COMPACT

TIJDSCHRIFT EDP-AUDITING

ACCOUNTANTSCONTROLE EN ICT

1998/3

KPMG EDP Auditors

Bezoekadres
Beneluxlaan 43
3526 KK Utrecht

Correspondentie-adres
Postbus 3222
3502 GE Utrecht

Telefoon (030)2810210
Telefax (030)2896714

KPMG Peat Marwick LLP
Mr R. Koorn
Victoria Street 685
CA 94127 San Francisco
USA

Utrecht, 31 juli 1998

Onderwerp: **Compact 1998/3: Accountantscontrole en EDP-audit**

Geachte heer Koorn,

Zoals gebruikelijk wordt ieder jaar in het derde nummer van Compact aandacht besteed aan accountantscontrole en EDP-audit. In de loop der jaren zijn artikelen verschenen inzake bijvoorbeeld System Review Services ofwel een aanpak voor systeembeoordeling, IT Benchmarking en dergelijke. In dit nummer treft u bijdragen aan van vijf auteurs, waarbij de externe auteurs ingaan op:

- "Het beheersen van risico's op het gebied van informatiebeveiliging: de visie van een klant" van de hand van mr. P. van Dijken;
- "Accountantscontrole, COSO en CobiT" van de hand van mevrouw drs. A.J.M Koopman.

In het laatste artikel wordt met name ingegaan op de bruikbaarheid van CobiT voor de beoordeling van de beheersing van de IT in het kader van de moderne controleaanpak ten behoeve van de jaarrekeningcontrole.

Drie auteurs van KEA-huize besteden achtereenvolgens aandacht aan:

- "Informatie- en communicatietechnologie en accountants: een verstandshuwelijk?", door prof. A.W. Neisingh RE RA;
- "EDP-auditor en jaarrekeningcontrole van vergaand geautomatiseerde organisaties", door W. de Korte RE RA;
- "ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking", door J.C. Boer RE RA.

Zoals al uit de titels blijkt, behandelen de auteurs de problematiek vanuit verschillende invalshoeken, echter, enige verschillen van inzicht laten zij niet ongenoemd. Ook voor u geldt dat de redactie van Compact de rubrieken van het tijdschrift gaarne beschikbaar stelt voor reacties op de artikelen.

Wij vertrouwen erop dat wij u met toezending van dit nummer van Compact een genoegen doen en wensen u in ieder geval naast leesplezier een prettige vakantie.

Hoogachtend,

Jo-Ann

J.C. Boer

Bijlage: Compact 1998/3

Compact ®
Jaargang 25, nummer 3
Een uitgave van KPMG EDP Auditors NV en ten Hagen & Stam BV.
Het blad verschijnt 6 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
Drs. P.P.M.G.G. Brouwers RE RA
Ir. J.A.M. Donkers RE
W. de Korte RE RA
J.C. van Praat RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Mr. P. van Dijken
G. van Essen RA
Prof.mr. H. Franken
Dr. K.IJ. Mollema RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Uitgeefassistent
C.M.A. van Houtum, ten Hagen & Stam, Postbus 34, 2501 AG Den Haag
Tel.: 070 – 304 57 52
Fax: 070 – 304 58 17
e-mail: c.houtum@wkths.nl
Basisvormgeving
Bureau Karakter, Delft
Opmaak
AlphaZet bv, Waddinxveen
Abonnementen
f 165,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Studentenabonnement f 95,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
Abonnementsadministratie
Samsom BedrijfsInformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 800
Fax : 0172 – 475 933
Adreswijzigingen – ook tijdelijke – moeten minstens 8 weken voor de verschijningsdatum bekend zijn.
Overname artikelen
Het overnemen en vermenigvuldigen van artikelen en berichten is slechts geoorloofd na schriftelijke toestemming van de uitgever.
Overdrukken artikelen
Overdrukken van artikelen kunnen worden aangevraagd bij de uitgeefassistent. Prijs per overdruk per artikel (inclusief omslag) f 5,-.

Uitgever
I.J. van Haren

Nederlands Uitgeversverbond
Groep vaktijdschriften

ISSN 0920 – 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals:
• beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacywetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor IT-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG, KPMG EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij ten Hagen & Stam BV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij de uitgeefassistent verkrijgbaar is.

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.

In het eerste artikel wordt de problematiek van de ICT in de jaarrekeningcontrole met betrekking tot routinematige transactieverwerking benaderd vanuit management control. De accountant zal bij routinematige transacties doorgaans een systeemgerichte controleaanpak toepassen. Het begrip systeem wordt hierbij ruim opgevat, hetgeen inhoudt dat dit begrip uit drie componenten bestaat: menselijke handelingen en verdeling van verantwoordelijkheden, de geautomatiseerde informatiesystemen en de technische infrastructuur. De componenten moeten in onderlinge samenhang worden beoordeeld. Vanuit management control wordt gesteld dat de accountant niet zelfstandig de werking van de general ICT controls hoeft te beoordelen; hij mag hierbij steunen op het stelsel van management control dat aanwezig is binnen de organisatie van de gecontroleerde.

In het tweede artikel wordt ingegaan op de aanpak welke de accountant zal volgen voor wat betreft de controle van de bedrijfsprocessen, zodat hij kan steunen op het stelsel van algemene maatregelen en beveiliging, alsmede op de maatregelen in de toepassingsprogrammatuur. Centraal staat hierbij het feit dat de gebruiker zal moeten steunen op de goede kwaliteit van de general ICT controls. De kwaliteit van geautomatiseerde informatieverzorging hangt in belangrijke mate af van de deugdelijkheid van de ontwikkelorganisatie, test-, acceptatie- en overdrachtsprocedures, het beheer van programmabibliotheken, de kwaliteit van het systeem van logische toegangsbeveiliging en dergelijke. De accountant zal de kwaliteit hiervan dienen te toetsen. Gesteld wordt dat de werking van de general ICT controls dient te worden getoetst teneinde te kunnen steunen op de maatregelen in de toepassingsprogrammatuur. Hierbij kan eventueel gebruik worden gemaakt van de werkzaamheden van de internecontrolefunctie in de organisatie. De beoordeling van de general ICT controls zal vanwege de noodzakelijke specifieke deskundigheid veelal verricht dienen te worden door een EDP-auditor. De rol van de EDP-auditor in de jaarrekeningcontrole zal in de toekomst toenemen, derhalve zullen EDP-auditors steeds vaker een geïntegreerd deel vormen van de controleploeg. Voorop staat hierbij dat accountants over voldoende kennis op het gebied van ICT dienen te beschikken om de EDP-auditor adequaat aan te kunnen sturen.

Het derde artikel gaat in op de vraag of de EDP-auditor op vaktechnisch verantwoorde wijze een uitspraak kan doen over de uitkomsten van informatiesystemen op de saldibalans. Deze vraag kan zich voordoen bij organisaties die vergaand zijn geautomatiseerd. De accountant zal vanwege het ontbreken van brondocumenten en de onzichtbare relatie tussen invoer en uitvoer van transacties dienen te steunen op de maatregelen welke zijn getroffen in de ICT-organisatie en de toepassingsprogrammatuur. Vervangende controles zijn er nagenoeg niet of zijn niet voorhanden. De uitspraak van de EDP-auditor zal derhalve in hoge mate de accountantsverklaring beïnvloeden. Beschreven wordt op welke wijze de EDP-auditor een deugdelijke grondslag kan verkrijgen voor een uitspraak over de betrouwbaarheid van de gegevens op de saldibalans.

