Informatie- en communicatie-technologie en accountants: een verstandshuwelijk?

Prof. A.W. Neisingh RE RA

De accountant belast met de controle van de jaarrekening heeft het moeilijk. ICT neemt in omvang en betekenis toe; de accountant kan het niet meer alleen af. Wie beoordeelt wat, waarom en op welk tijdstip? Discussiemogelijkheden te over!

Inleiding

Het gebruik van informatie- en communicatietechnologie (ICT) in organisaties is niet meer weg te denken. Accountants zullen in het kader van de jaarrekeningcontrole bij het definiëren van de controleaanpak rekening moeten houden met de invloed die het gebruik van ICT heeft op de beheersing van de organisatie, dat wil zeggen op de processen en de kwaliteit ervan. Ook de wetgever heeft niet stilgezeten. Op 1 maart 1993 werd de Wet computercriminaliteit van kracht die accountants verplicht – overeenkomstig nieuw BW boek II, artikel 393 lid 4 – hun bevindingen met betrekking tot de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking te rapporteren aan de Raad van Commissarissen en de directie. In de memorie van toelichting is terecht opgemerkt dat hiervan slechts sprake kan zijn ingeval de automatisering in de uitvoering van de controlewerkzaamheden is betrokken. Voor bank- en verzekeringswezen gelden memoranda met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking, uitgegeven door De Nederlandsche Bank, respectievelijk de Verzekeringskamer. In dit artikel zal niet worden ingegaan op deze memoranda en evenmin op het memorandum inzake de Jaar 2000-problematiek.
In dit artikel zal worden stilgestaan bij de situatie waarin de accountant kiest voor een systeemgerichte controleaanpak, dat wil zeggen: de accountant moet voor wat betreft de controle van de bedrijfsprocessen steunen op de kwaliteit van het stelsel van algemene maatregelen van interne controle en beveiliging.

Objecten van onderzoek

De geautomatiseerde bedrijfsprocessen zijn voor hun kwaliteit in belangrijke mate afhankelijk van die van het stelsel van algemene maatregelen. In dit licht kunnen dan ook vier afzonderlijke objecten van onderzoek door de accountant worden gedefinieerd, en wel:

a Het informatiebeveiligingsbeleid
Dit beleid zal slechts marginaal door de accountant worden getoetst. De geformuleerde uitgangspunten vormen de basis voor de kwaliteitsnormen waaraan de ICT moet voldoen.

b De systeemontwikkelings- en onderhoudsorganisatie
Het betreft hier niet de toepassingsprogrammatuur als zodanig, doch de organisatie die deze programmatuur ontwikkelt en onderhoudt. In dit artikel wordt niet uitdrukkelijk ingegaan op de geautomatiseerde informatiesystemen zelf, waarover de accountant – indien deze voor de accountantscontrole van belang zijn – zich een oordeel dient te vormen.

N.B.: Een rol kan voor de accountant zijn weggelegd bij de beoordeling van nieuwe, respectievelijk gewijzigde toepassingen, zowel in geval van door de organisatie ontwikkelde als standaardsoftware. Het is van betekenis dat een voldoende niveau van internecontrole- en beveiligingsmaatregelen aanwezig is en wordt geïmplementeerd, opdat accountantscontrole zo efficiënt mogelijk kan worden uitgevoerd. Een relatie met toekomstige controles (en controlekosten) kan in dat geval worden gelegd.

c Het rekencentrum
Op deze functie, ook wel verwerkings- en transportorganisatie genoemd, zal in dit artikel de nadruk worden gelegd. Het gaat daarbij primair om vast te stellen dat een adequaat stelsel van algemene organisatorische en ICT-maatregelen is geïmplementeerd.

d Calamiteitenopvangplannen
Het belang voor bijna iedere onderneming om bij voortduring te kunnen beschikken over haar geautomatiseerde gegevensverwerking (die zo volstrekt onmisbaar is voor de bedrijfsvoering), staat niet meer ter discussie. Accountants zullen in het kader van de controle van de jaarrekening de toereikendheid van de getroffen maatregelen beoordelen.

Het zal duidelijk zijn dat in een (hoog)geautomatiseerde omgeving waarbij de gegevensverwerking on-line/real-time plaatsvindt en in veel gevallen koppelingen via netwerken met derden bestaan, het niet beschikbaar zijn van de geautomatiseerde gegevensverwerking belangrijke gevolgen voor de continuïteit van de organisatie kan hebben. Uitval van de geautomatiseerde gegevensverwerking gedurende enige dagen kan er zelfs toe leiden dat een organisatie 'out of business' raakt.

