De beoordeling van ICT in het kader van de jaarrekeningcontrole

Mw. drs. M.J.A. Koedijk RA

De controleaanpak van accountants gaat voort in zijn ontwikkeling en daarmee de inzet van de ICT-auditor in het kader van de jaarrekeningcontrole. De verdere ontwikkeling van de jaarrekeningcontroleaanpak is gebaseerd op de Business Measurement Process (BMP)-methodologie. De nadruk bij BMP ligt op de analyse van strategische bedrijfsrisico's en de daarvoor door het management getroffen beheersmaatregelen. Bij deze analyse worden tevens de risico's onderkend die voortkomen uit de inzet van informatie- en communicatietechnologie (ICT) en de beoordeling van de daartoe getroffen beheersmaatregelen (al dan niet in de ICT).

Inleiding

De inzet door bedrijven van ICT ter ondersteuning van de efficiënte en effectieve uitvoering van de bedrijfsprocessen is vanzelfsprekend. De processen, de getroffen beheersmaatregelen en ICT zijn hierbij verregaand geïntegreerd, hetgeen zeker geldt voor de financiële transactiestromen en de logistieke processen. Daarnaast is de inzet van ICT gegroeid naar een strategisch instrument van het management, waardoor tijdige en effectieve ICT-inzet een kritieke succesfactor is geworden voor het bereiken van de bedrijfsdoelstellingen.

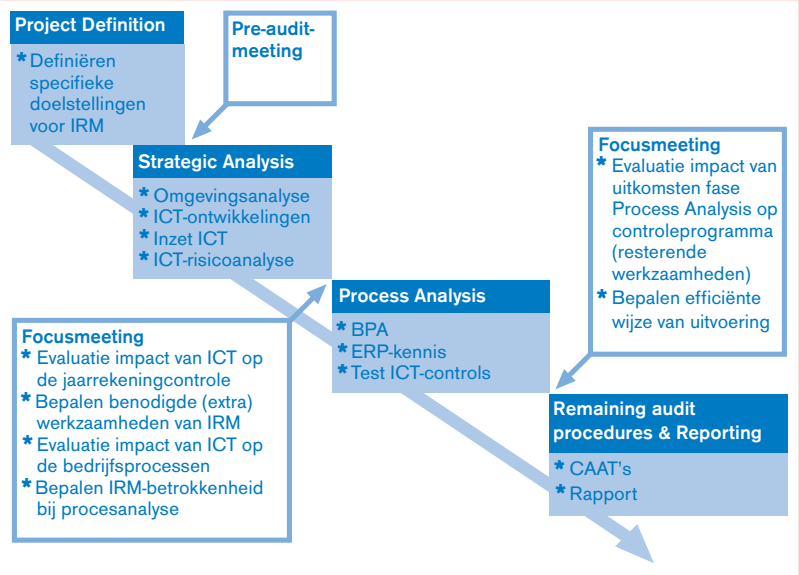
Bedrijfsrisico's en daaruit voortvloeiende accountantscontrolerisico's komen derhalve in toenemende mate voort uit (de inzet van) ICT. Bovendien worden deze risico's veelal beheerst door maatregelen in de ICT of in de ICT-organisatie. Door de snelheid van ontwikkelingen op het gebied van ICT, de complexiteit, de hoge investeringen, de omvangrijke projecten en de steeds verdergaande integratie van ICT met de bedrijfsprocessen, zal de accountant voor het identificeren van de ICT-risico's en de getroffen beheersmaatregelen de ICT-auditor inschakelen.

Ten behoeve van de ondersteuning van de accountant in het kader van de jaarrekeningcontrole zal de ICT-auditor invulling geven aan de ICT-aspecten in de verschillende fasen van de nieuwe controleaanpak. Deze op BMP[1] gebaseerde aanpak voor de controle van de jaarrekening kent de volgende fasen:

* Project Definition;
* Strategic Analysis;
* Process Analysis;
* Remaining audit procedures & Reporting.

In dit artikel zal per fase de (mogelijke) invulling van de inzet van de ICT-auditor worden uiteengezet. Uiteraard zal de daadwerkelijke inzet van de ICT-auditor per cliënt verschillen afhankelijk van (onder andere) de afhankelijkheid en complexiteit van de ICT. Ter illustratie zijn tevens enkele praktijkvoorbeelden opgenomen.

