluitingscontrole van een productiesysteem met het financiële systeem, waarbij de norm niet een van de twee systeemuitingen is, maar dat geen verschil geconstateerd mag worden. In dit geval is het risico laag dat één van de systeemuitingen of beide systeemuitingen onjuist zijn. De norm, dat het verschil tussen beide lijsten nul moet zijn, maakt dat dit risico verwaarloosbaar is.
Wanneer de betrouwbaarheid van de systeemuiting wordt bepaald, verschuift de scope van risicobepaling naar kansbepaling. De essentie is hier om vast te stellen wat de kans is dat de systeemuiting niet betrouwbaar is. Om dit te kunnen vaststellen staan twee zaken centraal. De eerste is de vraag of de betrouwbaarheid van de systeemuiting in één oogopslag bepaald kan worden. Een voorbeeld hiervan is de detailcontrole op de invoer. De kern is hierbij dat de juistheid van de invoer wordt gecontroleerd. Dit gebeurt in de praktijk vaak in de vorm dat medewerker A op basis van het brondocument invoert en dat medewerker B op basis van ditzelfde brondocument de invoer in het systeem accordeert. Doordat medewerker B de in het systeem ingevoerde data één op één vergelijkt met het brondocument is de betrouwbaarheid van de systeemuiting direct vast te stellen. Het tweede belangrijke punt is om vast te stellen of recente testresultaten van gebruikersacceptatie aanwezig zijn die een specifieke uitspraak doen over de betrouwbaarheid van de systeemuiting. Wanneer deze inderdaad aanwezig zijn, is de kans dat de systeemuiting niet betrouwbaar is, als laag te beschouwen.
Het aspect met betrekking tot het vaststellen wat de kans is dat een foutieve systeemuiting leidt tot een mogelijke materiële fout in de uitvoering van de manual control, is eveneens verbonden aan de kansbepaling. Centraal hierbij staat of een afwijking c.q. fout ten

opzichte van de norm in de systeemuiting direct wordt geconstateerd en dit vervolgens per definitie leidt tot een stoppende werking of vervolgactie in de manual control. Teruggrijpend op het eerdere voorbeeld geldt dat wanneer de handtekening in het systeem niet juist is, deze nooit overeen kan komen met de handtekening op het brondocument. Daar de gelijkheid van de handtekeningen de essentie is van deze controle, leidt een foutieve systeemuiting in dit geval tot een stoppende werking. Nu kan echter beargumenteerd worden dat deze stoppende werking in dit geval onterecht is en dat geen materieel, maar wel een claimrisico wordt gelopen. In de praktijk blijkt dat dit claimrisico doorgaans zeer laag is, omdat de controls rondom klachtenmanagement dit hoofdzakelijk afvangen.

6 Toepassen ITDMC R&CSA

Nadat de ITDMC R&CSA methodiek is geconcretiseerd met vragen en de weging van de antwoorden is vastgesteld, is de implementatie of uitrol van de methodiek de volgende stap. Gezien de aard van de specifieke ITDMC R&CSA-vragen is het noodzakelijk dat het toepassen op lokaal niveau gebeurt. Specifieke kennis omtrent de uitvoering van de manual control en de hierbij gebruikte systeemuiting is namelijk essentieel om te komen tot een juiste beantwoording van de opgestelde vragen. Omdat de R&CSA in essentie interactief van aard is, is een manier om dit realiseren het organiseren van lokale sessies. Uitgangspunt van deze sessies is dat het geheel aan manual controls door de methodiek wordt gehaald. De volgende stappen worden hierbij genomen:

Per manual control vaststellen of sprake is van een ITDMC.

Door middel van een R&CSA per ITDMC het risicoprofiel bepalen.

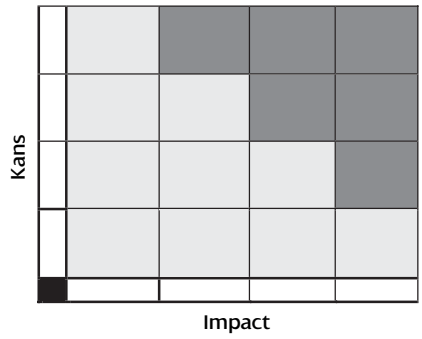
Consequenties van het risicoprofiel vastleggen.

