# Ongedeelde verantwoordelijkheid RA ter discussie: IT-auditor krijgt (eindelijk) erkenning!

*Prof. A.W. Neisingh RE RA*

**De titel van het artikel zegt in feite genoeg. Hoelang hebben zij die uitsluitend RA zijn het alleenvertoningsrecht voor de controle van de jaarrekening? Het betreft dan in het bijzonder de controle van organisaties die in vergaande mate geautomatiseerd zijn en waarbij onherroepelijk de kwaliteit van de ICT-organisatie object van onderzoek dient te zijn.**

## Inleiding

Een uitdagende titel siert dit artikel. Maatschappelijke ontwikkelingen waarbij ook de RA nauw betrokken is, staan niet stil. Over vaktechnische problematiek wordt veel geschreven en nagedacht. Echter, toen de beroepsorganisatie van RA's meende dat Register EDP-auditors (RE's) in de moederschoot moeten terugkeren ([NIVRA00]), achtte uw auteur de tijd gekomen eens na te gaan of de RA wel in staat is de ongedeelde verantwoordelijkheid te dragen voor de jaarrekeningcontrole nu de complexiteit van informatie- en communicatietechnologie (ICT) snel toeneemt. Immers, de invloed van het gebruik van ICT op interne beheersing en daarmee in relatie staande accountantscontrole is niet gering.

Ruim dertig jaar geleden startten de grote accountantsorganisaties met specialismen op het gebied van 'automatisering en controle'. De ontwikkelingen gingen snel; waar oorspronkelijk slechts RA's zich bezighielden met het vakgebied IT-auditing treft men in deze beroepsgroep relatief gezien steeds meer niet-RA's aan. Een gevolg van de succesvolle EDP-auditingopleidingen en de oprichting in 1992 van de Nederlandse Orde van Register EDP Auditors (NOREA).

Nederland ziet zich op dit punt overigens als voortrekker gepositioneerd. Het verwonderlijke is echter dat ondanks dat in veel organisaties RE's en RE RA's de algemeen accountant terzijde kunnen staan bij de uitvoering van de jaarrekeningcontrole, deze laatste vooral niet weet hoe te handelen. De vraag kan worden gesteld of de controleaanpak wel in alle gevallen correct is, doch ook of gezien de ontwikkelingen in ICT een ongedeelde verantwoordelijkheid van de RA nog wel mogelijk is. De tijd van een procentueel gezien volstrekt onvoldoende IT-auditbudget in relatie tot het totale controlebudget ter geruststelling van het geweten van de RA lijkt definitief voorbij.

In dit artikel wordt het gangbare begrip Information Risk Management (IRM)-deskundigen/specialisten gebruikt in plaats van EDP-auditor, ICT-auditor, etc. Het EDP-auditvakgebied heeft zich vergaand ontwikkeld; ook IT- of ICT-audit dekt de lading niet langer nu het steeds meer handelt om het beheersen van risico's ten gevolge van het gebruik van ICT in organisaties.

## Information Risk Management volwassen?

Onder de titels *EDP Audit volwassen?* ([NGI87]) en *Beveiliging in beweging* ([Paan95]) verschenen publicaties ter gelegenheid van de pensionering van twee grondleggers van het EDP-auditingvakgebied. Begonnen rondom de decenniumwisseling 1970 is er sprake van een langdurig proces waarin Information Risk Management (IRM), hetgeen beter de kern van het vakgebied weergeeft, rond de millenniumwisseling naar een zekere graad van volwassenheid is gegroeid. In den beginne was de ondersteuning van de accountants beperkt tot 'automatisering en controle' en gericht op het programmeren van accountantscontroleprogrammatuur, alsmede het bijwonen van de verwerking daarvan. Reeds snel werd duidelijk dat het voor een efficiënte uitvoering van de controle van de jaarrekening van grote betekenis was te weten welke geprogrammeerde controles in het geautomatiseerde deel van het informatiesysteem waren opgenomen om vervolgens vast te stellen of deze controlemaatregelen waren verankerd in de gebruikersorganisatie. Al snel werden derhalve IRM-deskundigen ingezet om audits naar de kwaliteitsaspecten betrouwbaarheid omvattende exclusiviteit, integriteit en controleerbaarheid, uit te voeren.

De methoden en technieken om deze systems audits uit te voeren ontwikkelden zich eveneens snel en na wat thans nog wordt genoemd business process analysis (d.w.z. gericht op de processen en niet zozeer op de systemen) ontstond de business-measurementprocesmethode. Een door accountants in vele landen gebruikte methodiek om alvorens tot beoordeling van geautomatiseerde processen te besluiten in te gaan op de risico's die met het proces te maken hebben. Waar deze methoden en technieken aanvankelijk derhalve door IRM-deskundigen werden gehanteerd, heeft successievelijk een verschuiving naar de 'gewone' accountantscontrolepraktijk plaatsgevonden ([Koed00]). Ingeval de gebruikte ICT zeer complex is, zal de specialist ondersteuning moeten verlenen bij de beoordeling van de kwaliteitsaspecten van de geautomatiseerde informatiesystemen/processen. Immers, in de opleiding tot RA wordt nog immer (te) weinig tijd besteed aan de problematiek ten aanzien van het gebruik van ICT in organisaties en de invloed daarvan op de beheersing en op de accountantscontrole. De Rijksuniversiteit Groningen ([Neis99a]) brengt hierin reeds jaren succesvol verbetering.

De ontwikkeling in de ICT kenmerkt zich onder meer door de introductie van multiprogrammering, het ontstaan van zogenaamde midrangecomputersystemen alsmede PC-netwerken, databasemanagementsystemen en dergelijke. Een ontwikkeling die grote consequenties heeft voor de te treffen beheersingsmaatregelen in organisaties en derhalve direct de kwaliteit van de organisaties raakt.

De ondersteunende rol van IT-auditors in de jaarrekeningcontrole verandert.

De accountant, ondersteund door deskundigen, onderzoekt in het kader van de controle van de jaarrekening veelal slechts op hoofdlijnen de kwaliteitsaspecten van de ICT-functie. Was het destijds voldoende om op deze wijze de ICT in de aanpak van de accountantscontrole te betrekken, ten gevolge van de hiervoor gememoreerde ontwikkelingen kon het niet uitblijven dat de nadruk van te treffen internecontrole- en beveiligingsmaatregelen ook kwam te liggen bij de ICT-functie zelve. Immers, de mogelijkheden tot het gebruik van onder meer datacommunicatiefaciliteiten nemen toe en derhalve is het noodzakelijk de functie- en taakverdeling van de gebruikersorganisatie te verankeren in de wijze waarop het toegangscontrolesysteem van de computer wordt geïmplementeerd ([Neis99b]).