1) Voor een nadere toelichting bij de uitgangspunten van BMP wordt verwezen naar het artikel van Jonker in *Compact & ICT-auditing*, 25 jaar Compact, jubileumuitgave ([Jonk99]).



Figuur 1. Inzet ICT-auditor in de diverse fasen van de jaarrekeningcontrole.

Beoordeling van ICT in de diverse fasen van de jaarrekeningcontroleaanpak

Project Definition

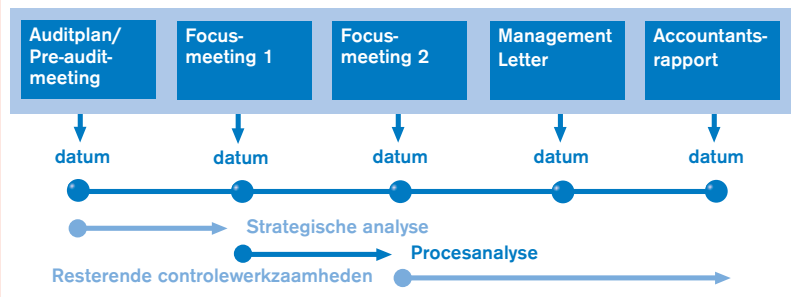
In de fase Project Definition wordt het auditplan opgesteld. De inhoud van dit auditplan bestaat onder andere uit:

* algemene cliëntinformatie;
* controleaanpak;
* clientserviceteam;
* planning;
* budget;
* inzet van experts (zoals de ICT-auditor);
* specifieke cliëntafspraken.

De accountant zal in overleg met de ICT-auditor de specifieke Information Risk Management (IRM)-projectdoelstellingen definiëren. De ICT-auditor legt deze afspraken vast in het ICT-auditplan, dat een onderdeel vormt van het auditplan van de accountant (zie ook het artikel over de samenwerking van de accountant en de ICT-auditor van Jonker en Van Langen ([Jonk00])). Belangrijk element van dit ICT-auditplan zijn de zogenaamde focusmeetings. Dergelijk overleg tussen de

accountant en de ICT-auditor vindt plaats na afronding van elke fase. Tijdens het overleg worden de bevindingen besproken en wordt vastgesteld welke inzet van de ICT-auditor in de volgende fase wordt verlangd. De concrete invulling van het ICT-auditplan vindt derhalve fasegewijs plaats (zie figuur 2), zodat de inzet van de ICT-auditor flexibel en op maat kan plaatsvinden.

In deze eerste fase van de controle zal een pre-auditmeeting plaatsvinden om de uitkomsten van de Project Definition aan alle teamleden te presenteren.



Figuur 2. Planning inzet van de ICT-auditor.

Strategic Analysis

Tijdens de strategische analyse worden de volgende activiteiten uitgevoerd:

* verkrijgen van inzicht in het bedrijf en de business, zoals de bedrijfsdoelstellingen en strategie, omgevingsfactoren en (technische) ontwikkelingen, de controleomgeving en de primaire en ondersteunende processen;
* identificeren van strategische bedrijfsrisico's;
* identificeren van de implicaties voor de financiële verslaglegging van de strategische bedrijfsrisico's en het identificeren van significante transactiestromen;
* selecteren van de relevante bedrijfsprocessen en het plannen van de procesanalyse.

Strategische bedrijfsrisico's

Tijdens de strategische analyse identificeert de accountant op basis van het verkregen inzicht de strategische bedrijfsrisico's, waarbij de volgende definitie van een strategisch bedrijfsrisico wordt gehanteerd: 'the threat that an event or action will adversely affect an entity's ability to achieve its business objectives and execute its strategies successfully'. De accountant zal vervolgens analyseren of deze strategische bedrijfsrisico's binnen een jaar een significante impact kunnen hebben op de jaarrekening(controle). Indien dit het geval is zal de accountant het proces waarin het risico door de onderneming wordt beheerst (of zou moeten beheersen), selecteren voor de procesanalyse.

De inzet van de ICT-auditor zal gericht zijn op het identificeren van de strategische ICT-risico's en de mate van beheersing daarvan door het management en de beoordeling van de impact (samen met de accountant) op de jaarrekeningcontrole (zie ook [Gils00]).

