IRM in de strategiefase van de jaarrekeningcontrole

Drs. H.G.Th. van Gils RE RA

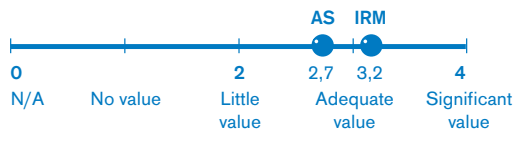
In dit artikel wordt ingegaan op de ondersteuning van de IRM-auditor (Information Risk Management) op het jaarrekeningcontroleproces van de accountant. Al jarenlang is zowel uit theoretisch als uit praktisch oogpunt sprake van een moeizame samenwerking. Door wijzigingen in het controleproces, binnen KPMG Business Measurement Process (BMP) genaamd, zijn er nieuwe mogelijkheden om de relatie kritisch te beschouwen en na te gaan waar verbeteringen mogelijk zijn. Met name de betekenis van IRM in de eerste fase van BMP, de strategiefase, is nog weinig belicht geweest. Vandaar dat in dit artikel vooral wordt stilgestaan bij deze strategiefase.

Accountancy en IT-auditing

Accountantscontrole en IT-auditing zijn al vanaf het begin van het computertijdperk met elkaar verbonden. IT-auditing is zelfs uit de accountancy ontstaan. Maar ook vanaf het begin is er sprake van afzonderlijke groepen accountants en IT-auditors en van een begripskloof tussen beide groepen. Toen de auteur van dit artikel in dienst trad van de gespecialiseerde Computer Audit Sectie van een accountantskantoor was de kloof nog klein: alle medewerkers waren primair accountant en secundair IT-auditor. En de taak voor de IT-auditors was duidelijk: hoofdzakelijk uitvoeren van bestandsonderzoeken met auditsoftware (ter ondersteuning van cijfermatige controles) en in mindere mate het uitvoeren van systeemonderzoeken. Dit laatste kwam een beetje opzetten in het kader van de analytische controle, maar men worstelde nog (net als nu) met wat je precies met de resultaten kon doen. Toen voor de IT-auditors duidelijk werd dat de kwaliteit van informatiesystemen mede was gebaseerd op de kwaliteit van de general IT controls en het derhalve noodzakelijk was daarin inzicht te verwerven, werd de kloof echt geschapen. Voor accountants staat dit type controls ver van de dagelijkse werkzaamheden af. De accountant blijkt moeite te hebben de invloed van de IT op de controleactiviteiten te doorgronden, terwijl de IT-auditor moeite heeft zijn bevindingen concreet naar de jaarrekeningcontrole te vertalen. Het is tenslotte niet eenvoudig om vast te stellen hoe veel meer (cijfer)controles uitgevoerd moeten worden als de IT-auditor na deskundig onderzoek tot de conclusie komt dat de 'change-managementprocedures niet geheel aan de redelijkerwijs te stellen eisen voldoen'. Helaas heeft dat soms geleid tot het afglijden naar de situatie dat de IT-auditor als vanzelfsprekend betrokken is bij de jaarrekeningcontrole, maar zijn inbreng terugvindt als onderdeel van de management letter. Van verdere integratie is dan geen sprake.

Naast het theoretische vraagstuk zijn er ook allerlei praktische belemmeringen voor een goede integratie. Eén van de barrières daarbij is de kennis die accountant en IT-auditor van het 'grijze gebied' moeten hebben om met elkaar te kunnen communiceren. Dit probleem zal zich mogelijk verergeren omdat steeds meer mensen worden opgeleid in accountancy óf IT-auditing. Een opleiding op beide gebieden komt steeds minder voor door het lange opleidingstraject dat daarvoor nodig is. Het vakgebied IT-audit is zich meer en meer zelfstandig gaan ontwikkelen met als gevolg dat de vroegere hechte relatie met accountancyvakken minder wordt. En vanuit mijn ervaringen in de accountantsopleiding merk ik dat accountancystudenten zich wel realiseren dat IT-kennis belangrijk is voor de accountant, maar dat anderzijds weinig studenten echt geïnteresseerd zijn in dat deel van de theorie. Ook de opleidingen zelf worstelen nog met de aard en diepgang van de IT-stof binnen de accountantsopleiding. Zie daarvoor het proefschrift van dr. R.G.A. Fijneman ([Fijn99]).