### Ontwikkelingen in werkterrein IRM

De IRM-praktijk heeft zich in de loop der jaren zowel 'in de diepte' als 'in de breedte' snel ontwikkeld. Met het begrip 'in de diepte' wordt bedoeld dat deskundigen op hardware-/softwaregebied aan de reeds aanwezige deskundigheid werden toegevoegd.
Deze deskundigen zijn bij uitstek in staat vast te stellen of de vereiste maatregelen van interne controle en beveiliging op een adequaat niveau zijn getroffen. De snelle ontwikkeling van hardwarecomponenten (van mainframe naar PC-netwerk), alsmede het ontstaan van een breed aanbod van zogenaamde harde software (besturingssysteem, toegangsbeveiligingssysteem, databasemanagementsysteem, bibliotheekbeheerssysteem, enz.) respectievelijk het samenvoegen van deze besturingssoftwarecomponenten in één besturingssysteem voor gebruik op midrangecomputer- en PC-netwerksystemen maakt specifieke deskundigheid noodzakelijk.
Waar echter de accountant belast met de controle van de jaarrekening nog immer in veel gevallen slechts een beperkt beroep doet op deze specialisten, is vervolgens een nieuwe markt van dienstverlening voor IRM ontstaan. Deze ontwikkeling heeft mede geleid tot het totstandkomen van zogenaamde security baselines, op tactisch niveau vastgelegd in de Code of Practice for information security management en vertaald in het Nederlands in de Code voor Informatiebeveiliging ([NNI00]). De security baselines zullen uiteraard dienen te worden toegesneden op de specifieke typologie van de organisatie, de gebruikte hardware- en software-infrastructuur. De invulling is verder afhankelijk van de specifieke risico's en de mate van afhankelijkheid van ICT van de organisatie. Daarmee worden security baselines als het ware 'moving targets'. Op termijn zal de baseline dienen te worden aangepast aan de ontwikkelingen in de ICT, terwijl het specifiek maken voor organisaties ook betekent dat nieuwe ontwikkelingen gevolgen moeten hebben voor het niveau, de aard en de omvang van de te treffen internecontrole- en beveiligingsmaatregelen. En zo wordt het IT-auditvakgebied dus nooit volwassen, immers het proces van definiëren van uitvoerings- en beoordelingsnormen, ontwikkelingen daarin en bijstellen is een perpetuum mobile.
ICT ontwikkelt zich, derhalve ontwikkelen de security baselines zich. IRM zal moeten bijblijven en desnoods anticiperen op het gebied van beheersing en beveiliging van de ICT opdat kwalitatief goede dienstverlening, zowel op audit- als adviesterrein kan worden geleverd.

Het pakket aan dienstverlening van IRM ontwikkelt zich niet slechts 'in de diepte', zoals hiervoor gemotiveerd en toegelicht, doch zeker ook 'in de breedte'. Was de insteek primair het ondersteunen van de accountantscontrolepraktijk en wel het geven van kwaliteitsoordelen over toepassingsprogrammatuur en zo nodig over de kwaliteit van voornamelijk de verwerkingsorganisatie van het computercentrum (onderdeel van de ICT-functie), al snel werd het werkterrein verbreed naar de beoordeling van methoden, technieken en procedures in de systeemontwikkelingsorganisatie. In deze systeemontwikkelingsorganisatie wordt toepassingsprogrammatuur ontwikkeld. De introductie van nieuwe toepassingsprogrammatuur brengt veranderingen teweeg in de gebruikersorganisatie en zal voor de accountant betekenen dat de toepassingscontroles opnieuw zullen moeten worden beoordeeld.
Het is niet uitgesloten dat de controleaanpak zal moeten worden gewijzigd. In de ontwikkelingsfase van nieuwe programmatuur kan derhalve al worden gesteld dat de controleaanpak voor toekomstige jaarrekeningen kan worden beïnvloed. Zowel het inbrengen van deskundigheid op het gebied van beheersing en beveiliging van de geautomatiseerde processen, als het beoordelen van de kwaliteit van de organisatie die deze toepassingsprogrammatuur ontwikkelt, is van belang. In dit verband verdient het inrichten van een quality-assurancefunctie (QA) de voorkeur. Deze QA-functie – als verzamelnaam – is verantwoordelijk voor het opstarten, stimuleren en sturen van de kwaliteitsbeheersing en verder het plannen, sturen en evalueren van de activiteiten die worden ondernomen in dat kader om het ontwikkelproces te verbeteren. Verder zal de QA-functie een formele toetsing uitvoeren om na te gaan of de opgeleverde of op te leveren producten voldoen aan de algemene en projectspecifieke eisen die aan die producten zijn gesteld ([Giel90]).

### Betekenis informatiebeveiligingsbeleid

De meetlat voor wat betreft te treffen maatregelen, waaronder ook begrepen maatregelen gericht op het waarborgen van de beschikbaarheid (continuïteit) van de geautomatiseerde informatieverzorging, kwam veelal voort uit professional judgement. Pas op een later moment werd duidelijk dat het hebben van een organisatiebreed informatiebeleid en daaruit afgeleid informatiebeveiligingsbeleid de basis zou dienen te vormen voor op tactisch niveau te definiëren maatregelen en op opera-

tioneel niveau in te voeren maatregelen. Voortschrijdend inzicht is nog steeds geen schande! Derhalve ontstond ook op dat gebied een verdergaande dienstverlening die thans wel wordt samengevat onder het begrip corporate information security. En de laatste jaren zien we specialisten op het gebied van controle en beveiliging van electronic-commerce(toepassingen) hun plaats in de IRM-organisatie innemen. Om de kwaliteit van trusted third parties te kunnen beoordelen is een diepgaande kennis nodig, die wordt opgebouwd door het adviseren respectievelijk (mede) implementeren van public key infrastructures, certification authorities en dergelijke. Nieuwe technologieën worden alweer aangekondigd, zoals WAP, hetgeen betekent dat IRM-organisaties in beweging blijven om ten minste gelijke tred te kunnen blijven houden met de ICT-ontwikkelingen en dus het gebruik in organisaties en de beheersing ervan. Er blijkt een gedegen groep specialisten te zijn opgestaan. Deze specialisten bieden zowel ondersteuning bij de controle van de jaarrekening, waar sprake is van complexe omgevingen, terwijl op brede schaal audits worden uitgevoerd en adviezen worden gegeven op verzoek van het management van de organisaties. Het gaat immers primair om de beheersing van de ICT-inspanning en van de organisaties, waarvoor het management verantwoordelijk is. En in feite pas later om de controle van de jaarrekening waar – afhankelijk van complexiteit van de ICT-inspanning – de ICT-functie steeds vaker een hoofdrol vervult.