In het vierde artikel wordt een beschrijving gegeven van de toepassing van de Code voor Informatiebeveiliging in ICT-organisaties. Hierbij wordt in de aanvulling aangegeven wat de Code van Informatiebeveiliging kan betekenen voor de jaarrekeningcontrole.

In het vijfde artikel wordt de relatie tussen de accountantscontrole, COSO en CobiT weergegeven. CobiT kan als hulpmiddel worden toegepast voor de beoordeling van de beheersing van de ICT in het kader van een moderne controleaanpak ten behoeve van een jaarrekeningcontrole door de accountant. Tussen de werkwijze binnen CobiT en de jaarrekeningcontrole bestaat een grote overeenkomst. COSO geeft praktische handreikingen voor een moderne controleaanpak.

De opgenomen artikelen zullen volgens de redactie voldoende stof bieden voor de discussie over de rol van de EDP-auditor in de jaarrekeningcontrole. EDP-auditors zullen zeker in situaties van vergaande automatisering hun rol kunnen vervullen. De discussie over de rol van de EDP-auditors in de jaarrekeningcontrole is, zoals uit de artikelen blijkt, echter nog zeker niet uitgekristalliseerd.

De redactie wenst de lezer veel plezier en succes met het toepassen van de vrucht van deze beschouwing in zijn of haar praktijk.

W. de Korte RE RA

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.

Accountant let op uw saeck.

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 algemene 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 ontwikkelingsorganisatie, 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 overallbevoegdheid 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.

Interne controle is object van onderzoek.

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.

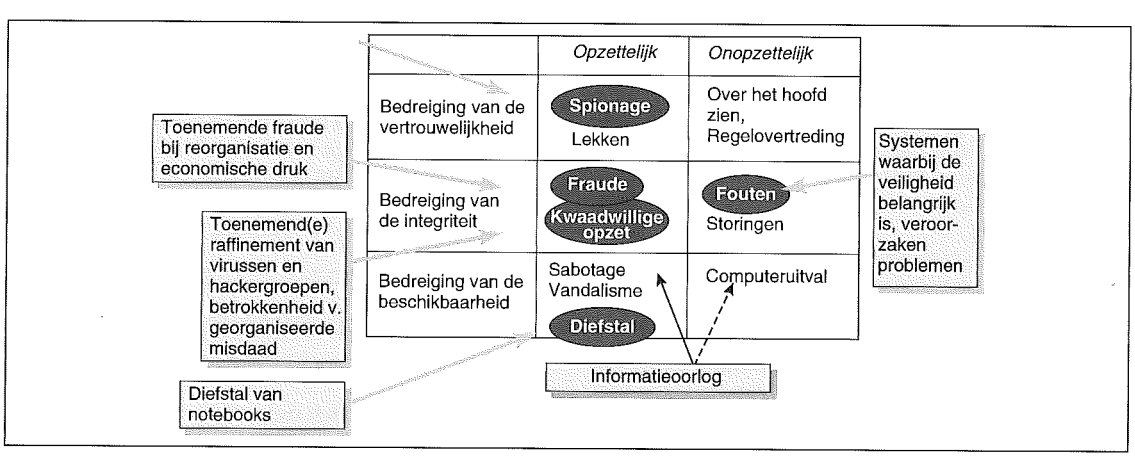
De uitkomst van de doorlichting op hoofdlijnen in de hier beschreven context geeft richting aan nader onderzoek op deelgebieden van de beheersing en beveiliging van de geautomatiseerde informatievoorziening. Van belang is vast te stellen dat de functie- en taakverdeling binnen de organisatie is verankerd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



Figuur 1. Aansluiting accountantscontrole met theorie.

geleefd. 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 efficiency-overwegingen 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 terzake 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, systeemonderzoeken 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 zich 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

Prof. A.W. Neisingh RE RA Is directeur van KPMG EDP Auditors N.V. en deeltijd hoogleraar aan de Rijksuniversiteit Groningen, Leerstoel betrouwbaarheidsaspecten geautomatiseerde informatiesystemen.

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 terzake kundig 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.

EDP-audit betekent toegevoegde waarde in controleproces.

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

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

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

[Jonk94] R.A. Jonker RA, *Geautomatiseerde gegevensbewerking en accountantscontrole*, Compact 94/4.

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

[Gils94] Drs. H.G.Th. van Gils, *Informatiebeveiliging: de tijd is rijp*, Compact 94/1.

[Neis94] Prof. A.W. Neisingh RE RA, *De invloed van IT op de beheersing van organisaties*, Compact 94/1.

[Fijn93] Drs. R.G.A. Fijneman RE RA, *Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving*, Compact 93/4.

[Paan93] Prof.dr.ir. R. Paans RE, *Beveiligingsstandaard voor informatiesystemen*, Compact 93/2.

[VElt91] Drs. P. Veltman RE RA, *Systemen voor logische toegangsbeveiliging*; Compact 91/4.

[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.*

[Koed96] Mw. M.J.A. Koedijk RA en mw. W.A. de Munck-Kraamer RA, *System Review Services*, Compact 96/3.

ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking

J.C. Boer RE RA

In organisaties van enige omvang is de verwerking van routinematige transacties een in hoge mate geautomatiseerd proces. Deze inleiding geeft een visie op de mate waarmee en de wijze waarop de accountant systeembeoordelingen en onderzoeken van de algemene computercontroles in zijn werkzaamheden moet betrekken.

INLEIDING

De werkzaamheden die nodig zijn voor de controle van de jaarrekening zijn van velerlei aard. Voor de planning van de werkzaamheden wordt veelal een onderscheid gemaakt tussen controlewerkzaamheden gericht op het verwerkingsproces van de routinematige transacties en de werkzaamheden gericht op de samenstelling van de jaarrekening. Dit artikel behandelt de accountantswerkzaamheden gericht op het vaststellen van de betrouwbaarheid van de routinematige transactieverwerking.

In organisaties van enige omvang is de verwerking van routinematige transacties een, in hoge mate, geautomatiseerd proces. In de ogen van de auteur ontbreekt het echter aan een sluitende theorie die een basis legt voor de mate waarin en de wijze waarop in de accountantscontrole van de routinematige processen, de gebruikte informatietechnologie (IT) moet worden betrokken. In dit artikel wordt een aanzet gegeven voor een sluitende theorievorming. Tevens is de intentie een basis te leggen voor een praktisch werkkader voor collega's die bij de uitvoering van hun werkzaamheden met dit vraagstuk worden geconfronteerd.

DRIE SYSTEEMCOMPONENTEN

De verwerking van de financiële en logistieke transactiestromen kenmerkt zich door een vaste systematiek die zich over het algemeen bij uitstek leent voor een systeemgerichte controlebenadering. Het begrip systeem moet hierbij ruim worden opgevat en bestaat uit de volgende componenten:

- de menselijke handelingen en verdeling van de verantwoordelijkheden;
- de geautomatiseerde informatiesystemen;
- de technische infrastructuur.