Nederland staat niet op zichzelf bij het zoeken naar de juiste wijze van integratie van IT-auditingactiviteiten in de accountantscontrole. In de Verenigde Staten is in 1998 binnen KPMG een onderzoek gedaan naar de samenwerking tussen accountants en IT-auditors bij een driehonderdtal opdrachten waarbij 103 auditpartners en 32 IRM-professionals hebben meegedaan. Het onderzoek is overigens uitgevoerd door een extern bureau. De aanpak betrof eerst een enquête, gevolgd door een (kleinere) discussiegroep met een beperkt aantal audit- en IRM-partners en -managers. Duidelijk bleek dat de respondenten moeite hadden met 'objectieve' oorzaken aan te geven voor een niet goede integratie van de twee disciplines bij hun klanten. De eigen perceptie wordt als realiteit ervaren, waarbij alleen onderwerpen die men in de eigen positie belangrijk acht, worden beklemtoond en andere juist niet. Duidelijk was ook het gevoel dat de integratie vooral 'van de andere partij' moest komen. Dat de IRM-professionals de eigen bijdrage hoger inschatten dan de auditpartners blijkt uit figuur 1.



Figuur 1. Bijdrage van IRM in het kader van de jaarrekening-controle.

Uit het onderzoek blijkt dat er wel veel overeenstemming bestaat over de meest en minst waardevolle activiteiten van IT-auditing in het kader van de jaarrekeningcontrole. In tabel 1 zijn de meest en minst waardevolle IRM-activiteiten samengevat. Daaruit kan geconcludeerd worden dat vooral behoefte bestaat aan het onderkennen van de impact van technologische vernieuwingen en het vaststellen van risico's voor de organisatie op het strategisch niveau.

IRM activities with greatest value	IRM activities with least value
* Assessing impact of technology advances	* Performing CAATs and tests of general IT controls
* Focusing on strategic level risks	* Providing tools to audit team
* Educating audit partner and team	* Using standard set of procedures
* Spending time with client	

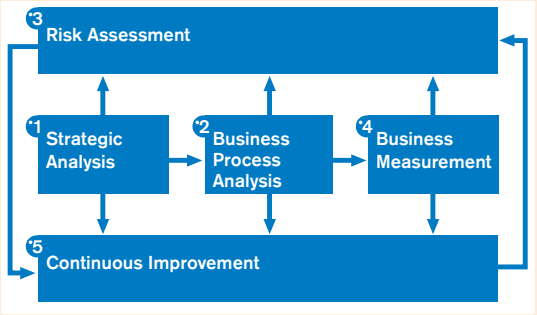
Tabel 1. Overzicht van meest en minst gewaardeerde IRM-activiteiten in het kader van de jaarrekening-controle.

Plezierig is de vaststelling dat verbijzonderde IT-audit wel nodig werd geacht door de accountant. Vandaar dat het geven van tools en standaardvragenlijsten minder werd gewaardeerd; het is effectiever dat de IT-auditor zelf de goede vragen stelt en de antwoorden direct kan evalueren.

Het onderzoeken van de general IT controls blijkt in het Amerikaanse onderzoek niet meer hoog op het verlanglijstje van de accountant te staan. Het is duidelijk dat hoe groter de impact van ICT op de bedrijfsprocessen is, hoe moeilijker het wordt om 'around the computer' te controleren of in belangrijke mate op gebruikerscontroles te steunen. Hier wordt volstaan met de verwijzing naar de discussie die eerder in Compact heeft gestaan omtrent de toegevoegde waarde van het toetsen van de werking van de general IT controls ([Boer98], [Kort98] en [Blok98]).

BMP: Business Measurement Process

De huidige controleaanpakken zijn gebaseerd op risicoanalyse. Op grond van de risico-inschatting wordt bepaald of en zo ja, met welke diepgang controleactiviteiten worden verricht. Als voorbeeld geldt de aanpak Business Measurement Process van KPMG. In figuur 2 zijn de belangrijkste stappen aangegeven.



Figuur 2. Stappen in het Business Measurement Process.

In de strategiefase (Strategic Analysis) wordt achtergrondinformatie van de klant bestudeerd en wordt onderzocht wat de bedrijfsdoelstellingen zijn en welke strategie wordt gevolgd om die doelstellingen te bereiken.