1

Door middel van het toepassen van de geconcreti-
2 seerde R&CSA wordt het risicoprofiel per vastge-
3 stelde ITDMC bepaald. Dit gebeurt op basis van het geheel aan geformuleerde antwoorden op de specifieke ITDMC R&CSA vragen. In lijn met de weging die aan de mogelijke antwoorden vanuit de R&CSA zijn gegeven, kan vervolgens per ITDMC de voor de ITDMC R&CSA aangepaste risicomatrix worden ingevuld (zie figuur 7).

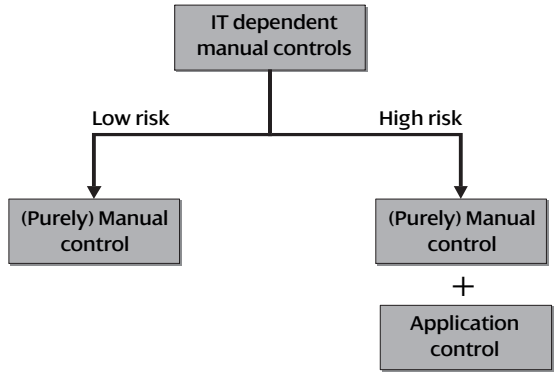
Afhankelijk van de combinatie risico en kans wordt het risicoprofiel van de ITDMC zichtbaar gemaakt. De combinatie bepaalt of de ITDMC in de risicomatrix een high risk indicator of een low risk indicator krijgt. Zoals uit de term indicator blijkt, moet de uitkomst in de risicomatrix als indicatie worden beschouwd. Het senior management is verantwoordelijk voor de uiteindelijke vaststelling van het definitieve risicoprofiel van de ITDMC. Het professional judgement van het management is hierbij de basis voor de beslissing.

Figuur 7: Voorbeeld ITDMC R&CSA risicomatrix



Vanuit het vastgestelde risicoprofiel van de ITDMC kunnen de consequenties van dit profiel worden bepaald. Hierbij geldt de primaire onderverdeling dat een low risk ITDMC beschouwd moet worden als een pure manual control en dat de high risk ITDMC uiteenvalt in een pure manual control en een application control (zie figuur 8).

Figuur 8



Wanneer sprake is van een low risk ITDMC kan de control dus beschouwd worden als een pure manual control. De consequenties hiervan zijn verwaarloosbaar. Daar de control reeds in essentie als manual was beschouwd, verandert deze vaststelling niets aan de beschrijving van de control en het vaststellen van de effectiviteit van de controle. Echter, wanneer sprake is van een high risk ITDMC, heeft dit wel de nodige

gevolgen. Naast het definiëren en aantonen van de pure manual control, zoals bij de low risk ITDMC, moet in dit geval een application control worden gedefinieerd. Bij het definiëren en aantonen van deze control staat de betrouwbaarheid van de systeemuiting centraal. Uitgangspunt hierbij is om de betrouwbaarheid van de systeemuiting aan te tonen door de functionaliteit van deze systeemuiting te testen.

7 Conclusie

Duidelijk is dat de IT Dependent Manual Control een fenomeen is dat steeds meer op de agenda van de accountantskantoren komt te staan. Door het ontbreken van een formele en eenduidige definitie en aanpak in huidige auditing standaarden, moeten ondernemingen samen met de (controlerend) accountant komen tot een eigen invulling om met de ITDMC-problematiek om te gaan. De intentie van dit artikel is om handvatten aan te reiken om de benodigde inhoud aan deze aanpak te geven. ■

Literatuur

Emanuels, J.A., O.C. van Leeuwen en Ph. Wallage (2004). Internal control volgens Sarbanes Oxley. *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 78, no. 7/8 (juli/augustus), pp. 348-355.

Rajamani, B., Certifying automated information technology controls. http://www.deloitte.com.

Division of Corporation Finance, Office of the Chief Accountant, US Security and Exchange Commission. Staff Statement on Management's Report on Internal Control Over Financial Reporting (May 16, 2005), http://www.sec.gov.

Public Company Accounting Oversight Board, http://www.pcaobus.org.

Sarbanes-Oxley - Financial and Accounting Disclosure Information; http://www.sarbanes-oxley.com