De accountant zal over een zodanige kennis met betrekking tot de kwaliteitsaspecten van ICT dienen te beschikken dat hij zich ten minste op hoofdlijnen een beeld moet kunnen vormen van de kwaliteit van het stelsel van alge-

mene maatregelen. In complexe gevallen moet hij zich (indachtig zijn grenzen van deskundigheid) kunnen laten bijstaan door ofwel EDP-auditors, ofwel de accountants die een grotere expertise bezitten op het vakgebied dan de behandelend accountant zelf. In dit artikel zal slechts globaal aandacht worden besteed aan de continuïteitsaspecten van ICT.

In deze beschouwing wordt uitgegaan van (hoog)geautomatiseerde omgevingen; de problematiek is vergelijkbaar voor groot- respectievelijk kleinschalige omgevingen omdat niet de schaalgrootte doch de typologie van de toepassing voor de afhankelijkheid van de kwaliteit van algemene maatregelen bepalend is.

Ontwikkelingen in het gebruik van ICT: gevolgen voor de beheersing van organisatie en procedures

Het gebruik van ICT in organisaties neemt grote vormen aan. Onder invloed van deze ontwikkelingen kiezen organisaties ervoor tot een hoge graad van automatisering in zowel de primaire als secundaire processen te komen en in dat verband computersystemen en netwerken met elkaar te verbinden, waarbij ook grensoverschrijdend ten opzichte van andere organisaties wordt gehandeld. Toepassing van electronic commerce (electronic data interchange), waarbij computers van handelspartners met elkaar zijn verbonden, zorgen voor (nagenoeg) papierloze organisaties. Volledig geautomatiseerde afrekeningen tussen ziekenhuis en zorgverzekeraars zijn al meer regel dan uitzondering en zorgen er bij alle partijen voor dat ook hier het gebruik van externe documenten wordt geminimaliseerd. Zonder bijzondere maatregelen (het opbouwen van een audit trail) vervalt echter een groot deel van registratie en het spoor van transacties en de verwerking ervan. De beheersing van de organisatie kan daardoor ernstig worden verstoord.

Een kwalitatief toereikend stelsel van algemene maatregelen dient permanent in de organisatie te zijn geïmplementeerd, opdat de beheersingsmogelijkheden adequaat blijven en de gebruikersorganisatie op deze kwaliteit kan steunen. Immers, ongeacht controlebreuken in applicatieprogrammatuur en dus in de toepassingscontroles, moeten gebruikers en controleurs ervan kunnen uitgaan dat juiste versies van programmatuur en bestanden worden gebruikt.

Niettemin dienen in geautomatiseerde informatiesystemen alsmede in de gebruikersorganisatie, die immers verantwoordelijk is voor de gegevens (integriteit, volledigheid) en de programmatuur (zij is eigenaar), voldoende maatregelen van interne controle en beveiliging te zijn getroffen. De basis voor een betrouwbare registratie komt dan te liggen in het stelsel van algemene maatregelen van interne controle en beveiliging, de general ICT controls.

Bij voortgaande integratie en het verdwijnen van controleerbare vastleggingen dient die gebruiker juist dan met zekerheid te weten dat ook tabellen, rekenregels en dergelijke bij voortduring werken zoals die oorspronkelijk zijn geïmplementeerd. De gebruiker zal een belangrijke rol moeten vervullen in de test-, acceptatie- en overdrachtsprocedure. Deze gebruiker stelt immers vast dat de opgeleverde functionaliteit overeenkomt met de gedefinieerde eisen. Vervolgens moet de gebruiker zeker zijn van het feit dat de door hem geteste en geaccepteerde programmatuur ook daadwerkelijk in productie wordt genomen en ongewijzigd voor hem beschikbaar is. En blijft!