De wijze waarop de drie componenten afzonderlijk moeten worden beoordeeld, is in theorie en praktijk in ruime mate uitgewerkt. De inrichting van organisaties is een vraagstuk dat wordt behandeld in de literatuur met betrekking tot de administratieve organisatie. Over de opzet van internecontrolefunctionaliteiten in informatiesystemen is slechts in beperkte mate specifieke literatuur aanwezig. Door het belang dat managers hechten aan een goede controlestructuur is in de praktijk waar te nemen dat interne controle en beveiliging in implementatietrajecten als één van de randvoorwaarden worden meegenomen. Met betrekking tot de wijze waarop systemen beoordeeld kunnen worden, is een scala van methoden beschikbaar. Ook de inrichting en de beoordeling van de interne controle en beveiligingsmaatregelen in de technische infrastructuur en de daarmee verbonden administratieve organisatie zijn ruimschoots uitgewerkt.

Op het punt van vaststellen van de betrouwbaarheid van ICT is redeneren vanuit de gebruikersomgeving logischer dan vanuit de verwerkingsomgeving.

De drie genoemde gebieden worden bij het inrichten van een audit veelal als losstaand beschouwd. De eerste systeemcomponent 'menselijke handelingen en verdeling van de verantwoordelijkheden' is een gebied dat door alle accountants kan worden afgedekt. In veel situaties is dit niet voldoende om tot een oordeel over de beheersing van de verwerking van de routinematige transacties te komen. Voor een effectieve controle zullen ook de relevante informatiesystemen en de technische infrastructuur in de beoordeling moeten worden betrokken. Wat betreft de wijze waarop dit moet worden opgepakt, wijzen accountants en IT-auditors naar elkaar zonder tot een realistisch en algemeen aanvaard werkprotocol te komen. In het *Handboek EDP Auditing* en het *Handboek Accountancy* vindt u over dit onderwerp (nog) geen artikel, in het boek *IT Auditing* van Van Biene-Hershey wordt aangegeven dat het de verantwoordelijkheid van de financial auditor is te bepalen welke IT-auditwerkzaamheden noodzakelijk zijn; verdere richtlijnen ontbreken. Ook in CobiT is niets opgenomen over de wijze waarop de objectives en audit guidelines kunnen bijdragen aan een oordeel over de betrouwbaarheid van het bovenliggende informatieverwerkende proces. Het NIVRA-studierapport 'Normatieve maatregelen voor de geautomatiseerde gegevensverwerking' handelt over de samenhang, maar er wordt aan de oplossing een uitwerking gegeven die niet aansluit op de dagelijkse praktijk. Helaas heeft het studierapport niet geleid tot de discussie die de samenstellers van het rapport hadden willen initiëren.

SAMENHANG

Tot nu toe zijn publicaties met betrekking tot de betekenis van de betrouwbaarheid van de informatie- en communicatietechnologie (ICT)[1] in het kader van de accountantswerkzaamheden gericht op het certificeren van de jaarrekening sterk beredeneerd vanuit de ICT. De betrouwbare werking van de general ICT controls moet worden vastgesteld als randvoorwaarde om in de controle te kunnen steunen op de beheersingsmaatregelen die deel uitmaken van de geautomatiseerde informatiesystemen.

Over het algemeen wordt er in de literatuur zonder meer van uitgegaan dat de betrouwbare *werking* van de ICT moet worden vastgesteld. Naast het ontbreken van een onderbouwing waarom de beoordeling zich op de werking moet richten, laten de budgetten voor de accountantscontrole een dergelijk onderzoek niet toe. Nu mag een budget vaktechnisch gezien geen belemmering zijn om werkzaamheden niet uit te voeren, maar een toename van de accountantswerkzaamheden past niet in het doel van het gebruik van ICT: 'het minder arbeidsintensief maken van processen en het efficiënt kunnen afhandelen van grote transactievolumes'. (Met als kanttekening de randvoorwaarde dat de ICT op een adequate wijze is georganiseerd.)

In de praktijk zien we dan ook dat accountants, uitzonderingen daargelaten[2], om de problemen met betrekking tot het vaststellen van de betrouwbaarheid van de ICT heen lopen. Uit gesprekken met vele vakgenoten is op te maken dat zij hun oordeel over de betrouwbaarheid van de door de cliënt gebruikte ICT veelal baseren op de mate waarin zich in het verleden incidenten hebben voorgedaan. Bij gebrek aan incidenten wordt nogal eens teruggevallen op de veronderstelling dat het proces betrouwbaar is verlopen. In deze redenering wordt dus impliciet gesteund op de wijze waarop de gebruikers in staat zijn geweest de betrouwbaarheid van de gegevensverwerking vast te stellen.

Het verschil tussen theorie en praktijk is ontstaan doordat in de theorievorming niet is geredeneerd vanuit de gebruikersomgeving. Zoals hierna zal worden aangetoond, wordt de onduidelijkheid weggenomen door te redeneren vanuit de gebruiker, via de systemen naar de ICT-infrastructuur. Deze redenering geeft een duidelijk inzicht welke beoordelingswerkzaamheden met welke diepgang moeten worden uitgevoerd.

Voor de theorievorming ligt een startpunt in de gebruikersomgeving meer voor de hand dan een start vanuit de ICT; dit kan worden beargumenteerd vanuit de doelstelling van de accountantscontrole. Het doel is de getrouwheid van de jaarrekening vast te stellen. Een 'halffabrikaat' is de informatie die uit de

1. Kort samengevat alle techniek die wordt gebruikt voor het verwerken van gegevens (programmatuur, netwerken, hardware, etc.).
2. Bij banken, door het DNB-memorandum.

routinematige processen komt; de betrouwbaarheid van het 'halffabrikaat' is één van de grondstoffen om tot een getrouwe jaarrekening te komen. Een zelfstandig oordeel over de werking van de systemen en de ICT-organisatie wordt, uit hoofde van de jaarrekeningcontrole, niet aan de accountant gevraagd en deze heeft een dergelijk oordeel, zoals uit het vervolg van dit artikel blijkt, vaktechnisch gezien ook niet nodig.

In de volgende paragrafen worden de genoemde componenten (menselijke handelingen, informatiesystemen en technische infrastructuur) nader uitgewerkt. De opbouw van het betoog is zo gekozen dat duidelijk wordt waarom bepaalde controlewerkzaamheden noodzakelijk zijn. Begonnen wordt met de menselijke controlehandelingen gevolgd door de beheersmaatregelen in de informatiesystemen. Deze opbouw wijkt af van de logische volgorde waarin de beoordelingswerkzaamheden over het algemeen worden uitgevoerd. De uitvoering van de werkzaamheden zal beginnen met de beoordeling van de informatiesystemen. Deze volgorde is nodig omdat anders niet kan worden bepaald welke inherente en internecontrolerisico's aan het systeem zijn verbonden en welke geprogrammeerde controles door gebruikers moeten worden opgevolgd. De verificatie van de veronderstelling van een adequate automatiseringsorganisatie en betrouwbare technische infrastructuur in de planningsfase van de controle wordt in dit artikel als laatste behandeld, in de praktijk is dit dikwijls de eerste stap. In de praktijk wordt hierdoor voorkomen dat te laat wordt vastgesteld dat de opzet van de automatiseringsorganisatie en technische infrastructuur niet aan de eisen voldoet.