In IRM-kringen worden de ICT-ontwikkelingen op de voet gevolgd en wordt getracht na te gaan welke gevolgen integratie van logistieke en administratieve processen, robotisering, WAP en dergelijke hebben op de beheersing van de ICT-inspanning van de organisaties en aansluitend daarop voor de accountantscontrole.

### Opleiding accountants schiet tekort

Waar in de praktijk van de accountantscontrole de invloed van het gebruik van ICT op de beheersing van organisaties en op de accountantscontrole in veel gevallen nog nauwelijks wordt onderkend, is reeds eind jaren tachtig bij de Rijksuniversiteit Groningen (RuG) een profielschets gemaakt voor een hoogleraar betrouwbaarheidsaspecten geautomatiseerde informatiesystemen, die onderwijs zou moeten geven met betrekking tot zowel de beheersingsaspecten als de accountantscontroleaspecten bij het gebruik van ICT, en tevens onderzoek terzake zou moeten uitvoeren. In het collegeprogramma is in de doctoraalopleiding bedrijfseconomie/bedrijfskunde, accountancyvariant circa tienmaal drie lesuren ruimte gecreëerd om de invloed van het gebruik van ICT op de beheersing van de organisaties te behandelen, terwijl in de postdoctorale opleiding (invloed van het gebruik van ICT op de accountantscontrole) eveneens circa tienmaal drie lesuren ruimte is geschapen. Hiermee onderscheidt de RuG zich al tien jaren van vele andere faculteiten waar slechts weinig tot geen ruimte voor behandeling van de onderhavige problematiek is ingeruimd. Aan deze situatie is overigens recent een halt toegeroepen. In de permanente werkgroep accountantscontrole, waarin de hoogleraren verbonden aan de accountancyopleidingen zitting hebben, is thans een ‘common body of knowledge’ geaccepteerd dat in het kader van zijn promotieonderzoek is gedefinieerd door dr. R.G.A. Fijneman RE RA ([Fijn99]). Deze actie moet leiden tot het opnemen ervan in de eindtermen voor de opleiding tot registeraccountant. En zo wordt met een vertraging van ten minste tien jaar een enigszins adequaat niveau terzake in Nederland bereikt. Helaas zal blijken dat beroepsgenoten er nog vele jaren voor nodig zullen hebben het geleerde daadwerkelijk in praktijk te brengen.

Een andere ontwikkeling die zeker niet ongenoemd mag blijven, omdat Nederland excelleert op dat terrein, betreft de postdoctorale EDP-auditopleidingen. Zowel aan de Katholieke Universiteit Brabant (KUB), de Erasmus Universiteit Rotterdam (EUR) en de Vrije Universiteit Amsterdam (VU) zijn EDP-auditopleidingen tot stand gebracht die als postdoctorale opleiding kunnen worden gevolgd. Deze opleidingen zijn overigens bedoeld voor de vorming van IRM-specialisten die als vooropleiding accountancy, bedrijfskunde, informatica, wiskunde of een dergelijke universitaire opleiding hebben. De noodzaak is onderkend een beroepsorganisatie van EDP-auditors tot stand te brengen; de Nederlandse Orde voor Register EDP Auditors (NOREA) is in 1992 opgericht en leidt een florerend bestaan.

### Ontwikkelingen ICT

In de vorige paragraaf werd reeds gewezen op de belangrijke ontwikkelingen die zich hebben voorgedaan in het gebruik en de toepassingsmogelijkheden van informatie- en communicatietechnologie. Het betreft echter niet slechts méér mogelijkheden voor gebruik, te realiseren door implementatie van databasemanagementsystemen, datawarehouses of iets dergelijks, doch evenzeer mogelijkheden tot versterking van de beheersing en beveiliging ervan.
Na de introductie van toegangscontrolesystemen die authenticatie uitvoerden op basis van bijvoorbeeld wachtwoorden, zijn ook op dat terrein belangrijke ontwikkelingen waargenomen. Zo ontstonden de retinascan, controles door gebruik te maken van vingerafdrukken en de combinatie van chipkaarten met password, om de afhankelijkheid van de gemakzucht van de mens te verkleinen respectievelijk te beperken. De in mindere of meerdere mate paperless society doet door de introductie van electronic commerce/electronic business belangrijk van zich horen.
Het betekent het verleggen van internecontrole- en beveiligingsmaatregelen van gebruikerscontroles naar maatregelen geïntegreerd in de ICT-functie, de hardware-/software-infrastructuur en/of de toepassingsprogrammatuur.

De introductie van midrangesystemen en PC-netwerken heeft geleid tot een groot aanbod van standaardprogrammatuur (toepassingsprogramma’s voor verwerking van allerhande functies, zowel administratie, logistiek, personeelsmanagement, salarisadministratie, e.d.). Dientengevolge is de omvang van afdelingen systeemontwikkeling in veel gevallen beperkter geworden, doordat in het geheel niet dan wel nauwelijks eigen functionaliteit aan standaardpakketten diende te worden toegevoegd. Het heeft overigens wel een afhankelijkheid van derden geïntroduceerd. Waar het management te allen tijde verantwoordelijk blijft voor de kwaliteit en performance

van de organisatie en de kwaliteit van de (geautomatiseerde) informatieverzorging, ontstaat nu ook de verantwoordelijkheid voor de kwaliteit van de uitkomsten die worden geleverd door een informatiesysteem dat van een derde is betrokken. Gelukkig biedt de – in de Nederlandse literatuur – third-partymededeling genoemde rapportering een oplossing. Een onafhankelijk deskundige, een IRM-deskundige, beoordeelt tegen een uitgebreid normenstelsel of in het pakket voldoende controle- en beveiligingsmaatregelen zijn opgenomen. Indien dat het geval is, wordt een oordeel gegeven en opgenomen in een third-partymededeling.