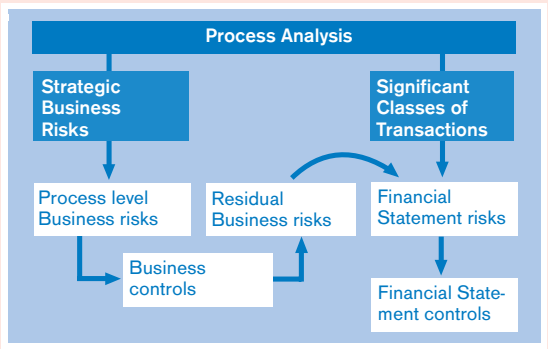
Ten behoeve van de identificatie van de strategische ICT-risico's zal de ICT-auditor allereerst inzicht moeten verkrijgen in de omgeving waarin het bedrijf opereert, de relevante (ICT)-ontwikkelingen en de externe krachten binnen de branche. Vervolgens zal worden kennisgenomen van de automatiseringsorganisatie, de configuratie en de diverse beleidsplannen, waarbij de aansluiting van de ICT-strategie op de bedrijfsstrategie zal worden vastgesteld. In deze strategische fase zal de ICT-auditor bovendien op basis van een aantal risicofactoren de ICT-component van de controleomgeving in kaart brengen. Deze factoren zijn bijvoorbeeld de afhankelijkheid van ICT, de mate van veranderingen in de ICT, het belang van en de aandacht voor informatiebeveiliging en de betrouwbaarheid, de kennis en vaardigheden van het personeel, en de afhankelijkheid van derden.

Op basis van de verzamelde informatie van de interne en externe omgeving en de risicofactoren zal de ICT-auditor de strategische ICT-risico's identificeren. Voorbeelden van strategische ICT-risico's die impact kunnen hebben op de jaarrekeningcontrole zijn het mislukken van een systeem(ERP-)implementatie en/of omvangrijke dataconversie, continuïteitsrisico's in verband met de afhankelijkheid van ICT en integriteitsrisico's als e-businessactiviteiten zijn of worden geïmplementeerd. De accountant zal tezamen met de ICT-auditor de strategische ICT-risico's beoordelen op significantie voor de jaarrekeningcontrole. Door deze gezamenlijke uitvoering kunnen beide professionals hun specifieke expertise inbrengen in het afwegingsproces.

Indien de impact op de jaarrekening significant is, zal ook voor de geïdentificeerde ICT-risico's het (sub)proces worden geselecteerd waarin het risico wordt beheerst, waaronder de (ITIL-)processen in de automatiseringsorganisatie.

Significante transactiestromen

Naast de processen waarin significante strategische bedrijfsrisico's worden beheerst, zal de accountant in het kader van de jaarrekeningcontrole significante transactiestromen selecteren voor de uitvoering van de procesanalyse. De definitie van significante transactiestromen is hierbij als volgt: 'a set of transactions having common features, properties or qualities that has a significant impact on the financial statements'. In de procesanalyse zullen deze significante transactiestromen (veelal routinematige processen) door de accountant worden beoordeeld met betrekking tot de beheersing van de jaarrekeningcontrolerisico's, terwijl bij de strategische bedrijfsrisico's tevens de 'business controls' worden beoordeeld (zie figuur 3).



Figuur 3. Selectie van processen en beoordeling van risico's.

Planning procesanalyse

De ICT-auditor zal de informatiesystemen in kaart brengen die de verschillende geselecteerde processen ondersteunen. Aan de hand van de bevindingen tijdens de strategische analyse en de zogenaamde 'trigger questions' (zie kader 1) zal de accountant overwegen welke inzet van de ICT-auditor wordt verlangd in de procesanalysefase. Deze afweging zal ter sprake komen in de focusmeeting en zal door de ICT-auditor worden vastgelegd in het ICT-auditplan.

