De spreadsheet van het strafbankje

Een pragmatische aanpak voor End User Computing

Trudy Onland

Sinds de introductie van Sarbanes Oxley wet (SOx) ontbreken duidelijke en eenduidige richtlijnen voor End User Computing (EUC). Uit de praktijk blijkt dat bedrijven die aan SOx moeten voldoen veel tijd besteden aan EUC, zonder daar een goed gevoel bij te hebben.

Auteur

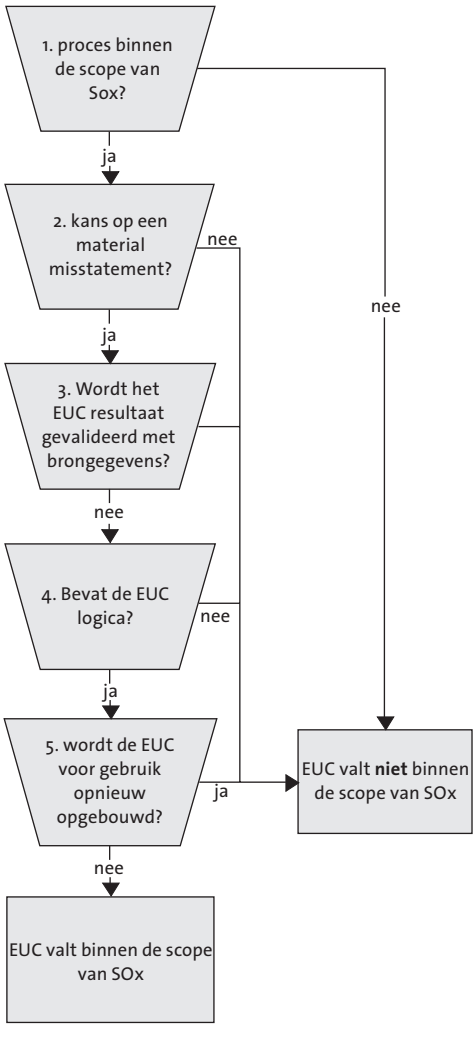
Ing. G.M. Onland RE MSc is Senior Manager bij KPMG en werkt als IT-auditor bij IT Advisory. De afgelopen jaren is zij betrokken geweest bij SOX-audits, zowel in de audit-rol als in de rol van adviseur. Zij heeft dit artikel op persoonlijke titel geschreven.

Niet alleen bedrijven zijn hier druk mee geweest, maar ook de accountant en IT auditors hebben de afgelopen jaren een uitdaging gehad aan het beoordelen van de management-activiteiten rondom EUC en het testen van EUC. Dit artikel beschrijft een pragmatische aanpak hoe om te gaan met EUC, zeker in relatie tot Audit Standaard No 5, die ook een pragmatische aanpak ondersteunt.

De onduidelijkheid over de aanpak van EUC in combinatie met SOx begint al bij de definitie van EUC en de bepaling van welke EUC in scope is voor SOx. Maar allereerst: wat is EUC nu eigenlijk? EUC heeft betrekking op applicaties en tools die door eindgebruikers zijn ontwikkeld en door eindgebruikers worden beheerd. Dit in tegenstelling tot applicaties en systemen waarvan de ontwikkeling en het beheer ligt bij professionele IT organisaties of IT afdelingen. Spreadsheets (bijvoorbeeld in MS Excel), databases (bijvoorbeeld in MS Access) maar ook reporting tools (zoals Business Objects en ACL) vallen binnen EUC.
Maar veel van de EUC die binnen organisaties wordt gebruikt in de bedrijfsvoering valt niet binnen de scope van SOx. Met andere woorden, niet alle EUC is relevant voor SOx. Dit kan komen door de significantie van het proces waarbinnen de EUC wordt gebruikt of de impact die het onbetrouwbaar functioneren van een EUC kan hebben op de financiële verslaglegging.
Dit betekent dat kritisch mag worden gekeken naar welke EUC er toe doet binnen de financiële verslaglegging. Dit moet voorkomen dat een lange lijst met spreadsheets, rapporten en databases aan de strenge SOx eisen moet voldoen zonder dat deze EUC invloed heeft op de financiële verslaglegging.
In dit artikel wordt met 'binnen de scope van SOx' bedoeld dat beheersmaatregelen om de betrouwbaarheid van de EUC te garanderen moeten worden geïmplementeerd en worden getest.