Zoals in de loop der decennia bij voortduring een wisselwerking centralisatie versus decentralisatie zichtbaar was, is in de afgelopen jaren een tendens ontstaan de rekencentrumfunctie (de verwerkingsorganisatie) uit te besteden aan een dienstverlener die daarvan haar kerntaak heeft gemaakt (outsourcing). Deze ontwikkeling past in het streven van een organisatie zich te oriënteren op haar kerntaken en – indien ICT niet per se daartoe behoeft te worden gerekend – deze uit te besteden. Ook in dit geval kan naar analogie van hetgeen over standaardpakketten is gezegd, worden gesteld dat het management vanzelfsprekend verantwoordelijk blijft voor het gehele proces van (de kwaliteit van) de geautomatiseerde informatieverzorging en dat het zich derhalve moet overtuigen van de kwaliteit van de organisatie en van de diensten die door de externe partij op het gebied van de operationele gegevensverwerking worden geleverd.

Op beide gebieden hebben IRM-deskundigen zich ontwikkeld, zodat zij in staat zijn oordelen terzake, gericht op de getroffen kwaliteitsmaatregelen, af te geven ([Velt95]).

Primair is audit van geautomatiseerde processen noodzakelijk.

Afzonderlijk moet nog melding worden gemaakt van het feit dat ook in de advocatuur dientengevolge een nieuwe richting is ontstaan: informaticarecht. Primair gericht op de beoordeling van contracten met betrekking tot aanschaf van pakketten en bescherming van de intellectuele eigendom ervan. Vervolgens op dienstverleningscontracten die verder moeten worden uitgewerkt in zogenaamde service level agreements, wetgeving op het gebied van ICT (zoals de Wet telecommunicatievoorzieningen, de Wet bescherming persoonsgegevens, de Wet computercriminaliteit), op ontwikkelingen met betrekking tot de bewijs- en bewaarplicht in verband met elektronische opslag en dergelijke.

### Controleaanpak (IRM in the external audit)

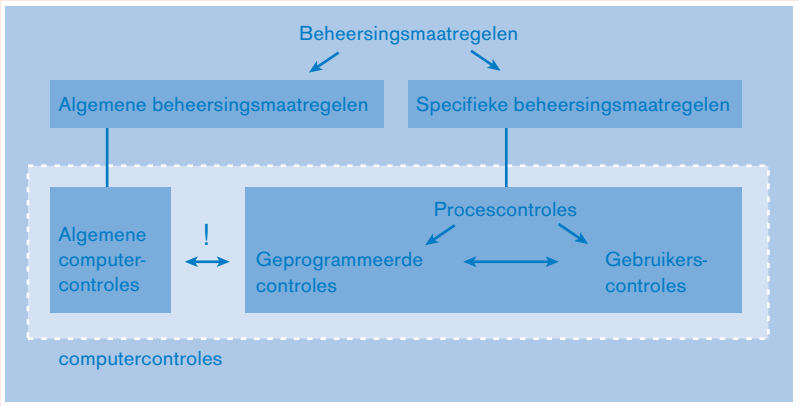
Het definiëren van een aanpak voor de controle van de jaarrekening is geen sinecure. Kennis van de te controleren organisatie is noodzakelijk om processen te kunnen identificeren en inzicht in de organisatorische opbouw is daarbij onontbeerlijk. Het gaat er ten slotte om tot een afgewogen oordeel te komen over de in te zetten controlemiddelen. Van belang is daarbij of en zo ja, in hoeverre kan worden gesteund op de kwaliteit van opzet en bestaan en aansluitend (en zeker zo belangrijk) werking van een adequaat ingericht stelsel van algemene maatregelen van interne controle en beveiliging. En daar wringt dan nog steeds de schoen. In nagenoeg alle gevallen wordt de controlerend accountant geconfronteerd met ICT-organisaties die in mindere of meerdere mate complex zijn. Veel geautomatiseerde processen zijn complex van aard en dienen eveneens object van onderzoek te zijn.

Het is dus niet voor niets dat in moderne accountantscontroleaanpakken verschillende fasen worden onderkend. Zo is er om te beginnen sprake van een strategiefase waarin wordt bepaald op welke wijze de kwaliteitsaspecten van ICT worden geëvalueerd ([Gils00]). Reeds verschillende malen is door vooraanstaande auteurs gepubliceerd over de modellen van samenwerking van financial en EDP-auditors ([Neis99c], [Jonk00]).

Uitgangspunt in dit artikel is dat de bedrijfsprocessen van de te controleren organisatie in vergaande mate geautomatiseerd zijn. Het betekent dat in die geautomatiseerde processen in de programmatuur en op grond van de aanwezige gegevens respectievelijk de ingevoerde gegevens beslissingen worden genomen en berekeningen worden uitgevoerd. Het gaat dan overigens om veelal routinematige processen ([Boer99]). De ICT-omgeving waarin dergelijke processen operationeel zijn, wordt steeds complexer. Computersystemen zijn door middel van netwerken verbonden met andere netwerken, andere computersystemen en met internet. De accountant zal dus genoodzaakt zijn zich primair een oordeel te vormen over de kwaliteit van de maatregelen van interne controle en beveiliging die in de geautomatiseerde processen zijn opgenomen. Koedijk ([Koed99]) geeft een uitgebreide beschrijving van de fasering die op hoofdlijnen als volgt kan worden weergegeven:

- *strategische analyse:* inzicht verkrijgen in het bedrijf, de strategie, de bedrijfsrisico's en doelstellingen, de bedrijfsprocessen en de IT-omgeving;
- *documentatie:* in kaart brengen van processtappen of activiteiten (inclusief mogelijk handmatige handelingen);
- *risk assessment:* definiëren van risico's met betrekking tot processtappen (of activiteiten); het inschatten van de kans van het zich voordoen van een risico en het bepalen van de toetsingseisen (normen);
- *identificeren controlemaatregelen:* vaststellen aan de hand van documentatie, waarnemingen en interviews welke beheersingsmaatregelen door het management daadwerkelijk zijn getroffen;
- *vaststellen/bepalen restrisico's:* op grond van de confrontatie norm versus daadwerkelijk getroffen maatregelen vaststellen of er sprake is van een toereikend stelsel van maatregelen om het risico te beheersen en eventueel daaruit resulterend het restrisico;
- *vaststellen werking van controlemaatregelen:* hierbij dient de relatie met het stelsel van algemene maatregelen niet uit het oog te worden verloren.