Juist dit onderdeel van de controleaanpak staat de laatste jaren steeds meer in de belangstelling. Door het onderkennen van de belangrijkste bedrijfsrisico's kan beter worden ingespeeld op de consequenties voor de controle. Ook uit tabel 1 blijkt dat met name deze fase het meest in de belangstelling staat. In de volgende paragraaf zal specifiek op de strategiefase verder worden ingegaan.

De tweede fase betreft de Business Process Analysis. In deze fase wordt er ingezoomd op de belangrijkste bedrijfsprocessen en wordt nagegaan welke inherente en internecontrolerisico's voor dat bedrijfsproces van toepassing zijn. Voor de bijdrage van de IT-auditor in dit proces wordt verwezen naar de uitgebreide beschrijving van de methodiek Business Process Analysis ([Koed99]), waarin duidelijk de evolutie wordt aangetoond van de eerder gangbare geïsoleerde systeembeoordeling naar de huidige procesbeoordeling.

Vanuit de risicoanalyses die door de accountant in de vorige twee fasen zijn uitgevoerd, zal de accountant nu nagaan op welke wijze het management van de klant maatregelen heeft getroffen om de risico's tot aanvaardbaar niveau terug te brengen.

Op grond van de aard en omvang van deze risico's en de getroffen beheersmaatregelen wordt het restrisico ingeschat, dat met name wordt betrokken bij het bepalen van de uit te voeren controlewerkzaamheden door de accountant. Door het uitvoeren van de vierde fase, Business Measurement, toetst de accountant de verwachtingen die in de voorgaande fasen zijn opgebouwd aan het feitelijke bedrijfsgebeuren.

De laatste fase is bedoeld om de klant voortdurend adviezen ter verbetering te geven aan de hand van bevindingen die tijdens de vorige stappen zijn opgedaan.

Voor een nadere beschrijving van deze BMP-controleaanpak wordt verwezen naar [Jonk99], waarin dieper op iedere fase wordt ingegaan en waarbij diverse ondersteunende IRM-tools zijn belicht.

Strategische analyse

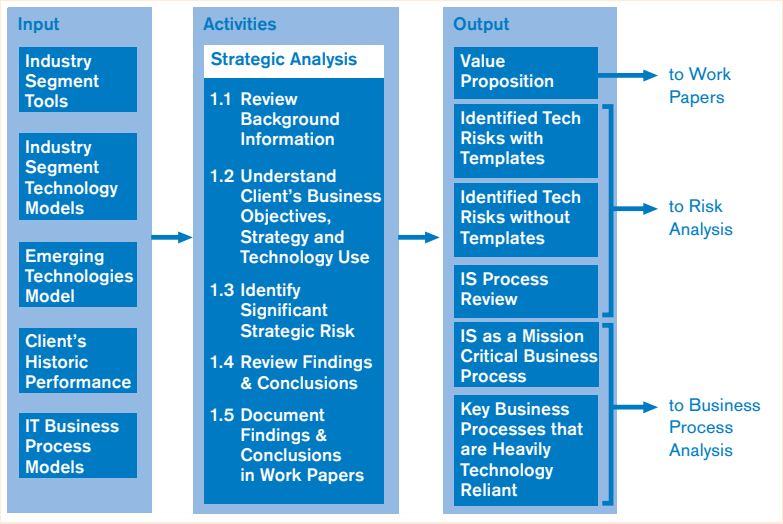
De strategische analyse kent een gefaseerde aanpak volgens figuur 3.

Binnen de BMP-gedachte gaat het er in eerste instantie om het 'klantrisico' in te schatten. Dit brengt goed naar voren dat het niet alleen om risico's gaat die direct betrekking hebben op de financiële posten, maar ook om andere risico's die op den duur de audit kunnen beïnvloeden. Vanuit het aandachtsgebied van dit artikel is één van die risico's het technologierisico. Hiermee worden de risico's bedoeld die samenhangen met het gebruik van informatietechnologie door de organisatie. Het is voor de IT-auditor verleidelijk om bij het onderzoeken van het technologierisico allerlei paden te betreden, die mogelijk minder relevant zijn voor de jaarrekeningcontrole, maar voor de organisatie van belang kunnen zijn bij de verdere bedrijfsvoering. Een bewuste afweging of van het hoofdpad kan worden afgeweken en de mate waarin dient vooraf met de accountant en de klant te worden vastgesteld om niet achteraf met budgettaire problemen te komen zitten!