Kader 1. Trigger questions

Triggers voor het inzetten van de ICT-auditor in de procesanalyse:

1. Is het bedrijfsproces sterk afhankelijk van ICT, bestaat een hoge graad van integratie en/of is sprake van een ERP-systeem?
2. Is het effectief inzetten van ICT een kritieke succesfactor?
3. Is sprake van e-business solutions/activiteiten?
4. Bestaan indicaties dat gebruikers onvoldoende zijn betrokken bij de ontwikkeling?
5. Bestaan indicaties dat er tijdens systeemontwikkeling geen aandacht is geweest voor kwaliteitsbewaking?
6. Bestaan indicaties dat er tijdens systeemontwikkeling geen aandacht is geweest voor beheersmaatregelen (AO/IC)?
7. Is informatiebeveiliging belangrijk uit het oogpunt van privacy en betrouwbaarheid?
8. Is er sprake van kritieke vaste gegevens?
9. Zijn management- en interne controles gebaseerd op (geautomatiseerde) standaardrapporten?

Voorbeeld. Strategisch bedrijfsrisico.

Bij een middelgrote verzekeraar bleek een duidelijke mismatch tussen de businessunits en de IT-unit. Signalering door de ICT-auditor droeg bij tot een tijdig onderkennen en aanpakken van de problemen en een hoge waardering door de klant. Het onderzoek duurde slechts enkele dagen en gaf tevens een goed beeld van het strategisch beleid van de organisatie.

In het kader van de strategische analyse nam de ICT-auditor kennis van het strategisch beleid van de klant. Met name werden het beleidsplan Leven en het beleidsplan Schade kritisch beoordeeld op het gebruik van ICT en in het bijzonder op de veranderingen die nodig waren om de beleidsplannen succesvol te maken. Daaruit bleek dat voor het realiseren van alle plannen in een bestek van drie jaar veel nieuwe systemen moesten worden ontwikkeld, zowel in de infrastructuur (zoals internetcommunicatie met klanten en tussenpersonen) als in informatiesystemen (zoals online acceptatieprogrammatuur). Meerdere keren stond in de beleidsplannen dat tijdige aanpassing van de ICT een kritieke succesfactor was; zonder tijdige aanpassing zou de bedrijfsvoering ernstig gevaar lopen, niet alleen intern, maar vooral ook in de concurrentiepositie met andere verzekeraars.

Vervolgens is met deze informatie het beleidsplan ICT bestudeerd. Hoewel de meeste ontwikkelingen die in de beleidsplannen van het leven- en schadebedrijf werden genoemd wel in het beleidsplan van de ICT-organisatie waren terug te vinden, bleek in het ICT-plan dat de vereiste capaciteit niet geleverd kon worden. Soms had dat te maken met de stand van de techniek of ontwikkelingen in de branche en vaak ook met de financiële, technische en personele capaciteit van de ICT-organisatie. In het plan was ieder project met enige voorbehouden vermeld en stond ergens verscholen dat niet alle projecten uitgevoerd konden worden en dat er zeker keuzen gemaakt moesten worden die ernstige gevolgen zouden hebben voor de andere projecten. Door het tamelijk zelfstandige optreden van de businessunits Leven en Schade en de vereiste marktconforme opstelling van de ICT-organisatie was de communicatie niet optimaal en sloten de plannen van de businessunits onvoldoende aan op die van de ICT-organisatie.

Door zo'n mismatch is het risico groot dat of systemen niet (tijdig) ontwikkeld worden, hetgeen tot omzetverlies of een verslechterde concurrentiepositie kan leiden, of dat systemen overhaast ontwikkeld en ingevoerd worden, hetgeen de betrouwbaarheid kan schaden.

(Met dank aan drs. H.G.Th. van Gils RE RA)

Process Analysis

In de procesanalyse moet inzicht worden verkregen in de geselecteerde processen, de bedrijfs- en/of jaarrekeningcontrolerisico's die voortvloeien uit deze processen en de beheersing van die risico's door het management.

In samenwerking met het controleteam zal de ICT-auditor de procesanalyses met behulp van de Business Process Analysis[2] (BPA)-methode uitvoeren. BPA kent de volgende fasering:

- inzicht verkrijgen in proces en ondersteunend informatiesysteem;
- risicoanalyse;
- identificeren beheersmaatregelen;
- bepalen restrisico.