Binnen de scope van SOx

Welke EUC valt binnen de scope van SOx? Om vast te stellen welke EUC binnen de scope valt van SOx kan het stroomdiagram (figuur 1) ter ondersteuning worden gebruikt. Het diagram is gebaseerd op de praktijkervaring van de auteur uit zowel audit- als advieswerkzaamheden op EUC. Hoewel dit diagram als een hulpmiddel kan dienen



1. Maakt de EUC onderdeel uit van een voor SOx in-scope proces of is de EUC onderdeel van een control behorende tot een in-scope proces? Alleen die, door eindgebruikers beheerde, spreadsheets, rapporten en databases die tijdens de walkthrough zijn geïdentificeerd vallen binnen de scope van EUC (mits de walktrough juist en volledig is uitgevoerd).

2. Kan een fout in de EUC leiden tot een material misstatement in de finaciële verslaglegging?

3. Steunt management op een control elders in het proces die de betrouwbare werking van de EUC aantoont? In zulke gevallen zijn aanvullende EUC maatregelen niet nodig.

4. Wordt de EUC ingezet als tekstverwerker en worden verder geen bewerkingen op de inhoud uitgevoerd? In zulke gevallen zijn aanvullende EUC-maatregelen niet nodig.

5. Als de EUC voorafgaand aan het gebruik volledig moet worden opgebouwd, dan zijn manual controls noodzakelijk om de juistheid en volledigheid van de uitkomst vast te stellen. IT general controls zijn op deze sheets niet van toepassing.

Figuur 1 Stroomdiagram om vast te stellen welke EUC binnen de scope van SOx valt

blijft het altijd noodzakelijk om op basis van 'professional judgement' de selectie uit te voeren.

Voorbeelden

Binnen de scope:

- Een spreadsheet berekent maandelijks de afschrijvingen van vaste activa op basis van rekenregels. De uitkomsten worden geladen in het financiële systeem.
- Een spreadsheet berekent voorzieningen op basis van gegevens uit een factureringssysteem. De uitkomsten worden geladen in het financiële systeem.

Buiten de scope:

- Een spreadsheet valideert de afschrijvingen die door een financieel systeem zijn berekend door dezelfde berekeningen uit te voeren. Dit systeem valt niet binnen de scope van SOx omdat de uitkomst wordt vergeleken met de bron en daardoor worden eventuele onjuistheden of onvolledigheden zichtbaar.
- Een ouderdomsrapport dat wordt gegenereerd door een EUC maar altijd wordt aangesloten met uitstaande facturen wordt buiten de scope gelaten. De aansluiting moet dan wel binnen de scope van SOX vallen.

In 2004 heeft PriceWaterhouseCoopers een whitepaper opgesteld over het gebruik van spreadsheets in combinatie met SOx. In de praktijk blijkt dat veel organisaties hun EUC-richtlijnen hierop hebben gebaseerd. Kenmerkend voor de methode die wordt beschreven is de classificatie van spreadsheets op basis van toepassingsgebied, complexiteit en hoeveelheid gebruikers. Variatie hierin kan volgens het whitepaper leiden tot verschillende sets van maatregelen om toch de betrouwbare werking te garanderen. Om tot een toereikende set van maatregelen te komen is het niet persé noodzakelijk een dergelijke classificatie aan te brengen. Vanuit een SOx perspectief is dit ook niet verplicht (de classificatie die het PwC whitepaper adviseert zal overigens niet leiden tot onjuiste conclusies). Zodra is vastgesteld dat een

EUC binnen de scope van SOx valt, dan gelden eisen ten aanzien van beheersmaatregelen rondom de EUC om de betrouwbare werking te garanderen. Voor een complexe EUC met veel gebruikers zal het vaststellen van de juiste werking complexer zijn dan bij een eenvoudige EUC. Daarnaast zullen maatregelen voor logische toegangsbeveiliging uitgebreider zijn bij veel gebruikers dan bij een beperkte groep. Het vaststellen van de potentiële invloed op de 'financial statement' en de mogelijkheid op een 'material misstatement' is wel noodzakelijk, omdat alleen die controls bij een niet toereikende werking kunnen leiden tot een 'material misstatement'. En dit is met de komst van Audit Standaard no. 5 een belangrijk criterium geworden.