MENSELIJKE (CONTROLE)HANDELINGEN

Onbetrouwbare registraties van de logistieke en financiële transacties leiden ertoe dat informatievoorziening aan het management niet meer overeenkomt met de werkelijkheid, hetgeen het risico met zich meebrengt dat besluiten worden genomen die niet leiden tot een optimale bedrijfsvoering (bijvoorbeeld grondstoffen worden te vroeg of te laat besteld). Onafhankelijk van de wijze van gegevensverwerking blijven functionarissen binnen een organisatie verantwoordelijk voor de juistheid en volledigheid van de informatieverwerking. Vanuit deze verantwoordelijkheden worden binnen organisaties maatregelen getroffen om de betrouwbaarheid te waarborgen. Voorbeelden hiervan zijn invoer-, verbands- en uitvoercontroles.

Ook al is informatieverwerking in hoge mate geautomatiseerd, er blijven uitzonderingssituaties bestaan die niet (geheel) door het systeem afgehandeld kunnen worden. Ondanks de geprogrammeerde controles en de general ICT controls kunnen fouten ontstaan als het systeem in situaties komt waarmee bij de ontwikkeling en het testen geen rekening is gehouden. Verder is het mogelijk dat door onvolkomenheden in het testen fouten onopgemerkt blijven. Dit is in zijn geheel niet denkbeeldig; dat het onmogelijk is om informatiesystemen volledig te testen behoeft voor de meeste lezers geen toelichting. Naast de in de vorige alinea aangehaalde controlemaatregelen gericht op de normale processgang, zal het management controlemaatregelen hebben getroffen om vast te stellen dat systeemfouten tijdig worden gesignaleerd.

De routinematige processen resulteren in informatie die de basis legt voor het opstellen van de jaarrekening. De accountantscontrole richt zich in deze fase van de controle op het vaststellen van de betrouwbaarheid van deze informatie. De eerste stap is de vaststelling van de wijze waarop de organisatie zelf de betrouwbaarheid van deze informatie bewaakt. De tweede stap is het kennisnemen van de binnen de organisatie uitgevoerde analyses om de betrouwbaarheid van de in de informatiesystemen vastgelegde gegevens vast te stellen.

Bij accountants is over het algemeen veel kennis en ervaring aanwezig voor het uitvoeren van de hiervoor beschreven gebruikerscontroles (door Starreveld c.s. aangeduid met 'informatiecontrole[3]'; omdat dit de doelstelling van de controle duidelijk weergeeft zal deze term in het vervolg van het artikel worden gebruikt).

Indien de accountant bij zijn beoordeling tot de conclusie komt dat de controlewerkzaamheden door de gebruiker onder de maat zijn, zal hij de organisatie aanzetten tot het uitvoeren van de noodzakelijke analyses of zelf overgaan tot het uitvoeren van aanvullende controlewerkzaamheden. De hier bedoelde accountantswerkzaamheden bestaan uit het uitvoeren van cijferanalyses (waaronder het leggen van verbanden) en gerichte detailcontroles.

De doelstelling van dit onderdeel van de accountantscontrole is zekerheid te verkrijgen over de getrouwheid van de door de informatiesystemen opgeleverde informatie. Bewust is gekozen voor de formulering 'getrouwheid ... informatie', hetgeen betekent dat geen absolute zekerheid nodig is maar zekerheid die ligt binnen de controletolerantie. Zolang het de informatie zelf betreft is het tolerantiebegrip goed hanteerbaar. Voor de beoordeling van systemen en organisaties ligt het hanteren van toleranties moeilijker. Hierop wordt in de volgende paragrafen teruggekomen.

Door het uitvoeren van informatiecontroles stelt de gebruiker van het systeem de betrouwbare werking doorlopend vast. Dit doet de gebruiker vanuit zijn/haar eigen verantwoordelijkheid ten aanzien van de juistheid en volledigheid van de informatieverwerking. Deze informatiecontrole is een prima aangrijpingspunt voor de accountantscontrole. Zowel voor de gebruiker als voor de accountant geldt dat de controles in het informatiesysteem van voldoende gehalte moeten zijn om deze te kunnen gebruiken voor de vaststelling van de betrouwbaarheid van de informatieverwerking. Het informatiesysteem zal de internecontrolefunctionaliteit in zich moeten hebben die nodig is om de betrouwbare werking te kunnen vaststellen. De systeembeoordeling die nodig is om vast te stellen dat alle foutkansen worden afgedekt (in accountantstermen de volledigheid en juistheid van de controlemaatregelen), wordt in de volgende paragraaf uitgewerkt.

3. De controle op de etrouwbaarheid van door het informatiesysteem geproduceerde informatie.

Om de waarnemingen met betrekking tot de toereikendheid van de internecontrolemaatregelen in de informatiesystemen om te kunnen vormen tot een beeld dat geldt voor een langere tijdsperiode, is het noodzakelijk dat:
- de toegangsautorisatiemechanismen adequaat zijn;
- de verwerkingslogica (de programma's) niet ongeautoriseerd verandert.

Deze maatregelen liggen binnen de automatiseringsorganisatie. Om de toereikendheid van de maatregelen vast te stellen zal in aanvulling op de beoordeling van de door de gebruikers uitgevoerde informatiecontroles en de systeembeoordeling, een beoordeling van de general ICT controls plaats moeten vinden. De mate waarin dit nodig is, zal in één van de volgende paragrafen worden uitgewerkt.

BEHEERSINGSMAATREGELEN IN INFORMATIESYSTEMEN

Over de wijze waarop controles binnen de organisatie moeten worden uitgevoerd, is van oudsher binnen het accountantsberoep veel ervaring opgedaan; dit aspect krijgt ook ruimschoots aandacht in de accountantsopleiding. Anders ligt het bij de beoordeling van de volledigheid van de controlefunctionaliteiten in de systemen die ten grondslag liggen aan de informatievoorziening. Hiervoor is inzicht nodig in de toereikendheid van de geprogrammeerde controles.

Het vaststellen van het bestaan en de werking is een onderdeel van de informatiecontrole.

De controles in het informatiesysteem moeten zodanig zijn ontworpen dat zij de operationele gebruiker en het management de mogelijkheid bieden de informatieverwerking onder controle te houden. Belangrijke controlepunten zijn:
- de acceptatie van de ingevoerde gegevens (zowel handmatig als digitaal);
- de volledigheid en juistheid van door het systeem geïnitieerde acties;
- de volledigheid en juistheid van de opgeslagen gegevens;
- de informatieverstrekking (zowel leesbaar als digitaal).

Een gedetailleerde behandeling van deze onderdelen valt buiten de reikwijdte van dit artikel. Thans wordt volstaan met het verwijzen naar normenkaders die op deze punten bij systeemonderzoeken worden gehanteerd.

De internecontrolemaatregelen in de geautomatiseerde onderdelen van de informatiesystemen worden aangeduid met geprogrammeerde controles. Deze controles zijn niet direct zichtbaar. Het is één van de functionaliteiten van het geautomatiseerde deel van de gegevensverwerking. Om inzicht te krijgen in de geprogrammeerde controles moet kennis worden genomen van het systeem. Dit kan door middel van documentatie maar ook door demonstraties en gesprekken met gebruikers. Het in zijn volle omvang doorgronden van een informatiesysteem is geen eenvoudige opgave.