De ICT-auditor zal zich bij de gezamenlijke uitvoering van de procesanalyse richten op de functionaliteiten van het ondersteunende informatiesysteem, de daarin getroffen geprogrammeerde controles en de inrichting van de autorisaties. Naast de beoordeling van de bedrijfsprocessen zal de ICT-auditor in deze fase ook zorg dragen voor de procesanalyse van de geselecteerde processen in de ICT-organisatie en daarmee voor de beoordeling van de relevante algemene computercontroles.

De beoordeling van de processen en de beheersmaatregelen zal allereerst plaatsvinden in opzet en bestaan. Samen met de ICT-auditor zal de accountant de uitkomsten beoordelen en de gevolgen voor de aanpak van de jaarrekeningcontrole bepalen. Indien de 'financial controls' van voldoende kwaliteit zijn, zal ten behoeve van het vaststellen van de werking een controleprogramma worden opgesteld en uitgevoerd.

2) Voor een uitgebreide beschrijving van BPA wordt verwezen naar het artikel 'Van systeem- beoordeling naar proces- beoordeling' ([Koed99]).

Wanneer de accountant wil steunen op geprogrammeerde controles, de (beheersing van de) inrichting van de autorisaties en/of (complexe) functionaliteit van het informatiesysteem zal de ICT-auditor worden gevraagd de werking hiervan vast te stellen. Veelal zal de ICT-auditor hiertoe de beheersmaatregelen in de ICT-organisatie (met name change management en security management) beoordelen.

Ter afsluiting van deze fase zullen op basis van alle bevindingen in de procesanalyse de resterende uit te voeren controles (cijferanalyses en detailcontroles) worden bepaald en vastgelegd in controleprogramma's.

Bij een beursgenoteerde beleggingsmaatschappij in vastgoed is ten behoeve van het vastgoedbeheer (waaronder de exploitatie van de gebouwen) een nieuw informatiesysteem in productie genomen. De implementatie van het vastgoedsysteem betekende een verregaande verandering van de processen (significante transactiestromen) en de beheersmaatregelen. In het kader van de jaarrekeningcontrole is een procesanalyse met behulp van BPA uitgevoerd.

Met behulp van interviews en het bestuderen van documentatie werd het proces (werden de processtappen) gekoppeld aan het vastgoedsysteem in kaart gebracht. Met als input de strategische analyse en de kennis van het proces en het systeem werd vervolgens een risicoanalyse uitgevoerd. De ICT-auditor en de accountants vervolgden het onderzoek met de inventarisatie van de beheersmaatregelen. Hierbij werd onderscheid gemaakt in de aangetroffen functiescheiding, geprogrammeerde controles, verslagen en analyses daarop en in gebruikerscontroles. Tot slot analyseerde de ICT-auditor samen met de accountant per processtap het zogenaamde restrisico. De vastlegging van de beoordeling vond plaats in een matrix. In deze BPA-matrix werden per processtap de geïdentificeerde risico's en eisen van interne controle vastgelegd, alsook de geïnventariseerde beheersmaatregelen en het restrisico.

De overallconclusie van het onderzoek was positief. Wel werden enkele gemiddelde restrisico's vastgesteld ten aanzien van het beheer van de autorisaties en de acceptatie van facturen inzake onderhoudswerkzaamheden. Met behulp van de BPA-matrix kon de accountant eenvoudig zijn controleprogramma opstellen, waarbij de accountant zijn systeemgerichte aanpak kon handhaven met extra aandacht voor de geconstateerde zwakkere plekken. De ICT-auditor werd verzocht om in het kader van de jaarrekeningcontrole de algemene computercontroles te beoordelen om de continue betrouwbare werking van de applicatie te beoordelen. De klant heeft met behulp van het rapport zijn processen en het vastgoedsysteem geoptimaliseerd. Tevens is op basis van het positieve rapport besloten het vastgoedsysteem als standaardpakket op de markt te gaan brengen.

Voorbeeld. Procesanalyse ([Koed00]).

Remaining audit procedures & Reporting

In de laatste fase worden de resterende controlewerkzaamheden uitgevoerd, waarna de controleverschillen en bevindingen worden geïdentificeerd en geëvalueerd. De ICT-auditor kan de accountant in deze fase ondersteunen bij bestandsonderzoeken en cijferanalyses (met behulp van CAAT's). Deze inzet is in de focusmeeting na de procesanalyse bepaald.