Nu de gebruiker zal moeten steunen op de goede kwaliteit van de general ICT controls, zal deze zich op enigerlei wijze moeten overtuigen van de kwaliteit van het geïmplementeerde stelsel van algemene maatregelen om er zeker van te zijn dat de geautomatiseerde gegevensverwerking voldoet aan de door de gebruikersorganisatie gestelde eisen.
Ongeacht hoe de afspraken met de ICT-organisatie zijn gemaakt (bijvoorbeeld door met hen een service level agreement af te sluiten), de gebruikersorganisatie blijft verantwoordelijk voor een betrouwbare en binnen de gestelde eisen continu beschikbare geautomatiseerde gegevensverwerking. Dit geldt overigens ook in geval van outsourcing van ICT.

Een informatiebeleid is voorwaardenscheppend met betrekking tot de kwaliteit van het stelsel van algemene maatregelen. Immers, de op strategisch niveau gedefinieerde uitgangspunten dienen op tactisch niveau (Code voor Informatiebeveiliging) te worden uitgewerkt en vervolgens te worden geïmplementeerd (operationeel niveau). Indien zo'n beleid niet is gedefinieerd, zal niettemin een normenkader moeten worden gedefinieerd. Echter, in dat geval door de gebruikersorganisatie zelf, die de werkelijkheid zal moeten toetsen om na te gaan of zij daadwerkelijk kan steunen op de kwaliteit van het stelsel van algemene maatregelen. Deze algemene maatregelen kunnen in drie categorieën worden ondergebracht, namelijk in maatregelen van organisatorische, logische en fysieke aard.

Maatregelen van organisatorische aard betreffen zaken als functiescheidingen, procedures, richtlijnen en voorschriften met betrekking tot de automatisering en de ontwikkeling van systemen; fysieke maatregelen zijn gericht op de bescherming van de geautomatiseerde gegevensverwerking tegen incidenten en calamiteiten, waarbij moet worden gedacht aan het aanhouden van back-ups, brand-, rook- en waterdetectieapparatuur, blusmiddelen en het beveiligen van het computercentrum tegen ongeautoriseerde toegang. De logische beveiligingsmaatregelen ten slotte hebben betrekking op de wijze waarop de toegang tot programmatuur en gegevens is beveiligd. Juist in on-line/real-time-omgevingen is de kwaliteit van de implementatie van de logische beveiliging alsmede het beheer van de bevoegdheden van cruciale betekenis. De in organisaties getroffen functiescheidingen, procedures en dergelijke, dienen te worden verankerd in het systeem van logische toegangsbeveiliging, waardoor wordt gewaarborgd dat de geïmplementeerde bevoegdheidsregelingen bij voortduring ongewijzigd van kracht blijven, behoudens geautomatiseerde aanpassingen.

In feite blijkt uit deze korte weergave dat de kwaliteit van de geautomatiseerde informatieverzorging in belangrijke mate afhangt van de deugdelijkheid van de ont-

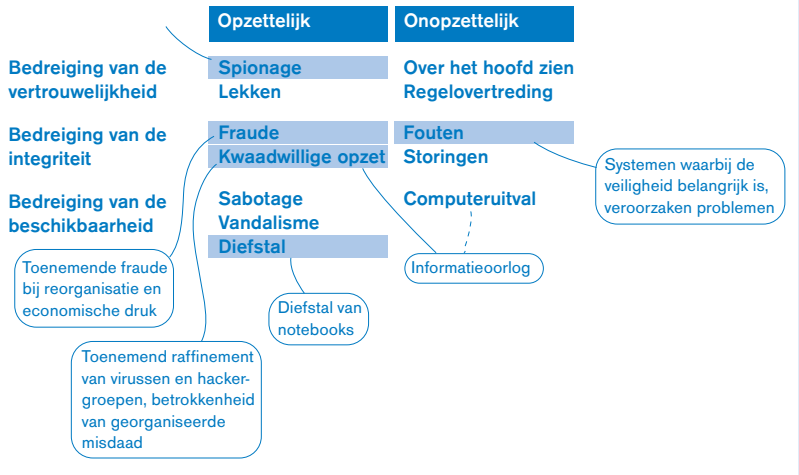
wikkelingsorganisatie, test-, acceptatie- en overdrachtsprocedure, het beheer van programmatuurbibliotheken, de kwaliteit van het systeem van logische toegangsbeveiliging en dergelijke.