Voor een beoordeling van de verwerking van de routinematige transacties binnen de kaders van de accountantscontrole past een integrale beoordeling van alle in het systeem opgenomen beheersingsmaatregelen niet. Dit zou, binnen de doelstelling van de accountantscontrole, veel te veel omvatten, hetgeen niet efficiënt is. Een toespitsing moet worden gemaakt op de processen die raakvlakken hebben met de informatiestromen die van belang zijn voor de accountantscontrole. Op basis van risicoanalyse moet worden bepaald welke maatregelen noodzakelijk zijn om te waarborgen dat de geautomatiseerde informatieverstrekking een betrouwbare afspiegeling is van de werkelijkheid.

De systeembeoordeling is gericht op de opzet en bestaan van alle op basis van de risicoanalyse noodzakelijk geachte controle- en beveiligingsfunctionaliteiten. De werking behoeft in deze fase van de controle niet te worden vastgesteld. Het vaststellen van de werking is een onderdeel van de hiervoor beschreven informatiecontrole. Een niet-adequate werking zal door de gebruikers worden gesignaleerd in de vorm van ontbrekende controle-informatie en/of geconstateerde fouten. Het als zelfstandig onderdeel vaststellen van de werking is, uit hoofde van de jaarrekeningcontrole, niet zinvol. De jaarrekeningcontrole richt zich op de getrouwheid van informatie en niet op de betrouwbaarheid van systemen.

Er kan nog een andere redenering worden gevolgd waaruit blijk dat de oordeelsvorming over de werking van de controlemaatregelen in een informatiesysteem een station te ver is. Het vaststellen van de werking van informatiesystemen vindt door de gebruikers plaats op basis van de analyses van de uitkomsten. Als vastgesteld is dat de informatie voldoende betrouwbaar is, is het voor de jaarrekeningcontrole niet nodig om terug te gaan naar het systeem. De systeembeoordeling hoeft niet verder te gaan dan de beoordeling van de toereikendheid van de controles om de betrouwbaarheid van de informatie te kunnen beoordelen. De context van deze beoordeling wordt bepaald door een risicoanalyse uit het oogpunt van de accountantscontrole.

Indien tot de conclusie wordt gekomen dat de internecontrolefunctionaliteit onvoldoende is, zal samen met de gebruiker gezocht moeten worden naar een oplossing. Compensatie door extra gebruikerscontroles zal lang niet altijd mogelijk zijn, omdat de benodigde controle-informatie ontbreekt. Aanpassen van het systeem, het ontwikkelen van queries of het gebruik van audit-software is de enige oplossing die dan nog resteert.

Naast inzicht in de geprogrammeerde controles moet er zekerheid zijn dat het systeem niet ongeautoriseerd kan veranderen en dat de gegevens alleen binnen de aangegeven autorisatie worden vrijgegeven voor inzage of bewerking. Indien dit

niet bewust wordt beheerst, kunnen de conclusies uit de informatiecontroles niet worden gebruikt als graadmeter voor de algehele betrouwbare werking.

TECHNISCHE ORGANISATIE

De general ICT controls zijn de basis voor een betrouwbare geautomatiseerde gegevensverwerking. Deze controles zijn er onder meer op gericht te waarborgen dat de functionaliteit van de programmatuur geen ongeautoriseerde wijziging ondergaat en dat de gegevens slechts op een geautoriseerde wijze kunnen worden gemuteerd. Naast de betrouwbaarheid zijn de controles ook bedoeld om de toereikendheid van de continuïteitsmaatregelen te waarborgen. Het betreft maatregelen om te voorkomen dat gegevens verloren gaan en dat herstel van de gegevensverwerking langer duurt dan vanuit het bedrijfsproces toelaatbaar wordt geacht.

Het uitgangspunt is dat gegevensverwerkende processen betrouwbaar moeten verlopen. Een professionele organisatie streeft ernaar foutloos te werken. De gevolgen van fouten en het herstellen van fouten brengen extra kosten met zich mee. Ondersteuning bij de realisatie van betrouwbare processen kan door een gespecialiseerde accountant of IT-auditor worden verleend. Dit zijn advieswerkzaamheden die geen onderdeel uitmaken van de reguliere accountantscontrole.

In het algemeen legt de diepgang van de beoordeling van de general ICT controls een belangrijk gat tussen de theorie en de praktijk bloot. In de theorie wordt gewoonlijk gesteld dat de werking moet worden beoordeeld. In de praktijk wordt in het kader van de accountantscontrole zeer pragmatisch met het beoordelen van automatiseringsorganisaties omgegaan en blijft de beoordeling veelal beperkt tot opzet en bestaan. Ligt het knelpunt in de praktijk (wordt het niet goed gedaan) of moet de theorievorming nader worden gedifferentieerd? In de volgende alinea's worden enkele aspecten rond deze vragen toegelicht.

Bij de controle van de verwerking van de routinematige transacties is het werkprogramma van de accountant, bij een systeemgerichte controle, toegesneden op het vaststellen van een betrouwbare gegevensverwerking. Doorredenerend zou dit betekenen dat de accountant opzet, bestaan *en werking* van de automatiseringsorganisatie zou moeten beoordelen. De automatiseringsorganisatie is één van de componenten uit het totale systeem dat bepalend is voor de betrouwbaarheid van de vastlegging en verwerking van de routinematige transacties. Het vaststellen van de voortdurend betrouwbare werking van een automatiseringsorganisatie vereist een 'zware' audit. Indien deze audit geïsoleerd wordt uitgevoerd, is het vertalen van de bevindingen naar de betekenis voor de betrouwbaarheid van de door de geautomatiseerde systemen opgeleverde informatie niet eenvoudig. In de praktijk doen zich regelmatig afwijkingen voor in de werkprocedures en vinden beveiligingsincidenten (veelal vergissingen) plaats. Het tolerantiebegrip kan hierop echter niet worden toegepast. De tolerantie geldt voor de informatie en kan niet worden doorvertaald naar het systeem. Dit komt doordat een kleine afwijking van de werkwijze of een minieme afwijking in de beveiliging vergaande gevolgen kan hebben voor de betrouwbaarheid van de uitkomsten van de gegevensverwerking en de opgeslagen gegevens. Het kan echter ook zo zijn dat de afwijking geen enkel gevolg heeft voor de kwaliteit van de informatieverwerking en de betrouwbaarheid van de opgeslagen gegevens. Slechts een analyse van de gevolgen van de verstoring voor de betrouwbaarheid van de informatieverstrekking kan hierin helderheid verschaffen. Deze analyse komt, voorzover het de jaarrekening betreft, overeen met de in een vorige paragraaf uiteengezette informatiecontrole! Deze informatiecontrole wordt door de gebruikers uitgevoerd en leidt direct tot een beeld van de betrouwbaarheid van het informatiesysteem, hetgeen in de ogen van de auteur duidelijk maakt dat in het kader van de jaarrekeningcontrole een specifiek onderzoek naar de *werking* van de automatiseringsorganisatie niet nodig is. De werking wordt indirect vastgesteld door middel van de informatiecontroles.

De diepgang van de beoordeling van de general ICT controls toont een belangrijk gat tussen de theorie en de praktijk.