Zodra de accountant heeft vastgesteld dat inderdaad sprake is van complexe geautomatiseerde processen en dat zowel de gebruikersorganisatie als ook hij-/zijzelf zal moeten steunen op de uitkomsten van de processen die langs geautomatiseerde weg totstandkomen, zal dat consequenties hebben voor zijn/haar werkzaamheden. Met andere woorden, een onderzoek zal moeten worden uitgevoerd met betrekking tot de kwaliteit van de ICT-organisatie en wel primair naar opzet en bestaan en zodra is vastgesteld dat deze van adequaat niveau zijn, ook naar de werking ([Kort99]). Nimmer mag impliciet worden gesteund op bestaan en goede werking terwijl daarnaar nauwelijks of geen onderzoek is uitgevoerd. Overigens gebiedt de eerlijkheid te zeggen dat de uitkomsten van het onderzoek naar opzet en bestaan van het stelsel van algemene maatregelen en procedures dat geldt voor alle geautomatiseerde processen, van invloed zijn op de te treffen controlemaatregelen in de geautomatiseerde processen. De relatie tussen de verschillende controlemaatregelen wordt in figuur 1 uiteengezet.




*Figuur 1. Relatie tussen de verschillende controlemaatregelen.*

### Inzet IRM-deskundigen noodzakelijk

Weliswaar kan op hoofdlijnen door de algemene accountant worden onderzocht of de opzet toereikend is in het kader van de controle van de jaarrekening, doch veelal zal blijken dat de kennis benodigd om het daadwerkelijk bestaan en dus het vaststellen van de kwaliteit van de getroffen maatregelen niet aanwezig is bij die algemeen accountant. Deze zal dus 'gedwongen worden' collega-specialisten, IRM-deskundigen, in te schakelen. Een en ander betekent dus dat IRM initieel een diepgaand onderzoek moet uitvoeren, want – om een en ander nog eens op een andere wijze te formuleren – het gaat de gebruiker erom zeker te weten en erop te kunnen vertrouwen dat de door hem verworven toepassingsprogrammatuur ofwel de geautomatiseerde processen, die door hem uitdrukkelijk zijn getest en geaccepteerd, daadwerkelijk in de productieomgeving (van het computersysteem) zijn opgenomen en in continuïteit ongewijzigd worden gebruikt. Wanneer de gebruiker van de kwaliteit van de maatregelen en procedures uitgaat, zal de accountant moeten vaststellen dat terecht wordt gesteund op de goede kwaliteit van maatregelen en procedures die in de ICT-organisatie terzake zijn getroffen.

### Benchmarking ICT-controls

Het onderzoek naar de kwaliteit van de maatregelen en procedures in de ICT-organisatie zal allereerst op hoofdlijnen worden toegespitst ([Boer00]). Het stelsel van algemene maatregelen van interne controle en beveiliging dient dan te worden onderzocht. De onderverdeling zoals gebruikt in de Code voor Informatiebeveiliging wordt hierbij veelal gehanteerd, te weten:

* beveiligingsbeleid;
* beveiligingsorganisatie;
* classificatie en beheer van bedrijfsmiddelen;
* beveiligingseisen ten aanzien van personeel;
* fysieke beveiliging en beveiliging van de omgeving;
* beheer van communicatie- en bedieningsprocessen;
* toegangsbeveiliging voor systemen;
* ontwikkeling en onderhoud van systemen;
* continuïteitsmanagement;
* naleving.

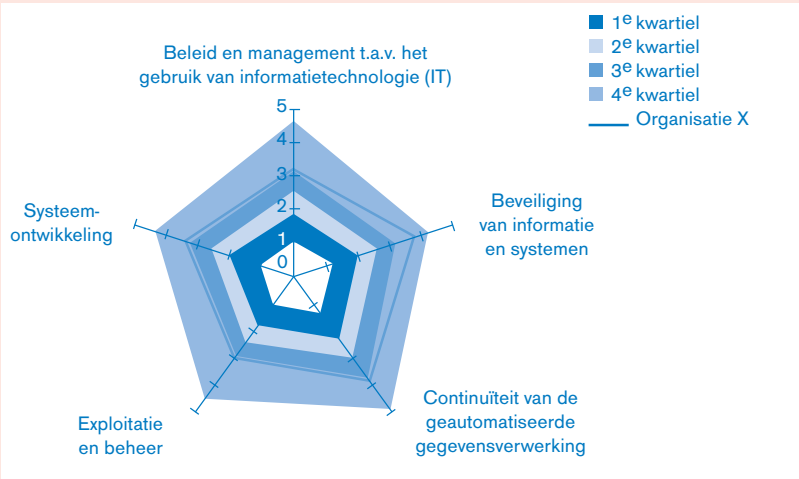
Om snel inzicht te verkrijgen wordt veelal gebruikgemaakt van vastlegging in een benchmarkingtool, waardoor het bijvoorbeeld mogelijk is de uitkomsten te vergelijken met die van organisaties in dezelfde branche ([Boer00]). De uitkomsten worden dan grafisch weergegeven in zogenaamde spinnenwebben (zie figuur 2).

Het gebruik van benchmarks kan als een toegevoegde waarde aan de audit worden gezien. Toepassing ervan geeft immers op relatief eenvoudige wijze inzicht in de kwaliteit van (complexe) ICT-organisaties.

In veel gevallen zal niet kunnen worden volstaan met het slechts kennisnemen op hoofdlijnen van de kwaliteit van de ICT. Daadwerkelijk goede kennis van de belangrijkste maatregelen en procedures, bijvoorbeeld ingericht naar ITIL-model (Information Technology Infrastructure Library) kan nodig zijn. Dit vereist diepgaande ICT-kennis die vrijwel nooit bij de algemeen accountant aanwezig zal zijn.