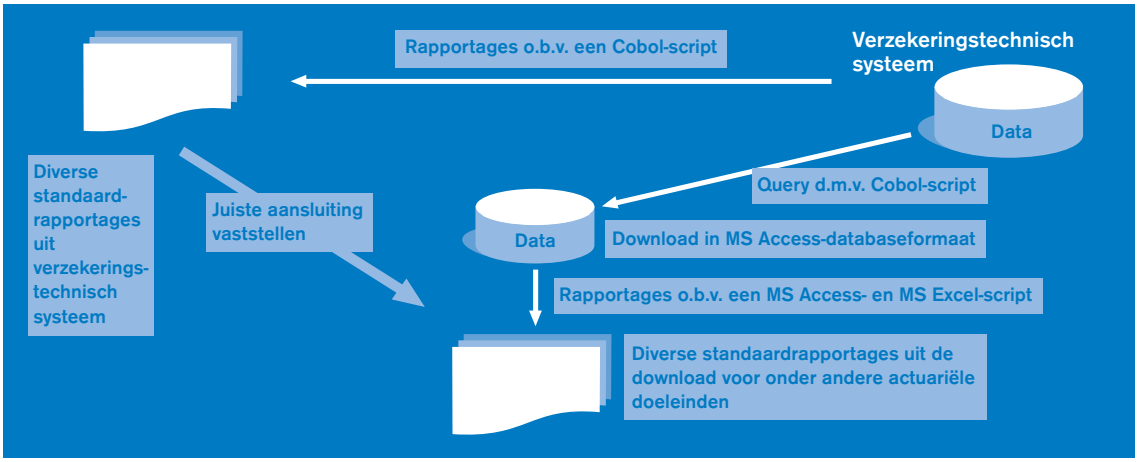
Als alle bevindingen bekend zijn, zal de accountant zijn oordeel vormen. De ICT-auditor kan hierbij worden gevraagd om de impact van zijn bevindingen toe te lichten. De accountant zal zijn bevindingen en aanbevelingen aan het management rapporteren, waaronder de bevindingen van de ICT-auditor. Bij omvangrijke onderzoeken door de ICT-auditor wordt echter meestal gekozen voor een afzonderlijk rapport.

Een verzekeraar maakt deel uit van een groot internationaal verzekeringsconcern. Aan het begin van het nieuwe jaar werd door de klant de actuariële voorziening berekend ten behoeve van de jaarrekening. Deze voorziening wordt voor een groot deel bepaald door de samenstelling van de deelnemersadministratie op een zeker moment. Aangezien bij de accountant onzekerheden waren blijven bestaan over de juistheid en de volledigheid van deze voorziening, mede omdat deze voorziening met behulp van een aantal queries uit de bestanden van het verzekeringstechnisch systeem was gegenereerd, besloot hij een ICT-auditor in te schakelen.

De ICT-auditor stelde vast dat behalve van de standaardrapportages uit het verzekeringstechnisch systeem door de eindgebruiker (actuaris) gebruik werd gemaakt van zelf gedefinieerde rapportages met behulp van Access- en Excel-scripts. De benodigde gegevens werden met behulp van een query uit het systeem gedownload. De eindgebruiker had hiertoe besloten omdat hij geen vertrouwen had in de standaardrapportages, die dan ook afweken van de rapportages die de eindgebruiker zelf had samengesteld (zie figuur 4).

Als gevolg van het onderzoek naar de totstandkoming van de standaardrapportage (programmaregels) en de wijze waarop de query van het actuariaat was opgebouwd, kwam de ICT-auditor tot de volgende bevindingen:

* De standaardrapportage gaf de stand per 30 juni, de query per 1 juli.
* De query toetste alleen op het veld royementsdatum en niet ook op het veld beëindigingsdatum van een polis, waardoor te veel polissen en dus deelnemers werden geteld.
* Een bepaalde aanvulling op een standaardverzekering werd door de query dubbel geteld (zodat een aantal verzekerden twee keer werd geteld).
* Een tweetal kolommen op de standaardrapportages gaf de verkeerde aantallen weer, doordat ook deelnemers van andere verzekeringen werden meegenomen.



Figuur 4. De totstandkoming van rapportages ten behoeve van het opstellen van de voorziening.