Een bijzondere problematiek doet zich voor wanneer in organisaties gebruik wordt gemaakt van één of meer middelgrote (midrange) computersystemen. Bedoeld zijn computersystemen waarbij een minimale bezetting aan mankracht noodzakelijk is om de geautomatiseerde gegevensverwerking te laten plaatsvinden. Als onderdeel van het besturingssysteem van de computer is over het algemeen een toegangscontrolesysteem beschikbaar, waarbij de overall bevoegdheid ten aanzien van beheersing en controle van het computersysteem wordt toebedeeld aan een zogenaamde security-officerfunctie. Deze security-officerfunctie dient nimmer direct betrokken te zijn bij ontwikkeling en/of de operationele gegevensverwerking of rechtstreeks verantwoordelijk te zijn voor enig deel van de gebruikersorganisatie. Deze functie is namelijk in staat het gehele systeem naar z'n hand te zetten. Overigens zij hier opgemerkt dat het inbedden van deze securityfunctie in de organisatie eenvoudiger is gezegd dan gedaan. In kleinere organisaties zal de security-officerfunctie vaak zelfs maar een nevenfunctie zijn van de 'almachtige' systeembeheerder; voorwaar een verder complicerende factor.

Accountantscontrole in een (hoog)geautomatiseerde omgeving

In deze paragraaf zal aandacht worden besteed aan de invloed van gebruik van ICT op de accountantscontrole. In de hiervoor geschetste situatie rest de accountant belast met de controle van de jaarrekening niets anders dan bij voortduring te steunen op de kwaliteit van de stelsels van maatregelen, alsmede de handhaving en naleving van de getroffen stelsels.
Deze situatie doet zich bijvoorbeeld voor, indien het direct verband tussen de invoer van gegevens en de uitvoer van de verwerking ontbreekt (ten gevolge van de aard van het systeem, de typologie van de onderneming, e.d. – eerder als 'controlebreuk' aangeduid) of indien de organisatie en ook de accountant gebruik moeten maken van uitkomsten uit het systeem (ten gevolge van het gebruik van tabellen en rekenregels) en het niet (eenvoudig) mogelijk is via totaal- en/of verbandscontroles de juistheid en volledigheid van de verwerking vast te stellen.

Figuur 1. Aansluiting accountantscontrole met theorie.



De accountant zal zich moeten realiseren, dat – ongeacht wat hij doet – in meerdere of mindere mate zal worden gesteund op de goede werking van de ICT-organisatie, de daarin verankerende maatregelen van interne controle en beveiliging, alsmede op de maatregelen in de toepassingsprogrammatuur. Probleem is nu dat de 'interne controle' object van onderzoek is geworden!
Er staat de accountant een aantal dingen te doen. Allereerst zal hij zich een oordeel moeten vormen over de kwaliteit van de stelsels van maatregelen van interne controle en beveiliging zoals deze in de voor hem van belang zijnde toepassingsprogrammatuur zijn geïmplementeerd. Zo'n onderzoek zal zich richten op de zogenaamde application controls, dat wil zeggen de in de gebruikersorganisatie geïmplementeerde maatregelen (user controls) en de in het geautomatiseerde deel van het informatieverwerkende systeem opgenomen maatregelen (programmed procedures), afzonderlijk en in samenhang tot elkaar. Op grond van deze beoordeling kan de accountant zich een oordeel vormen in hoeverre sprake is van een adequaat stelsel van controlemaatregelen. Hierbij dient in ogenschouw te worden genomen dat leemten in dat stelsel kunnen bestaan omdat het directe verband tussen in het geautomatiseerde systeem ingevoerde gegevens en de uitvoer ervan niet zonder meer vaststaat. Wel blijkt uit dit onderzoek in welke mate op de geprogrammeerde controles moet worden gesteund. Met andere woorden, hoe kritisch het vaststellen van (goede) opzet en bestaan enerzijds en handhaving en naleving van general ICT controls anderzijds is voor het totaalbeeld (kwaliteit) van de interne controle en beveiliging voor de accountant. Aan de aanpak van zo'n systeembeoordeling wordt in deze context geen aandacht besteed. De samenhang van de verschillende onderwerpen blijkt uit figuur 1.