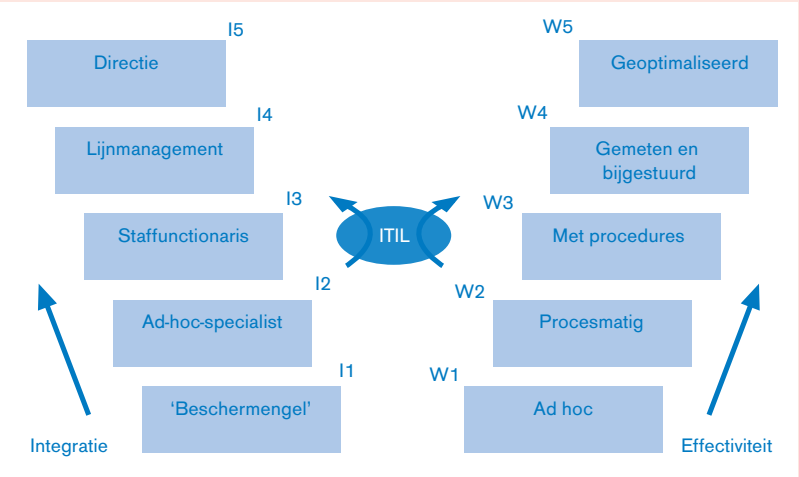
Er moet in bedoelde gevallen sprake zijn van een aanpak 'in de breedte' en 'in de diepte'. Om te beginnen zal kennis moeten worden genomen van het informatiebeveiligingsbeleid, dat overigens dient te zijn afgeleid uit het informatiebeleid. Het daarin gestelde met betrekking tot kwaliteitsaspecten van ICT (zoals beschikbaarheid, exclusiviteit, integriteit en controleerbaarheid) zal moe-

*Figuur 2. Een benchmark van IT-beheersingsmaatregelen.*



ten zijn vertaald naar normen op tactisch niveau. In feite is in dit proces de meetlat gelegd die in de organisatie nader dient te zijn uitgewerkt, en door de accountant als uitgangspunt bij de beoordeling zal moeten worden gebruikt. Vanzelfsprekend zal marginale toetsing door de accountant van het informatiebeveiligingsbeleid van belang zijn. Veel verder zal de accountant niet kunnen gaan. Er is sprake van een beleidsdocument dat dient te zijn gesanctioneerd door de hoogste leiding. Zo'n informatiebeveiligingsbeleid is overigens geen statisch document; de ontwikkelingen in de ICT gaan snel, de toepassingsmogelijkheden in de organisaties volgen in een iets trager tempo en de invloed op aard, omvang en kwaliteit van te treffen controle- en beveiligingsmaatregelen kan groot zijn. De meetlat, afgeleid uit het informatiebeveiligingsbeleid, is in feite een moving target. Toch blijft het van belang vast te stellen dat het management voldoende aandacht besteedt aan het definiëren van een informatiebeveiligingsbeleid, maar evenzeer aan het implementeren daarvan, hetgeen mede betekent dat een uitgebreid awarenessprogramma moet worden gestart om alle lagen in de organisatie te beïnvloeden en te overtuigen van de betekenis van zo'n informatiebeveiligingsbeleid en de uitwerking daarvan. Ten slotte wordt iedereen geconfronteerd met de maatregelen en procedures die zijn afgeleid uit dat beleid. Of het nu gaat om fysieke toegang tot computerapparatuur en netwerkapparatuur, om de telefooncentrale, om het toegang verkrijgen via PC's en terminals tot gegevens dan wel om het testen van nieuwe respectievelijk gewijzigde programmatuur.

Het is steeds vaker gebruikelijk dat tussen de ICT-organisatie en de gebruikersorganisaties zogenaamde service level agreements (SLA's) worden afgesloten. Veelal wordt het begrip SLA gebruikt in de relatie van servicebureau ten opzichte van zijn afnemers, doch met name intern en dus ter ondersteuning van goede interne verhoudingen is het noodzakelijk de afspraken met betrekking tot de kwaliteitseisen ten aanzien van de werking van geautomatiseerde processen goed vast te leggen. Aandacht dient ten minste te worden besteed aan beschikbaarheidseisen, integriteits- en exclusiviteitseisen, waarbij op het punt van beschikbaarheid niet uitsluitend moet worden gedacht aan uitvallen van de beschikbare verwerkingscapaciteit gedurende kortere of langere tijd, maar eveneens aan responstijden, workload en dergelijke.




*Figuur 3. Volwassenheidsniveau in relatie tot niveau informatiebeveiliging.*

### Volwassenheidsniveau organisatie in relatie tot informatiebeveiliging

Het volwassenheidsniveau van de organisatie kan ook in relatie worden gebracht met het niveau van informatiebeveiliging. Spruit ([Spru00]) brengt de volwassenheidsniveaus die met ITIL-security management kunnen worden bereikt in beeld, zoals weergegeven in figuur 3.

Voor wat betreft de beoordeling van de geautomatiseerde informatieverzorgingsprocessen geldt dat de algemeen accountant de aangewezen persoon is deze te beoordelen. De accountant kent de specifieke organisatie en de processen en moet derhalve in staat worden geacht gegeven de typologie van de organisatie en van de geautomatiseerde processen de toetsingsnormen te definiëren. Op grond van ervaringen zijn algemene toetsingsnormen inmiddels gedefinieerd (denk hierbij aan de vele audits van standaardpakketten waarover in de vorm van third-partymededelingen is gerapporteerd); deze algemene normen dienen te worden toegesneden op de te beoordelen processen.

Wanneer er sprake is van complexe toepassingen/processen kan de algemeen accountant altijd een beroep doen op IRM-deskundigen. Dit zal veelal het geval zijn bij het gebruik van complexe ICT-infrastructuren en/of -processen waarin rekenregels zijn opgenomen, respectievelijk op grond van confrontatie met (vaste) gegevens beslissingen worden genomen en ook de onderliggende programmatuur, zoals databasemanagementsystemen, van belang zijnde functionaliteit bevat. Te denken valt hierbij aan de verankering van de functie- en taakverdeling binnen organisaties in de programmatuur.

Nu zowel aandacht is besteed aan benchmarking van ICT-controls, dus het verkrijgen van een oordeel over de kwaliteit van het stelsel van algemene maatregelen van interne controle en verder aan onderzoeken naar de toereikendheid van toepassingscontroles, lijkt het nog slechts een kleine stap de gegevensgerichte controlebenadering (in geval van routinematige processen) in te ruilen voor de systeemgerichte controleaanpak. Niets is echter minder waar!

### Consequenties van de keuze van de controleaanpak

Nu de keuze door de accountant moet worden gemaakt tussen een systeemgerichte en een gegevensgerichte benadering, dat wil zeggen steunen op de werking van de goede kwaliteit van het stelsel van algemene maatregelen van interne controle en beveiliging, alsmede op de geprogrammeerde controles in de toepassingsprogrammatuur respectievelijk het toch kiezen voor een gegevensgerichte controlebenadering, moet worden vastgesteld dat veelal en terecht gekozen wordt voor een systeemgerichte benadering. Echter, de consequenties voor de aanpak van de accountantscontrole worden niet getrokken.