Voor de jaarrekeningcontrole is belangrijk dat sprake is van een beheerst verwerkingsproces. Indien het stelsel van geprogrammeerde controles en informatiecontroles adequaat is, zullen fouten hierdoor uiteindelijk aan het licht komen. Echter, fouten maken extra correctie-inspanning noodzakelijk en veel fouten vertroebelen de controle-informatie. Om fouten te voorkomen moet er zekerheid zijn over het bestaan van een verwerkingsorganisatie die onder controle is. Indien de inrichting van de verwerkingsorganisatie niet aan de minimale betrouwbaarheidseisen voldoet, dan is er onvoldoende basis om op de geprogrammeerde controles te steunen voor het signaleren van mogelijke fouten in de verwerking. Aan een beoordeling van de opzet en het bestaan van de betrouwbaarheidsmaatregelen binnen de automatiseringsorganisatie zal dus niet voorbij kunnen worden gegaan.

Change management (inclusief testen) en logische toegangsbeveiliging zijn uit oogpunt van de beheersing van de werking van informatiesystemen de belangrijkste processen. De eerste moet voorkomen dat er verschillen ontstaan tussen de door de gebruiker, mede op grond van de aanwezige controlefunctionaliteit, geaccepteerde systemen en de in werkelijkheid operationele systemen. De logische toegangsbeveiliging moet waarborgen dat slechts geautoriseerde transacties in de gegevensbestanden/databases worden verwerkt. Uit hoofde van de jaarrekeningcontrole dienen deze twee processen ten minste te worden beoordeeld. Bij de beoordeling van de opzet en het bestaan van de automatiseringsorganisatie in het kader van de jaarrekeningcontrole moeten met betrekking tot de processen zowel de procedures, de beveiligingsmaatregelen als de in-

J.C. Boer RE RA
Is sinds 1985 verbonden aan KPMG EDP Auditors NV, sinds 1992 als directeur. Hij is verantwoordelijk voor de KPMG IT-auditpraktijk in het midden en het oosten van het land. Binnen KPMG heeft hij zitting in het college Vaktechniek met als specifiek aandachtspunt audit en assurance.

ternal control[4] worden betrokken. Zonder de werkprocedures en beveiligingsmaatregelen als onbelangrijk terzijde te schuiven, dient het accent van de beoordeling te liggen op de internal control. De internal control is overkoepelend en vormt het sluitstuk van de inrichting van de organisatie. De controlemaatregelen en de correctieprocedures vormen het herstellend vermogen van de organisatie.

In deze paragraaf is geconstateerd dat er een verschil is tussen de theorie en de praktijk bij de beoordeling van automatiseringsorganisaties in het kader van de jaarrekeningcontrole. De vraag in hoeverre de theorie of het dagelijks handelen bijstelling behoeft, is een knelpunt in de praktische betekenis. Op basis van het voorgaande behoeft vooral de theorievorming een bijstelling. Echter, ook de dagelijkse praktijk kan efficiënter, en wel door het onderzoek vooral te richten op het change management en de logische toegangsbeveiliging. De beoordeling van deze processen moet zich, naast de inrichting van deze procedures, vooral richten op het bestaan van internal control, gericht op de goede werking van de genoemde procedures.

4. Voor de Engelse term is gekozen om een duidelijk onderscheid te maken met het engere begrip interne controle. Met internal control wordt naast controle ook aangeduid het bijsturen en het correctief aanpassen van de organisatie en procedures.

SAMENVATTING

Op dit moment ontbreekt het aan een eenduidig standpunt over de diepgang van de noodzakelijke beoordeling van informatiesystemen en automatiseringsorganisaties in het kader van de accountantscontrole. De praktijk gaat hiermee anders om dan de theorie. De praktijk neemt in zijn redenering de uitkomsten van de gegevensverwerking als uitgangspunt, de theorie werkt daarentegen over het algemeen meer vanuit de gebruikte ICT.

De beoordeling van de gebruikte IT hoeft niet gericht te zijn op de werking.

De conclusie is dat in het kader van de jaarrekeningcontrole de beoordeling van de gebruikte IT niet gericht hoeft te zijn op de werking. De betrouwbaarheid van de uitkomsten van de gegevensverwerking wordt vastgesteld op basis van de informatiecontroles gebaseerd op een fundament van geprogrammeerde controles en internal control binnen de automatiseringsorganisatie. De geprogrammeerde controles en general ICT controls zijn de voorwaarde om informatiecontroles te kunnen uitvoeren. Het vaststellen in hoeverre aan deze voorwaarde wordt voldaan, kan beperkt blijven tot de opzet en het bestaan; de werking wordt gelijktijdig met het vaststellen van de betrouwbaarheid van de uitkomsten (de informatiecontrole) vastgesteld. Impliciet is met het vaststellen van de betrouwbaarheid van de uitkomsten ook vastgesteld dat de werking van informatiesystemen en de technische infrastructuur betrouwbaar is geweest. Voor de jaarrekeningcontrole is dit minder interessant omdat de werking van deze elementen in dit kader geen afzonderlijk object van onderzoek is.

Dit artikel is bedoeld als bijdrage aan de discussie waartoe het studierapport 'Normatieve maatregelen voor de geautomatiseerde gegevensverwerking' van het NIVRA de betrokkenen heeft willen aanzetten. De auteur staat open voor reacties op zijn zienswijze en zal gaarne meewerken aan verdere publicaties over dit onderwerp.

LITERATUUR

[Bien95] Margaret E. van Biene-Hershey, *IT Auditing, An Object Oriented Approach*, Delwel, 1995.

[ISAC96] ISACA, *CobiT: Control objectives for information and related Technology*, 1996.

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

[NIVR95] Koninklijk NIVRA, studierapport *Normatieve maatregelen voor de geautomatiseerde gegevensverwerking*, 1995.

[Limp97] Limperg Instituut, *Interne controle en Informatiecontrole*, Kluwer Bedrijfsinformatie, 1997.

EDP-auditor en jaarrekeningcontrole van vergaand geautomatiseerde organisaties

W. de Korte RE RA

Bij de controle van de jaarrekening van organisaties die in hoge mate zijn geautomatiseerd, zal de accountant bij zijn oordeelsvorming bijzonder afhankelijk zijn van de toepassing van IT bij de gecontroleerde organisatie. De controlemiddelen en -technieken van de accountant zullen bij deze organisaties veelal tekortschieten voor een deugdelijke grondslag. Kan de EDP-auditor vanuit zijn deskundigheid een uitspraak doen over posten in de saldibalans en derhalve de beperkingen van de controlemiddelen en technieken van de accountant compenseren?

INLEIDING

Reeds decennia lang neemt de automatiseringsgraad binnen organisaties toe. Taken worden meer en meer geautomatiseerd uitgevoerd. Vele controletaken van gebruikers worden in de vorm van controleprocedures in de toepassingsprogrammatuur opgenomen. Dit heeft mede tot gevolg dat veel controles in de bedrijfsprocessen niet (altijd) meer zichtbaar zijn voor de gebruiker.

Een belangrijk controlemiddel voor de accountant is de beoordeling van de opzet van de stelsels van maatregelen van interne controle en het vaststellen van de juiste werking daarvan. Het vervallen van zichtbare gebruikerscontroles en functiescheiding noodzaakt de controlerend accountant er steeds meer toe bij de controle van de jaarrekening gebruik te maken van de controles die binnen de automatisering zijn aangebracht. De EDP-auditor zal vanuit zijn deskundigheid de accountant kunnen ondersteunen bij het routinematige deel van de uitvoering van de controle van de jaarrekening.