Vervolgens zal de aandacht zich richten op het stelsel van algemene maatregelen van interne controle en beveiliging, dat wil zeggen de general ICT controls. Een eerste oriëntatie met betrekking tot de kwaliteit ervan kan plaatsvinden door het uitvoeren van een doorlichting op hoofdlijnen van de maatregelen van organisatorische, logische en fysieke aard. Bedacht dient overigens te worden dat de accountant voorafgaand daaraan de normen moet definiëren, waaraan hij de uitkomsten wenst te toetsen. Om iedere discussie te vermijden is het verstandig vooraf de geformuleerde toetsingsnormen aan de directie voor te leggen en op dit punt overeenstemming te bereiken. In de rapportage aan het management zal – ingeval geen informatiebeveiligingsbeleid is vastgelegd – worden opgenomen dat de tijd is gekomen zo'n beleid te formuleren. Wanneer een informatiebeveiligingsbeleid wel is gedefinieerd, zal de accountant dat beleid ten minste marginaal toetsen.

De uitkomst van de doorlichting op hoofdlijnen in de hier beschreven context geeft richting aan nader onderzoek op deelgebieden van de beheersing en beveiliging van de geautomatiseerde informatievoorziening. Van belang is vast te stellen dat de functie- en taakverdeling

binnen de organisatie is verankerd in het toegangscontrolesysteem en dat dit op een correcte wijze is geïmplementeerd. Verder geldt dat de accountant zich een oordeel zal moeten vormen over de kwaliteit van test-, acceptatie- en overdrachtsprocedure, het bibliotheekbeheer en dergelijke.

Voor wat de beschikbaarheidsproblematiek betreft zal het onderzoek zich richten op het al dan niet voorhanden zijn van voorzieningen van computeruitwijk, het aanhouden van kopieën van bestanden, besturingssystemen en toepassingsprogrammatuur ook op een externe locatie, het voorhanden hebben van een actueel en getest noodvoorzieningenplan en dergelijke. Vanzelfsprekend zal deze beoordeling plaatsvinden in het licht van de oordeelsvorming over de kwaliteit van de organisatorische en fysieke beveiliging ter zake van ICT.

Op dit punt aangekomen zal blijken dat de kennis en ervaring van de accountant belast met de controle van de jaarrekening op dit terrein tekortschiet. De ondersteuning door een EDP-auditor zal zonder meer noodzakelijk zijn om de kwaliteit te leveren die nodig is om de accountantscontrole naar de huidige maatstaven te kunnen uitvoeren.
Een afzonderlijk probleem ontstaat wanneer het stelsel van algemene maatregelen niet geheel voldoet aan daaraan redelijkerwijze te stellen eisen, terwijl de accountant op grond van allerhande overwegingen (zie hiervoor) toch op dat stelsel moet steunen ter uitvoering van een efficiënte en volkomen controle van de jaarrekening. Op deze situatie zal thans niet worden ingegaan.

De toereikendheid van de opzet van de stelsels van controle- en beveiligingsmaatregelen (in applicaties en in de ICT-infrastructuur) wil nog niet zeggen dat deze ook in continuïteit worden gehandhaafd en nageleefd. Voor wat betreft veranderingen in de 'opzet' zal de accountant zich periodiek moeten laten informeren door het (ICT-) management.
De accountant zal zich – in navolging van de gebruiker – moeten overtuigen van de goede werking van de stelsels om er zeker van te zijn dat in continuïteit op deze stelsels kan worden gesteund. In deze toch niet eenvoudige omstandigheden zal de accountant een beroep moeten doen op EDP-auditors, immers evidence zal moeten worden verkregen ten aanzien van het functioneren van deze stelsels.

Van grote betekenis is vast te stellen of de EDP-auditor uit vaktechnische en/of efficiencyoverwegingen de controle geheel zelfstandig zal moeten uitvoeren, dan wel inzet van een internecontrolefunctie in de organisatie zal vereisen. Deze IC-functie fungeert primair voor de gebruikersorganisatie. Wanneer op dag-, week- en maandbasis een grote hoeveelheid controlewerkzaamheden ter vaststelling van de handhaving en naleving (werking) dient te worden uitgevoerd op de ICT-organisatie, is het praktisch niet haalbaar dit door de EDP-auditor (die de accountant ondersteunt) te laten uitvoeren. In geval van inschakeling van een internecontrolefunctie kan de EDP-auditor in principe volstaan met kennisnemen van dossiers inzake de uitvoering van de werkzaamheden en het met lagere frequentie zelfstandig uitvoeren van vergelijkbare werkzaamheden.