Maatregelen

Welke maatregelen moeten minimaal zijn ingericht? Als een organisatie gebruikt maakt van EUC dat binnen de scope van SOx valt, dan moet de organisatie beheersmaatregelen implementeren die zorgdragen voor een betrouwbare (juist en volledige) verwerking van gegevens. Hierbij zijn twee soorten te onderscheiden:

- maatregelen om de betrouwbare werking van de EUC vast te stellen;
- maatregelen die ervoor zorgen dat de werking van de EUC betrouwbaar blijft: IT General Controls.

De betrouwbare werking van de EUC

De eerste stap is vaststellen dat de EUC werkt zoals het is bedoeld. Hiervoor moeten alle scenario's worden doorlopen, waarbij de uitkomsten van deze reperformance moeten worden vergeleken met de uitkomst van de spreadsheet. Een voorbeeld hiervan is dat bij het afschrijven van vaste activa per mogelijke afschrijvingsmethode moet worden gevalideerd of datgene wat de EUC heeft berekend klopt. Een andere mogelijkheid om de betrouwbare werking van de EUC vast te stellen is een inspectie van de logica gebruikt in de EUC om na te gaan of onder alle omstandigheden de juiste uitkomst kan worden gegenereerd. Hierbij worden bijvoorbeeld de berekeningen in Excel nagekeken. Deze beoordeling moet alle mogelijke bewerkingen bevatten dus ook de mogelijkheid om te sorteren, samen te vatten en te rapporteren alsmede de input- en outputfunctie.
Het vaststellen van de juiste werking valt onder baselining. Iedere keer dat de EUC wordt gewijzigd dient het vaststellen van de betrouwbare werking tot de testprocedure te behoren.

Als de IT general controls rondom de EUC effectief zijn, dan zijn gedurende het jaar geen aanvullende testwerkzaamheden op de betrouwbare werking van de EUC noodzakelijk. Maar als de IT general controls niet effectief zijn, dan is het noodzakelijk om voorafgaand aan het gebruik van de EUC vast te stellen dat de EUC ongewijzigd is en dus nog steeds doet wat het moet doen. Omdat dit als het handmatig moet gebeuren een tijdrovende en foutgevoelige bezigheid is, is een geautomatiseerde controle aan te bevelen, bijvoorbeeld met behulp van een tool die de EUC vergelijkt met de laatste keer dat het is gebruikt en de afwijkingen rapporteert.

IT General Controls

Om ervoor te zorgen dat de werking van de EUC betrouwbaar blijft is het noodzakelijk de IT general controls in te richten. Dit artikel beschrijft een aantal logische maatregelen die verwacht mogen worden bij EUC en die voldoende borging zouden moeten geven voor een betrouwbare werking van de EUC.

• Toegangsbeveiliging

EUC-beleid en -richtlijnen voor logische toegangsbeveiliging zijn opgesteld, geïmplementeerd en effectief:

- toegang tot de EUC is ingericht op basis van een *need to know* en *need to use*-basis. Dit is formeel gedocumenteerd;
- de EUC is beveiligd met een sterk wachtwoord (conform de binnen de organisatie geldende wachtwoordinstellingen);
- cellen die logica bevatten worden bevroren voor de gebruikers.

• Change management

Beleid en richtlijnen over change management zijn opgesteld, geïmplementeerd en effectief voor EUC:

- wijzigingen worden gedocumenteerd en afgetekend door een andere persoon dan de persoon die de wijzigingen doorvoert;
- wijzigingen worden formeel getest om de betrouwbare werking van de EUC te garanderen;
- de mogelijkheid om wijzigingen door te voeren in de EUC is beperkt tot een gelimiteerde groep gebruikers.

Testen

Hoe moeten EUC en de controls rondom EUC voor SOx worden getest? De organisatie dient de betrouwbare werking van de EUC aan te tonen. Voor SOx moet het management van de organisatie, maar ook de externe accountant, vaststellen dat de organisatie hiervoor adequate maatregelen heeft ingericht en dat deze maatregelen over een bepaalde periode effectief zijn gebleken. Dit kan door de accountant op twee manieren worden vastgesteld door reperformance van de betrouwbaarheidscheck (zoals eerder beschreven) of inspectie van de betrouwbaarheidscheck. De keuze hangt af van professional judgement en zal afhankelijk zijn van de risico's die samenhangen met het gebruik van de desbetreffende EUC.