Het betekent dat de samenstelling van de controleploeg zal moeten worden gewijzigd, in die zin dat 'eenvoudige' accountantscontrolearbeid dient plaats te maken voor inzet van IRM-deskundigen in de controle. Het gaat er ten slotte om te aanvaarden dat in het kader van die controle dient te worden vastgesteld dat het stelsel van alge-

mene maatregelen – dat zo bepalend is voor de kwaliteit van de geprogrammeerde controles – op handhaving en naleving (goede werking) dient te worden beoordeeld. Veelal wordt gesteund op de goede werking van het stelsel van algemene maatregelen zonder dat de consequentie wordt getrokken dat die goede werking dan ook in de loop van het jaar dient te worden vastgesteld.

De aandacht van de door de accountant ingezette IRM-deskundige zal zich in belangrijke mate moeten richten op de waarborging van de kwaliteit van het change- en problem-managementproces (inclusief incidentmanagement). Het gaat er ten slotte om vast te stellen dat de gebruikersorganisatie, die eigenaar van de toepassingsprogrammatuur en de data is, er terecht zeker van kan zijn dat de door haar geteste en geaccepteerde toepassingsprogrammatuur daadwerkelijk in productie is genomen en in continuïteit ongewijzigd in productie is gebleven.

De vraag is nu waaruit de terughoudendheid voortkomt bij accountants om IRM-deskundigen in te schakelen. In het bank- en verzekeringswezen is inzet van IRM-deskundigen in de jaarrekeningcontrole vanzelfsprekend geworden, mede ten gevolge van de introductie van memoranda inzake betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking, zoals het memorandum van DNB uit september 1988 en het memorandum outsourcing d.d. 27 mei 1994. Deze zijn recent vervangen door de Regeling Organisatie en Beheersing.

Echter, ook de Wet computercriminaliteit is van toepassing. Aan de tekst van artikel 393 lid 4 Boek 2 BW 'De accountant brengt omtrent zijn onderzoek verslag uit aan de Raad van Commissarissen en de directie' is een tweede zin toegevoegd die luidt: 'Hij maakt daarbij ten minste melding van zijn bevindingen met betrekking tot betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking'.

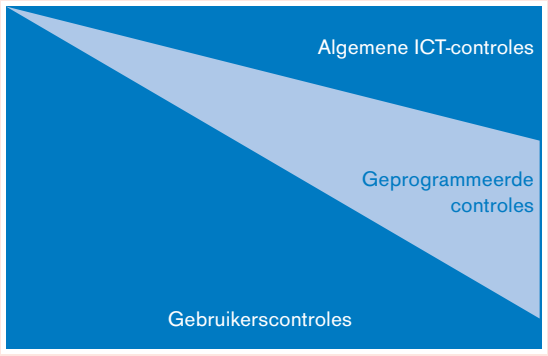
In de opvatting van de minister van Justitie brengt deze wet geen verandering in de controlewerkzaamheden van de accountant. De minister heeft in de nota naar aanleiding van het eindverslag (Tweede Kamerstuk 21551 nr. 11) het volgende gesteld: 'Deze bevindingen kunnen alleen zaken betreffen die de accountant bij de uitoefening van de controle van de jaarrekening tegenkomt. In het kader van de controle komt de accountant in aanraking met de administratieve organisatie en de interne controle van de onderneming. Langs die weg zal hij ook de geautomatiseerde gegevensverwerking onderzoeken voorzover noodzakelijk voor de jaarrekeningcontrole.' De minister veronderstelt derhalve dat de accountant, voorzover noodzakelijk in het kader van de controle van de jaarrekening, bevindingen heeft over het functioneren van de geautomatiseerde gegevensverwerkende systemen.

Waarom dan toch niet de IRM-deskundigen ingeschakeld? Een mogelijke oorzaak kan gevonden worden in enerzijds het opleidingsniveau van de algemeen accountant met betrekking tot de invloed van ICT op de beheersing van organisaties en op de accountantscontrole en anderzijds op het feit dat zij daardoor onvoldoende in staat zouden kunnen zijn te definiëren welke werkzaamheden door deskundigen in het kader van de controle van de jaarrekening zouden moeten worden uitgevoerd om de accountant de benodigde zekerheid te kunnen bieden. Een veel gestelde vraag vanuit de accountant is: 'Welke meerwaarde biedt de inzet van IRM-deskundigen in de jaarrekeningcontrole?' Een tegenvraag zou kunnen zijn: 'Welke meerwaarde biedt de jaarrekeningcontrole indien IRM-deskundigen niet zouden worden ingeschakeld? Kan er in de gegeven voorbeelden dan eigenlijk nog wel sprake zijn van een deugdelijke grondslag?'

Laat overigens duidelijk zijn dat van de algemene accountant nooit verwacht mag worden dat deze de goede werking van de ICT-organisatie kan controleren. Zijn kennis zal altijd tekortschieten, mede ten gevolge van de snelle ontwikkelingen in de ICT en de wijze waarop organisaties daarvan gebruikmaken. Van deskundigen mag die kennis wel worden verwacht. Denk in dit verband aan de toenemende omvang van het gebruik van electronic business- en electronic commerce-toepassingen, die zelfs binnen het IRM-deskundigheidsgebied weer een verdergaande specialisatie tot gevolg heeft gehad.

### Kwaliteitsaspecten van de controleaanpak

Waar in de vorige paragraaf vanuit de theorie geredeneerd en met een knipoog naar de praktijk gemotiveerd werd dat inzet van IRM-deskundigen in de jaarrekeningcontrolepraktijk in steeds meer gevallen onvermijdelijk wordt, kan ook de vraag worden gesteld of de efficiency en de effectiviteit van de uitvoering van het controleproces er niet bij gebaat zouden zijn deze deskundigen op grotere schaal in te zetten. In figuur 4 is schematisch weergegeven hoe de omvang van controlemaatregelen uit te voeren door de gebruikersorganisatie afneemt ten gunste van de geprogrammeerde controles die overigens in steeds verdergaande mate afhankelijk zijn van de kwaliteit van het stelsel van algemene maatregelen.




*Figuur 4. Samenhang controlemaatregelen.*

Strikt redenerend zouden de gebruikerscontroles kunnen tenderen naar nul, omdat volledig wordt gesteund op de controlemaatregelen begrepen in de bovenliggende niveaus.