Voorbeeld. Best practice: Remaining audit procedures (queries).

Zowel de standaardrapportage als de query bevatte fouten. Door een door de ICT-auditor uitgevoerde herberekening van de deelnemersadministratie bleek dat de getroffen voorziening in de jaarrekening te hoog was. Door de werkzaamheden van de ICT-auditor kon worden voorkomen dat de jaarrekening een materiële fout bevatte, zowel in de voorziening als in de verlies- en winstrekening.

(Met dank aan drs. A.R.J. Basten)

Resultaat

De betrokkenheid van de ICT-auditor bij de jaarrekeningcontrole moet leiden tot een beter inzicht in de ICT-risico's en de beheersing daarvan door het management.

Dit inzicht wordt door de ICT-auditor en de accountant samen zo concreet mogelijk vertaald in de gevolgen voor de jaarrekeningcontrole. De accountant kent hierdoor zijn accountantscontrolerisico's die voortkomen uit de inzet van ICT en kan zijn controlewerkzaamheden hierop afstemmen, wat zal leiden tot hogere controlezekerheid. Indien sprake is van een sterke ICT-controleomgeving zal het inzicht in de (ICT-)beheersmaatregelen bovendien kunnen leiden tot een efficiëntere controleaanpak.

De inzet van de ICT-auditor in het kader van de jaarrekeningcontrole wordt gaandeweg het controleproces bepaald. Na elke fase wordt geanalyseerd of verdere inzet noodzakelijk dan wel efficiënt is, zodat zoveel mogelijk wordt gerealiseerd dat de door de ICT-auditor uit te voeren werkzaamheden helder en concreet worden gedefinieerd en tevens toegevoegde waarde opleveren voor de accountant. De ICT-auditor zal niet standaard de algemene computercontroles beoordelen, maar alleen als dat op basis van de strategische analyse of op basis van de beoordeling van de beheersmaatregelen in de processen noodzakelijk wordt geacht. De daadwerkelijke inzet van de ICT-auditor zal per cliënt verschillen en is afhankelijk van de strategische ICT-risico's en de wijze en complexiteit van de ondersteuning van de processen door informatiesystemen. Minimaal zal de ICT-auditor echter betrokken moeten zijn bij de strategische analyse om bovenstaande factoren te analyseren.

De inzet van de ICT-auditor leidt bovendien tot bevindingen en aanbevelingen op een gebied waarin de klant in het algemeen veel investeert, maar dat nog vaak een relatief onbekend terrein is. Dit betekent dat onderzoeken op het gebied van ICT veel toegevoegde waarde voor de klant kunnen opleveren.

Mw. drs. M.J.A. Koedijk RA is werkzaam als seniormanager bij KPMG Information Risk Management. Zij is verantwoordelijk voor de implementatie van de werkzaamheden van de ICT-auditor in de nieuwe controleaanpak van KPMG (Information Risk Management in KPMG Audit). Haar werkterrein beslaat naast werkzaamheden ter ondersteuning van de jaarrekeningcontrole voornamelijk proces- en systeembeoordelingen van zowel ERP-pakketten als maatwerksystemen. Zij is verantwoordelijk voor de ontwikkeling van methoden, producten en trainingen op beide werkterreinen en treedt op als docent van interne en externe cursussen.

Literatuur

[Gils00]
Drs. H.G.Th. van Gils RE RA, *IRM in de strategiefase van de jaarrekeningcontrole*, Compact 2000/2.

[Jonk99]
R.A Jonker RE RA, *Information risk management en audit 2000*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[Jonk00]
R.A. Jonker RE RA en drs. R.J.M. van Langen RA, *Samenwerking financial auditor en EDP-auditor*, Compact 2000/2.

[Koed99]
Mw. drs. M.J.A. Koedijk RA, *Van systeembeoordeling naar procesbeoordeling*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[Koed00]
Mw. drs. M.J.A. Koedijk RA, *Business Process Analysis en de jaarrekeningcontrole; een praktijkcasus*, Compact 2000/2.

[KPMG00]
KPMG Audit Manual

[Meul00]
Drs. ing. A.M. Meuldijk, *De rol van de accountant in ERP-implementatieprojecten*, Compact 2000/2.