Illustratief was een onderzoek bij een middelgrote verzekeraar in Nederland, waarbij de IT-auditor in het kader van de strategische analyse kennis nam van het strategisch beleid van de klant en met name het beleidsplan Leven en het beleidsplan Schade kritisch beoordeelde op het gebruik van IT en vooral ook op de veranderingen in de ICT die nodig waren om de beleidsplannen succesvol te maken. Daaruit bleek (natuurlijk) dat voor het realiseren van alle plannen in een bestek van drie jaar veel nieuwe systemen moesten worden ontwikkeld, zowel in de infrastructuur (zoals Internet-communicatie met klanten en tussenpersonen) als in informatiesystemen (zoals on-line-acceptatieprogrammatuur). Meerdere keren stond in de beleidsplannen dat tijdige aanpassing van de IT een kritische succesfactor was; zonder tijdige aanpassing zou de bedrijfsvoering ernstig gevaar lopen, niet alleen intern, maar met name ook in de concurrentiepositie met andere verzekeraars.

Vervolgens is met deze informatie het beleidsplan IT bestudeerd. Hoewel de meeste ontwikkelingen vermeld in de beleidsplannen van het leven- en schadebedrijf wel in het beleidsplan van de IT-organisatie waren terug te vinden, bleek in het IT-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 IT-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 zelfstandig optreden van de businessunits Leven en Schade en de vereiste marktconforme opstelling van de IT-organisatie was de communicatie niet optimaal en sloten de plannen van de businessunits onvoldoende aan op die van de IT-organisatie.

Kader 1. Casus.

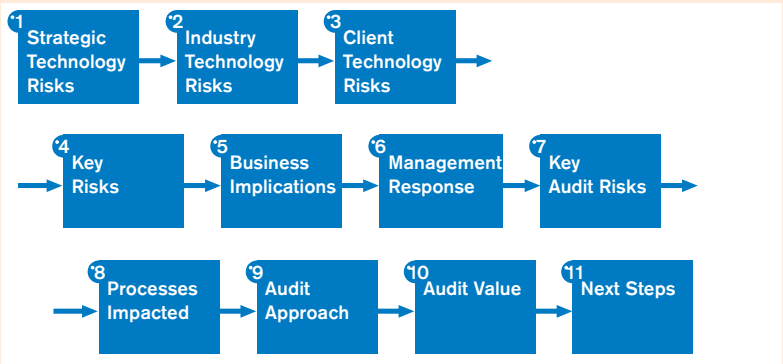


Figuur 3. Overzicht activiteiten van de strategische analyse.

Mede aan de hand van dit voorbeeld is duidelijk dat het technologierisico samenhangt met het auditrisico. Door de zware wissel die vanuit de businessunits op de IT-organisatie wordt getrokken, inclusief de noodzaak om op korte termijn nieuwe technologieën in te zetten, is de kans groot dat de kwaliteit van de systemen (en administratieve organisatie) onvoldoende zal zijn, hetgeen een directe invloed kan hebben op het inherente en interne-controlerisico in de accountantscontrole. In figuur 4 (overgenomen van [Tayl98]) is dat stapsgewijs in kaart gebracht. Hoewel hier steeds afzonderlijke stappen zijn getekend, is het meer een conceptueel framework, dat in de praktijk veelal als één samenhangend proces zal worden uitgevoerd.

Het technologierisico kan van verschillende kanten worden benaderd. Ten eerste vanuit de algemene IT-trends die zich in de maatschappij voordoen. Zeker op dit moment met alle e-ontwikkelingen. Vanuit deze algemene IT-trends kan de IT-auditor zich een voorstelling maken wat de impact kan zijn voor de klant dan wel hoe de klant gereageerd heeft op deze trends.

Binnen een specifieke branche spelen IT-trends vaak een directere rol op het punt van bedrijfsstrategie. Zeker de laatste paar jaar proberen ondernemingen juist op het IT-terrein voorop te lopen ten opzichte van branchegenoten waar het gaat om de inzet van technologische mid-



Figuur 4. Technology Risk Process map ([Tayl98]).

delen en staan de kranten bol van aankondigingen van grote investeringen op het gebied van wat zo fraai de emerging & enabling technologies heet. Aankondigingen van de ene organisatie leiden tot snelle besluitvorming bij andere organisaties in de branche, ook al haast het management zich om weer te geven dat een grote investeringsbeslissing niet is ingegeven door een besluit van een branchegenoot. Voor de controleaanpak is het dan van belang tijdig na te gaan wat de impact op de bedrijfsprocessen kan zijn en op welke wijze het management de relevante risico's beheerst.