Het is dus efficiënt en effectief IRM-deskundigen in te schakelen bij de beoordeling van de kwaliteit van het stelsel van algemene maatregelen, alsmede in continuïteit van de werking daarvan en vervolgens een keuze te maken of de algemene accountant, dan wel de deskun-

dige de geautomatiseerde processen dient te beoordelen. De keuze zal afhangen van het kennis- en ervaringsniveau van de algemeen accountant, doch evenzeer van de complexiteit van de geautomatiseerde processen in relatie tot de ICT-infrastructuur waarop deze worden verwerkt. Een bijzondere problematiek doet zich voor wanneer de organisatie van de gecontroleerde gebruikmaakt van standaardpakketten, waarbij een zogenaamde third-partymededeling is afgegeven, respectievelijk de geautomatiseerde gegevensverwerking heeft uitbesteed aan een externe dienstverlener, waarvoor steeds vaker geldt dat ook zij verantwoording over de kwaliteit van hun organisatie laten afleggen in de vorm van een door een IRM-deskundige af te geven third-partymededeling op deze verwerkingsorganisatie.

De consequenties voor de aanpak van de accountantscontrole en de bemanning van de controlepraktijk kunnen dus groot zijn. Het zal daarbij overigens duidelijk zijn dat de werkpapieren van de IRM-deskundige een integraal onderdeel dienen te vormen van het accountantscontroledossier. De timing van de werkzaamheden van de IRM-deskundige zal verschillen van die van de algemeen accountant. De eerste zal met grotere regelmaat bij de cliënt waarnemingen dienen te verrichten met het oog op het vaststellen van de in continuïteit goede werking van het stelsel van algemene maatregelen.

De prangende vraag is nu of gegeven de ontwikkelingen in het gebruik van ICT in de organisaties en de consequenties die dat heeft voor de aanpak van de accountantscontrole, waarbij IRM-deskundigen een substantieel deel van het controlewerk zullen overnemen, de algemeen accountant (RA) de ongedeelde verantwoordelijkheid kan blijven houden voor de uitvoering van de jaarrekeningcontrole.

## Conclusie

De apotheose is nabij. Van een ongedeelde verantwoordelijkheid van de RA kan geen sprake (meer) zijn in situaties zoals geschetst in de vorige paragrafen. Zo is de rol die de actuaris inneemt in de controle van de verzekeringsmaatschappij of de rol van de belastingconsulent voor wat betreft het vaststellen van de fiscale verplichtingen niet vergelijkbaar met die van de IRM-deskundige die een steeds groter deel van de accountantscontrolewerkzaamheden zal moeten uitvoeren. Iedere vergelijking op dit terrein met andere door de algemeen accountant ingeschakelde dienstverleners gaat mank.

Er is evenwel nog toekomst voor de RA. Bij een grote accountantsorganisatie in Nederland is gekozen voor een model waarin juist afgestudeerde accountants voor een periode van drie jaar worden overgeplaatst naar de IRM-organisatie. Zij blijven voor circa zeshonderd uren per jaar ingeschakeld in controleopdrachten waar ICT een rol van betekenis speelt, volgen de postdoctorale EDP-auditopleiding, en worden overigens ingezet voor het uitvoeren van IRM-opdrachten. Na deze periode van drie jaar, waarin zij een brede kennis en ervaring hebben kunnen opdoen met betrekking tot het uitvoeren van IRM-opdrachten, keren zij terug naar de algemene controlepraktijk en zijn daarmee de toekomstige generatie accountants die in de controlepraktijk beter de inzet van IRM-deskundigen kunnen bepalen en aansturen. Enig werk kunnen zij uiteraard zelf uitvoeren respectievelijk onder hun directe leiding laten uitvoeren, waardoor ook in de algemene controlepraktijk tot een verhoging van kennis- en ervaringsniveau met betrekking tot het gebruik van ICT in organisaties en de accountantscontrole kan worden gekomen.

De verwachting is dat het proces van uitvoering van de controle van de jaarrekening kan worden versneld, zodat het er in deze eenentwintigste eeuw toch van moet komen dat de jaarrekening op 2 januari wordt getekend door ... de RA?, ... de RE?, ... of de RE RA?

## Literatuur


[Beek99]
J.J. van Beek RE RA, J.A.M. Donkers RE en K.M. Lof, *Het belang van ICT binnen due-diligence onderzoeken*, Compact 1999/4.

[Boer98]
J.C. Boer RE RA en J.R.M. Vandecasteele, *De EDP-auditor en de veranderende ICT-organisatie*, Compact 1998/2.

[Boer99]
J.C. Boer RE RA, *ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[Boer00]
J.C. de Boer RE en mw. ir. E.R. van Sommeren RE, *Benchmarking van de general IT-controls in de praktijk*, Compact 2000/2.

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

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

[Giel90]
L.J.M.W. Gielen RI en G.J.P. Swinkels, *Kwaliteitsbeheersing bij systeemontwikkeling*, Compact 1990/2.

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

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

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

[Kort99]
W. de Korte RE RA, *EDP-auditor en jaarrekeningcontrole van vergaand geautomatiseerde organisaties*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[Neis99a]
A.W. Neisingh RE RA, *Van automatisering en controle tot IT-audit*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[Neis99b]
A.W. Neisingh RE RA, *Noodzakelijke assurance over IT*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[Neis99c]
A.W. Neisingh RE RA, *Informatie- en communicatietechnologie en accountants: een verstandshuwelijk?*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[NGI87]
NGI, *EDP Audit Volwassen?*, 1987.

[NIVRA00]
Koninklijk NIVRA, Beleidsnota *Kwaliteit en transparantie*, mei 2000.

[NNI00]
NNI, *Code voor Informatiebeveiliging*, 2000.

[Paan95]
R. Paans, (red.), *Beveiliging in beweging*, Samsom BedrijfsInformatie, Alphen aan den Rijn 1995.

[RAC]
*RAC401: controle in een omgeving waarin gebruik wordt gemaakt van geautomatiseerde informatiesystemen (CIS)*

[Spru00]
M.E.M. Spruit, *ITIL Security Management: een kritische beschouwing*, Compact 2000/4.

[Velt95]
P. Veltman RE RA, *Third party review en -mededeling bij uitbesteding van IT-services*, Compact 1995/3.


*Prof. A.W. Neisingh RE RA* is partner van KPMG Information Risk Management en (deeltijd)hoogleraar Betrouwbaarheidsaspecten geautomatiseerde informatiesystemen aan de Rijksuniversiteit Groningen. Verder is hij al jaren hoofdredacteur van Compact.