Veelal krijgt de beoordeling van de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking nog weinig aandacht of staat dit los van de jaarrekeningcontrole. In feite blijkt in de praktijk nog steeds een voorkeur te bestaan voor de eertijds gebruikelijke 'audit around the computer'. De EDP-audits worden veelal uitgevoerd ten behoeve van het management en zijn met name gericht op verbeteringen, hetgeen zijn neerslag vindt in de adviesbrief en omdat BW boek II artikel 393 lid 4 dat in een aantal gevallen vereist.

De vraag of de EDP-auditor zich een oordeel moet vormen over de hierboven genoemde (deel)aspecten van de geautomatiseerde gegevensverwerking ten behoeve van ondersteuning van de accountant bij zijn controlerende taken is nu en zeker in de toekomst niet de enig relevante. Momenteel is een aantal organisaties reeds op een zodanige wijze geautomatiseerd, dat controle met behulp van brondocumenten onmogelijk is geworden of op korte termijn onmogelijk zal worden. De accountant zal bij zijn onderzoek naar de getrouwheid van de jaarrekening zonder de geautomatiseerde gegevensverwerking daarbij te betrekken in deze gevallen niet tot een oordeel kunnen komen omtrent de volledigheid, het bestaan en de accuratesse (juistheid) van posten in de jaarrekening.

Dit artikel gaat in op de vraag of het voor een EDP-auditor mogelijk is een uitspraak te doen over beweringen (van posten) in de saldibalans in het kader van de controle van de jaarrekening van organisaties die in hoge mate zijn geautomatiseerd (op basis waarvan de accountant zich vervolgens zelfstandig een oordeel kan vormen).

Het onderwerp leent zich ongetwijfeld voor verdere discussie tussen accountants en EDP-auditors. Dit artikel is een weergave van de aanpak en noodzakelijke werkzaamheden van de EDP-auditor voor het verkrijgen van een deugdelijke grondslag voor het doen van een uitspraak over beweringen (aangaande posten) in de saldibalans in het kader van de controle van de jaarrekening.

CASUS SECURITY FIRST NETWORK BANK

De actualiteit van de in de Inleiding geschetste vraagstelling wordt ter illustratie verduidelijkt door onderstaande casus.

Security First Network Bank (verder te noemen SFNB) maakt gebruik van de mogelijkheden die door Internet worden geboden. Alle transacties worden door cliënten via Internet en het netwerk van de betaal- en geldautomaten aangeleverd. Het inlezen van de transacties in de geautomatiseerde informatiesystemen (verder te noemen GIS) geschiedt volledig automatisch gepaard gaande met geprogrammeerde invoercontroles. Vervolgens worden de transacties, omgeven door geprogrammeerde controles, automatisch verwerkt in de GIS. Na verwerking worden de mutaties op de rekeningoverzichten van de cliënten automatisch bijgewerkt. Tevens vindt renteberekening en tarifering van transacties (waaronder effecten) periodiek volledig automatisch plaats. De cliënt kan via Internet zijn rekeningoverzichten opvragen. Nagenoeg alle handmatige activiteiten zijn overgenomen door de applicaties of worden uitgevoerd door de cliënt (invoer van transacties). Slechts enkele (controle)werkzaamheden worden door de medewerkers van de bank verricht, waaronder beoordeling van de kredietaanvragen van cliënten. De accountant wordt verzocht de jaarrekening van een verklaring te voorzien. Er zijn bij SFNB nagenoeg geen fysieke brondocumenten voorhanden op basis waarvan de accountant een controle op de volledige en juiste verwerking van transacties (met name ten behoeve van de verantwoording van de omzetprovisie, transactiekosten vreemde valuta, rentebaten en -lasten en opbrengsten van effectentransacties, herwaardering positie in vreemde valuta en effecten inclusief off-balanceposities) kan controleren 'om de GIS heen'.

De accountant zal de volledigheid van de registratie van de invoer van geaccepteerde en uitgevoerde transacties moeten kunnen vaststellen. Hiertoe is geen soll-positie vanuit fysieke brondocumenten aanwezig. De geprogrammeerde invoercontroles (onvervangbare maatregelen van interne controle vanwege het ontbreken van een goederenbeweging) dienen zorg te dragen voor volledige, juiste en tijdige registratie (kortom betrouwbaar) van geaccepteerde en uitgevoerde transacties. De accountant zal een systeemgerichte controleaanpak dienen te selecteren als gevolg van het ontbreken van andere controlemiddelen, waarbij gebruik wordt gemaakt van maatregelen van interne controle binnen de automatiseringsorganisatie (general ICT controls) en de applicaties.

De accountant blijft volgens de Richtlijnen voor de Accountantscontrole eindverantwoordelijk voor het oordeel over de getrouwheid van de jaarrekening.

SAMENWERKING ACCOUNTANT EN EDP-AUDITOR IN GEVAL VAN COMPLEXE GIS

De accountant dient te overwegen in welke mate de GIS van invloed zijn op de controle. De accountant moet voldoende kennis bezitten omtrent de GIS om de (te) verrichte(n) werkzaamheden te kunnen plannen, sturen, begeleiden en beoordelen. Hij dient derhalve te overwegen of er ten behoeve van de controle behoefte is aan specialistische kennis op het gebied van GIS. Indien een deskundige op het gebied van GIS wordt ingeschakeld, dient de accountant de zekerheid te verkrijgen, dat dergelijke werkzaamheden toereikend zijn voor zijn controledoelstellingen, met inachtneming van hetgeen hierover is opgenomen in de Richtlijnen voor de Accountantscontrole. Volgens de Richtlijnen voor de Accountantscontrole blijft de accountant eindverantwoordelijke voor de af te geven accountantsverklaring bij de jaarrekening. De accountant dient zich zelfstandig een oordeel te kunnen vormen omtrent de uitkomsten van de uitvoering van de EDP-audit.

Vanwege het ontbreken van een definitieve richtlijn waarin de samenwerking tussen accountants en EDP-auditors wordt beschreven (de ontwerprichtlijn over de samenwerking is niet aangenomen), wordt bij de beantwoording van de vraagstelling gebruikgemaakt van Richtlijn 621 (Samenwerking Accountant en Actuaris). Het is overigens ook mogelijk dat EDP-auditors binnen de accountantsorganisaties gehouden zijn aan interne kantoorrichtlijnen.