Mocht vorenstaande benadering niet noodzakelijk zijn (i.c. inschakeling IC-functie), dan dient te worden bepaald met welke frequentie en in welke omvang controlewerkzaamheden dienen te worden uitgevoerd opdat de accountant een voldoende basis heeft om te steunen op de kwaliteit van de general ICT controls en de in de toepassingsprogrammatuur opgenomen programmed procedures (controls). Duidelijk wordt dat de EDP-auditor ten gevolge van deze problematiek een geïntegreerd onderdeel zal dienen uit te maken van de controleploeg.

De EDP-auditor onmisbaar

De beleidslijn van accountants belast met de controle van de jaarrekening zou moeten zijn dat geautomatiseerde informatieverzorgende systemen in principe worden beoordeeld door de controlestaf. Ten gevolge van de toegepaste ICT en de voortdurende ontwikkelingen daarin, blijkt de daarvoor noodzakelijke kennis bij de controlerend accountant niet altijd in voldoende mate aanwezig. Enerzijds omdat hij nooit echt ervaren wordt in systeemonderzoeken, zeker niet indien sprake is van technisch complexe systemen en anderzijds ten gevolge van de onmogelijkheid de ontwikkelingen op alle fronten bij te houden. Gecontroleerden zijn nu eenmaal allen uniek, zodat ieder voor een ander hardware-/softwareplatform heeft gekozen met voorzover niet kan worden beschikt over standaardprogrammatuur, eigen specifieke toepassingen. Een beroep op uitvoering van systeembeoordelingen door EDP-auditors is dan niet slechts efficiënt doch vaktechnisch zeer verantwoord.

Inschakeling van EDP-auditors is niet langer facultatief.

Dezelfde redenering gaat in nog sterkere mate op voor de beoordeling van de general ICT controls. Vanuit de opleiding zal de algemene accountant een brede algemene kennis ter zake hebben; in de beginjaren van zijn opereren zal hij deze kennis kunnen uitbreiden, respectievelijk zich er verder in verdiepen. Daarna zal hij zijn belangstelling ten gevolge van de ontwikkelingen in het accountantsberoep als geheel (externe verslaggeving, fiscale zaken, e.d.) moeten verdelen; uit de praktijk blijkt dat ICT slechts zelden een hoge prioriteit heeft. Er zijn slechts weinigen die zich als registeraccountant nog verder specialiseren tot (Register) EDP-auditor.

Overigens is de inzet van specialisten, in het onderhavige geval van EDP-auditors, niet uniek. Door toenemende complexiteit van de materie zijn historisch gezien specialisaties ontstaan (vergelijk actuarissen, fiscalisten en anderen). Voor wat betreft de EDP-auditor heeft dit nu betrekking op het terrein van de administratieve organisatie en interne controle, in het bijzonder als gevolg van complexe ICT. Voor de uitvoering van de controlewerkzaamheden betekent de ontwikkeling waarbij EDP-auditors steeds verdergaand een integrerend onderdeel uitmaken van de jaarrekeningcontrole, dat een wezenlijk budget ten behoeve van hun werkzaamheden beschikbaar zal moeten worden gesteld. Immers, systeemonder-

zoeken in een complexe situatie zullen over het algemeen door EDP-auditors worden uitgevoerd. Hetzelfde geldt voor de beoordeling van de kwaliteit van de general ICT controls. De omvang van de 'normale' controlewerkzaamheden zal afnemen ten gunste van de EDP-auditor. Per slot van rekening zal moeten worden gesteund op de goede kwaliteit en de handhaving en naleving van de general ICT controls en van de operationele informatiesystemen.

Wil de accountant in de controlerende functie zijn positie in controles waar sprake is van complexe ICT behouden, dan zal hij kennis moeten verwerven over de ontwikkelingen op het gebied van ICT en de invloed die deze hebben op de beheersing van de organisatie en op de controle van de jaarrekening. Anders verliest de accountant de mogelijkheid de EDP-auditor in een voor de controle relevante richting aan te sturen.

Tot slot: verhoging kwaliteit van de controle

In grote lijnen kan het werk van de accountant belast met de controle van de jaarrekening worden opgedeeld in een aantal logisch bij elkaar behorende elementen. Vanzelfsprekend begint het proces met het plannen van de audit, waarin begrepen achtereenvolgens de beoordeling van de administratieve organisatie en het stelsel van maatregelen van interne controle, alsmede het vervolgens uitvoeren van specifieke controlewerkzaamheden, opdat een oordeel over de getrouwheid van de jaarrekening kan worden verkregen. Verder is sprake van werkzaamheden op het gebied van presentatie, waardering en fiscale aangelegenheden.