IT General Controls

De organisatie dient een stelsel van maatregelen te hebben geïmplementeerd dat zorg draagt voor een IT-omgeving waarin ongeautoriseerde wijzigen op de logica en de inhoud niet kunnen worden doorgevoerd. Om vast te stellen dat deze maatregelen hebben gewerkt moeten de IT general controls worden getest. Dit testen wijkt niet af van het testen van IT general controls voor applicaties en systemen die door een professionele IT afdeling worden beheerd.


BELEGGERS BELANGEN EN DELTA LLOYD PRESENTEREN
WIE BELEGT HET BESTE
HET MEEST REALISTISCHE BELEGGINGSSPEL VAN NEDERLAND
DOE MEE EN WIN EEN REIS NAAR WALL STREET
SPEEL HET SPEL OP WWW.BELEGGERSBELANGEN.NL
Beleggers Belangen
BRON VOOR ACTIEVE BELEGGERS
powered by delta lloyd

Audit Standaard nummer 5 en EUC

Met de invoering van Audit Standaard nummer 5 (AS5) [AS507] is SOx pragmatischer geworden. Dit geldt ook voor EUC, en wel op twee onderdelen:
'risk based approach' en 'using the work of others'.

Risk based approach

Het toepassen van een 'risk based approach' bij het selecteren van wat in scope is voor SOx is behandeld in de paragraaf 'Binnen de scope van SOx', waar wordt gekeken naar de financiële impact die een fout in de EUC kan hebben op de jaarrekening. Als een fout niet kan leiden tot een material misstatement dan vereist AS5 geen testwerk. Als voorbeeld dient back-up en recovery dat voorheen standaard onderdeel uit maakte van de IT general controls. Met de komst van AS5 is de keuze om back up en recovery maatregelen rondom de spreadheet binnen de scope van SOx mee te nemen minder voor de hand liggend omdat een probleem hiermee niet meteen zal leiden tot een materiele fout in de jaarrekening.

Using the work of others

De mate waarin de auditor kan steunen op het testwerk dat onder verantwoordelijkheid van management is uitgevoerd is enerzijds afhankelijk van de risico-inschatting van de control (bijvoorbeeld het inherente risico en de 'risk of failure') en anderzijds van de bekwaamheid en objectiviteit van degene die namens het management het testwerk heeft uitgevoerd. Het is de auditor toegestaan gebruik te maken van het testwerk van het management en daarop te steunen voor het eigen oordeel. De strikte regels die hiervoor voorheen golden zijn versoepeld en de auditor mag meer varen op professional judgement zolang de onderbouwing voor de wijze waarop de assurance wordt verkregen maar formeel word gedocumenteerd.

Conclusie

Een kritische blik op alle EUC en vervolgens bepalen welke EUC voor SOx in scope is, leidt tot minder lange lijsten met EUC. Het implementeren van een beperkt aantal adequate maatregelen zorgt voor een betrouwbare werking van de EUC, zonder dat het doel voorbij wordt geschoten. De mogelijkheden om bij het testen van EUC als auditor meer te steunen op de werkzaamheden van het management moeten er voor zorgen dat de werkzaamheden rondom EUC voor SOx minder arbeidsintensief wordt. Zo valt End User Computing toch best wel mee. ■

Referenties

[PWC04] The Use of Spreadsheets: Considerations for Section 404 of the Sarbanes-Oxley Act*, juli 2004

[AS507] Auditing Standard No. 5 – An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements, juni 2007

Compleet werkt beter

Elsevier FiscaalTotaal. Alle fiscale antwoorden op een rij.
Soms is het overduidelijk dat iets niet compleet is. Maar zo eenvoudig is het niet altijd voor fiscaal professionals. Kies daarom voor Elsevier FiscaalTotaal. Dan heeft u altijd alle fiscale informatie en actualiteiten snel, eenvoudig en gesorteerd op uw scherm. Vanuit één bron, één handige site. Met uw eigen aantekeningen. Dat bespaart u kostbare zoektijd. Bovendien weet u zeker dat u kwalitatief en compleet advies geeft. Ontdek het zelf op www.fiscaaltotaal.nl.

ELSEVIER
FiscaalTotaal *

Elsevier Fiscale Media Reed Business