Technologierisico's kunnen derhalve voortkomen uit het omarmen van nieuwe IT-ontwikkelingen, maar ook juist door dat niet te doen als branchegenoten het wel doen. Daarbij speelt natuurlijk ook de kennis en ervaring van de organisatie die de nieuwe IT-ontwikkelingen moet implementeren, alsmede de cultuur van de organisatie om met die veranderingen om te gaan. De auteur is betrokken geweest bij een evaluatie van een IT-project waarbij bleek dat door de IT-organisatie weliswaar een goed (modern) systeem was ontwikkeld, maar geen rekening was gehouden met het (beperkte) aanpassingsvermogen van de gebruikersafdeling, die al vele jaren op dezelfde wijze werkte en niet in staat bleek zich snel aan te passen. Er werden weer eigen registraties bijgehouden en velden in de database werden misbruikt voor andere doelen. Dat dit een grote impact had op de integriteit van de gegevens en de controleerbaarheid van het proces spreekt voor zich. Dergelijke signalen komen in het algemeen ook uit onderzoeken, zoals de Business Process Analysis (BPA)-methode van KPMG.

Meer dan in het verleden moet de IT-auditor beginnen bij het begin, namelijk in de strategiefase van het auditproces.

Een ander voorbeeld van klantspecifieke invloeden op het technologierisico betreft een organisatie die besloot de computerverwerking aan een externe organisatie in het buitenland over te dragen (outsourcing). Pas later ontdekte het management twee gevolgen, die wellicht de keuze voor outsourcing in een ander daglicht hadden gesteld en ook zeker gevolgen hadden voor de audit. Het uitbesteden was primair ingegeven door mogelijke besparingen op de kosten. Echter, na enige tijd bleken de kosten aanzienlijk hoger te zijn. Pas toen kwam goed naar voren dat de organisatie veelvuldig gebruikmaakte van allerlei queries, die een flinke belasting voor het computersysteem betekenden en waarvan de kosten dan ook werden doorbelast. De beoogde schaalvoordelen gingen dus niet echt op. Een forse, soms ongemotiveerde sanering van overzichten werd daarom doorgevoerd. Ook overzichten die vooral uit controleoogpunt relevant waren, kwamen opeens niet meer beschikbaar. Een tweede gevolg was dat voor 'kleinere' toepassingen afzonderlijke systemen werden binnengehaald. Dat was veel eenvoudiger dan applicaties voor het mainframe van de outsourcepartij te laten ontwikkelen. Maar wat als kleine toepassingen begon groeide uit tot grote toepassingen en binnen enkele jaren stonden er op allerlei afdelingen midrangecomputers van verschillende merken en met verschillende besturingssystemen (Windows, verschillende Unix-varianten en een AS400). Het systeembeheer was nauwelijks professioneel opgezet en de informatiesystemen niet geïntegreerd. Hoewel er op het mainframe een applicatie aanwezig was voor relatiebeheer, waren er binnen de lokale applicaties meerdere klantenbestanden aanwezig. Kortom, een flink risico voor de betrouwbaarheid van de informatievoorziening. Eén van de negatieve gevolgen voor de accountant was bijvoorbeeld dat de waardering van debiteuren aanzienlijk werd bemoeilijkt ten opzichte van vorige jaren, omdat de informatie verspreid was door de organisatie.

Hulpmiddelen voor het onderzoek van de technologierisico's

Voor het onderzoek van de risico's die vanuit de technologie voortkomen zijn er, zoals eerder is aangegeven, drie bronnen, namelijk vanuit de maatschappelijke ontwikkelingen, de brancheontwikkelingen en krachten die binnen de organisatie spelen. Om dit type risico's goed te kunnen onderkennen is natuurlijk kennis van markt, branche en organisatie vereist.

Binnen KPMG zijn Technology Issues per branche beschikbaar. Dit zijn korte documenten waarin per branche de relevante businesstrends zijn weergegeven. Vervolgens is daarbij per trendbeschrijving aangegeven wat daarbij de technologytrend is en wat daarbij de issues en de risico's zijn. Hoewel dit geen zeer gedetailleerde beschrijvingen zijn geven zij een goed beeld van de trends en risico's en ondersteunen zij de communicatie tussen de accountant en de IT-auditor, en desgewenst ook met de klant.