In dit artikel is aangegeven dat voor wat betreft de beoordeling van de geautomatiseerde informatiesystemen, inclusief de maatregelen getroffen in de betrokken gebruikersorganisatie, deze over het algemeen zal kunnen worden uitgevoerd door de algemeen accountant; echter, ingeval sprake is van ingewikkelde toepassingen (te denken valt hierbij aan on-line/real-time-systemen, het gebruik van databasemanagementsystemen, e.d.) zal de beoordeling door specialisten moeten plaatsvinden. Vanzelfsprekend komen EDP-auditors hiervoor in aanmerking. Doch ook accountants die gedurende enkele jaren een verdergaande training en opleiding op het gebied van de EDP-auditing hebben gehad en als zodanig ten minste drie jaren onderdeel hebben uitgemaakt van de EDP-auditorsorganisatie, zijn als terzakekundig aan te merken. Een niet te onderschatten deel van het werk zal betrekking hebben op het vaststellen dat de kwaliteit van de ICT-organisatie aan daaraan redelijkerwijze te stellen eisen voldoet en verder het in continuïteit vaststellen dat het beoordeelde stelsel van algemene maatregelen gedurende het jaar ook daadwerkelijk is gehandhaafd en nageleefd.

Voor het maken van een schatting van de benodigde inspanning, in uren uitgedrukt en gerubriceerd naar de kwaliteit van EDP-auditors, zal empirisch onderzoek moeten plaatsvinden. Het zal evenwel duidelijk zijn dat de omvang van de werkzaamheden van EDP-auditors bij de uitvoering van jaarrekeningcontrole beduidend zal moeten toenemen. Het is derhalve niet uitgesloten dat in situaties waarin sprake is van een 'perfecte' kwaliteit van de geautomatiseerde informatieverzorging, de controlewerkzaamheden op een geheel andere wijze zullen worden 'ingevuld'.

De vraag die vervolgens beantwoord zou moeten worden, is hoe lang het nog verantwoord is dat de algemeen accountant het primaat heeft de jaarrekening te controleren van bedrijven die in zo vergaande mate afhankelijk zijn van de kwaliteit van de geautomatiseerde gegevensverwerking en waarbij de rol van de EDP-auditor groot tot zeer groot is geworden, terwijl zijn oordeel in voorkomende gevallen nogal eens van ondergeschikt belang wordt gevonden.
Deze vraag behoeft nu nog niet beantwoord te worden, doch leent zich voor indringende discussie...

Literatuur

[Boer94]
J.C. Boer RE RA, *De invloed van informatietechnologie op de interne controleprincipes*, Compact 1994/4.

[Fijn93]
Drs. R.G.A. Fijneman RE RA, *Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving*, Compact 1993/4.

[Frie93]
Prof.dr. A.B. Frielink RA en prof. H.J. de Heer RA, *Leerboek Accountantscontrole*, deel 3b: Capita selecta, Stenfert Kroese, Leiden-Antwerpen, 1993.

[Gils94]
Drs. H.G.Th. van Gils, *Informatiebeveiliging: de tijd is rijp*, Compact 1994/1.

[Jonk94]
R.A. Jonker RA, *Geautomatiseerde gegevensbewerking en accountantscontrole*, Compact 1994/4.

[Koed96]
Mw. M.J.A. Koedijk RA en mw. W.A. de Munck-Kraamer RA, *System Review Services*, Compact 1996/3.

[Neis94]
Prof. A.W. Neisingh RE RA, *De invloed van IT op de beheersing van organisaties*, Compact 1994/1.

[NIVR]
Koninklijk NIVRA, Richtlijn 622, *Samenwerking tussen accountant en EDP-auditor ter zake van de controle van een verantwoording.*

[NIVR95]
Koninklijk NIVRA, Studierapport: *Normatieve maatregelen voor de geautomatiseerde gegevensverwerking.*

[Paan93]
Prof.dr.ir. R. Paans RE, *Beveiligingsstandaard voor informatiesystemen*, Compact 1993/2.

[Praa]
J. van Praat en H. Suerink, *Inleiding EDP-auditing, kwaliteitscontrole en beveiliging van informatiesystemen.*

[Velt91]
Drs. P. Veltman RE RA, *Systemen voor logische toegangsbeveiliging*, Compact 1991/4.