Voor het onderkennen van de impact van nieuwe technologieën en de daarmee samenhangende risico's zijn binnen KPMG zogenaamde Risk Analysis Modules (RAM's) ontwikkeld. Dat zijn verschillende programma's die rond een thema zijn opgezet. Zo bestaan er RAM's voor ERP-systemen, Secure E-Commerce, Information Security, Internet Banking, Business Continuity, Privacy, etc. Deze programma's zijn specifiek gemaakt voor de strategische-analysefase binnen BMP en zijn niet bedoeld als marketingtool voor andere IT-producten. Het uitvoeren van deze (beperkte) programma's heeft mede als doel om met name de controlerend accountant duidelijk te maken wat de gevolgen van bepaalde technologieën zijn op de business risk van de klant, waardoor de controlerend accountant beter in staat is de gevolgen voor de controlewerkzaamheden te overzien.

Conclusie

Al jaren is er sprake van een moeizame communicatie tussen de accountant en IT-auditor met betrekking tot de aard en omvang van de werkzaamheden van de IT-auditor. De laatste jaren is de accountant binnen de controleaanpak duidelijk meer aandacht gaan besteden aan huidige bedrijfs- en procesrisico's die vroeg of laat tot risico's in de jaarrekeningcontrole zullen leiden. Dit biedt goede kansen voor accountant en IT-auditor om nader tot elkaar te komen, aangezien veel bedrijfs- en procesrisico's een basis hebben in de risico's in de IT.

Duidelijk is geworden dat de IT-auditor niet primair met gedetailleerde general IT controls-vragenlijsten hoeft te komen, omdat dan de relatie met de bedrijfsprocessen en de impact van eventuele tekortkomingen onvoldoende gewogen kunnen worden. Wel moet een programma worden opgesteld dat de communicatie tussen IT-auditor, accountant en klant versterkt, zodat begrip ontstaat voor de gevolgen van IT-ontwikkelingen op de klantorganisatie en vervolgens op het controleprogramma van de accountant. Meer dan in het verleden moet de IT-auditor beginnen bij het begin, namelijk in de strategiefase van het auditproces. Door de betrokkenheid in deze fase komt de IT-auditor los van technische details en is hij daardoor een betere gesprekspartner voor de controlerend accountant en het management van de klant. Vanuit die positie is vervolgens op grond van de onderkende risico's een beter begrip van de impact van ICT op de bedrijfsprocessen aanwezig en is zowel de accountant als de IT-auditor beter in staat vast te stellen op welke gebieden een onderzoek naar het beheer van de achterliggende systemen gewenst is.

Dit vereist wel dat de IT-auditor ook daadwerkelijk gesprekspartner is op strategisch niveau en in staat is de issues helder aan zijn beide klanten, de controlerend accountant en het management van de te controleren organisatie, over te brengen. Ook vereist het van de accountant dat hij voldoende inzicht heeft in de gevolgen van ICT op de bedrijfsvoering van zijn klanten. En met alle e-ontwikkelingen zal de ICT-impact op de bedrijfsvoering en de controleerbaarheid van die processen groot zijn.

Literatuur

[Blok98]
Prof. J.H. Blokdijk RA, *EDP Auditorium: Reactie op het artikel van J.C. Boer RE RA*, Compact 1998/5.

[Boer98]
J.C. Boer RE RA, *ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking*, Compact 1998/3.

[Fijn99]
Dr. R.G.A. Fijneman RE RA, *De betekenis en inhoud van 'jaarrekening ICT-auditing' als onderdeel van de jaarrekeningcontrole*, Tilburg University Press, 1999.

[Jonk99]
R.A. Jonker RA, *Information Risk Management en Audit 2000*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

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

[Kort98]
W. de Korte RE RA, *EDP-auditor en jaarrekeningcontrole van vergaand geautomatiseerde organisaties*, Compact 1998/3.

[KPMG00]
KPMG, *KPMG Audit Manual*, (draft), Interne publicatie KPMG, 2000.

[Tayl98]
Frank Taylor, *IT Risk to Audit Risk*, interne presentatie KPMG US, 1998.

Drs. H.G.Th. van Gils RE RA
is coördinator van de business line IRM in the external audit en voorzitter van de productontwikkelingsgroep Pakketcertificering. Daarnaast is hij docent IT-auditing binnen de accountantsopleiding aan de Universiteit van Amsterdam.