In Richtlijn 621 wordt gesteld dat de actuaris verantwoordelijk is voor de materiële juistheid en toereikendheid van de voorziening voor verzekeringsverplichtingen/pensioenverplichtingen. Naar analogie hiervan kan gesteld worden dat de EDP-auditor verantwoordelijk is voor het deel van de controle, dat door hem wordt uitgevoerd. Het betreft een onderzoek waarbij het doel is het vaststellen van de materiële betrouwbaarheid van de uitkomsten van de GIS. Hierna zal dit verder worden uitgewerkt. Verder wordt in Richtlijn 621 aangegeven dat de actuaris bij zijn oordeelsvorming rekening houdt met het oordeel van de accountant over de bij de waardering van de verzekeringsverplichtingen/pensioenverplichtingen gehanteerde basisgegevens en uitgangspunten. De EDP-auditor zal het normenkader voor zijn onderzoek derhalve dienen af te leiden van de inschattingen van de accountant ten aanzien van de noodzakelijke administratieve organisatie en internecontrolemaatregelen en de fouttoleranties ten aanzien van de uitkomsten van de GIS. Naar analogie van Richtlijn 621 stelt de EDP-auditor de informatie, op grond waarvan hij tot zijn oordeel is gekomen, aan de accountant ter beschikking teneinde deze in staat te stellen tot een zelfstandig oordeel te komen over de verantwoording van de gecontroleerde organisatie. Hierbij valt te denken aan:

- het normenkader voor de noodzakelijke administratieve organisatie en internecontrolemaatregelen ten aanzien van de te onderscheiden processen afgeleid van de risicoanalyse (gebaseerd op de inschatting van het inherente risico en internecontrolerisico en de fouttoleranties in de jaarrekening);
- de beschrijving van de opzet van de general ICT

controls en een oordeel over de toereikendheid daarvan;
- de functionele beschrijving van de opzet van de gecontroleerde systemen met daarin opgenomen de aanwezige toepassingscontroles;
- de beschrijving van het datamodel binnen de GIS en dataflow door de GIS;
- de beschrijving van de onderzochte rekenregels binnen de GIS;
- de weergave van de uitgevoerde controlewerkzaamheden gericht op de opzet, het bestaan en de werking van procedures binnen de automatiseringsorganisatie en de opzet en het bestaan van toepassingscontroles;
- de strekking van het oordeel van de EDP-auditor gebaseerd op de uitgevoerde werkzaamheden.

De accountant en de EDP-auditor overleggen ten slotte over de resultaten van hun werkzaamheden en de gevolgen daarvan voor de af te geven verklaring.

POSITIONERING EDP-AUDIT IN PROCES VAN TOTSTANDKOMING JAARREKENING

De jaarrekening komt doorgaans tot stand in twee fasen ([Frie91]). In de eerste fase vindt registratie van transacties in de bedrijfsprocessen plaats ondersteund door GIS. Aan het einde van deze fase wordt binnen de financiële administratie een saldibalans opgemaakt. In de tweede fase worden handmatig journaalposten geboekt voor onder andere de schattingsposten in de jaarrekening zoals voorzieningen. Tot slot zal de jaarrekening opgesteld worden als resultante van saldibalans plus voorafgaande journaalposten. De tweede fase is doorgaans niet omgeven met een adequaat stelsel van maatregelen van interne controle. De voorafgaande journaalposten bestaan doorgaans uit niet-routinematige posten. De accountant zal de tweede fase derhalve doorgaans gegevensgericht controleren. De EDP-auditor zal hierbij in het algemeen geen rol van betekenis spelen. (Bij waarderingsvraagstukken rondom IT en informatiesystemen en systemen in ontwikkeling speelt hij mogelijk wel een rol.) De rol van de EDP-auditor zal zich derhalve beperken tot het vaststellen van de betrouwbaarheid (juistheid, tijdigheid en volledigheid) van de gegevens op de saldibalans. Een dergelijk onderzoek van de EDP-auditor zal zich richten op de initiatie van transacties (invoer in GIS), de verwerking in de GIS alsmede de uitvoer op de saldibalans.

Bij het onderzoek naar de betrouwbaarheid van de gegevens op de saldibalans spelen voor de EDP-auditor de volgende beweringsaspecten een rol: volledigheid, bestaan en accuratesse van de gegevens. Ten aanzien van de beweringsaspecten: waardering, presentatie en toelichting (het traject na de totstandkoming van de saldibalans) zal de accountant geen ondersteuning van de EDP-auditor kunnen verkrijgen vanwege enerzijds het ontbreken van een adequate organisatie en anderzijds het subjectieve gehalte van de schattingen, waarbij de vakkundige oordeelsvorming van de accountant noodzakelijk is. (In de praktijk blijkt de EDP-auditor een goed klankbord te kunnen zijn op het gebied van eerdergenoemde waarderingsvraagstukken met betrekking tot IT en systemen.) Eigendom wordt doorgaans op andere wijze dan door middel van systeemgerichte controles vastgesteld.

OBJECTEN VAN ONDERZOEK BIJ EDP-AUDIT IN KADER VAN CONTROLE JAARREKENING

Het management van een organisatie is verantwoordelijk voor de realisering van de organisatiedoelstellingen. Dit artikel richt zich op de werkzaamheden van de EDP-auditor bij de beoordeling van de betrouwbaarheid van de totstandkoming van de saldibalans. Teneinde de realisering van een betrouwbare saldibalans te beheersen zal een cyclus van het sturen van de activiteiten en het meten van de resultaten van de activiteiten noodzakelijk zijn voor het initiëren en het uitvoeren van bijsturingsacties. Ten aanzien van de geautomatiseerde gegevensverwerking geldt hetzelfde beheersingsprincipe ([Donk95]). De realisering van de geformuleerde doelstellingen (gekoppeld aan de te beoordelen kwaliteitsaspecten) zal beheerst dienen te worden.

De betrouwbaarheid van de uitkomsten van een GIS wordt grotendeels bepaald door de general ICT controls en de toepassingscontroles.

De betrouwbaarheid van (de uitkomsten van) een GIS wordt grotendeels bepaald door computercontroles met een algemeen karakter, de general ICT controls, en computercontroles die zich richten op de werking van een specifieke applicatie, de toepassingscontroles ([Koed96]). General ICT controls hebben invloed op het inherente risico en het internecontrolerisico. Toepassingscontroles hebben invloed op het internecontrolerisico. De EDP-auditor zal de deugdelijke grondslag aan deze controles dienen te ontlenen.

General ICT controls

General ICT controls moeten worden onderzocht per IT-infrastructuur. IT-infrastructuur kan worden gedefinieerd als het geheel van hardware, software, computergerelateerde communicatiefaciliteiten, documentatie en vaardigheden die vereist zijn ter ondersteuning van IT-diensten. Dit houdt in dat elke afzonderlijke IT-infrastructuur apart beoordeeld dient te worden.

Vanuit de controle van de jaarrekening wordt veelal het volgende onderscheid in general ICT controls gemaakt ([Munc95]):
- beleid en management;
- functiescheidingen;
- logische toegangsbeveiliging;
- fysieke toegangsbeveiliging;

- systeemontwikkeling en onderhoudsprocedures (change management);
- continuïteit;
- systeembeheerprocedures en rekencentrumprocedures;
- gebruikerssatisfactie.

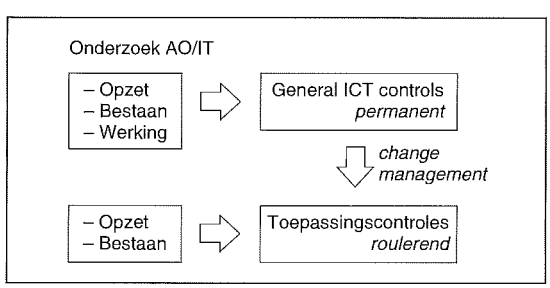
Ten aanzien van afzonderlijke IT-infrastructuren kunnen verschillende eisen gesteld worden. De eisen worden gesteld vanuit de wijze van beheersing van de bedrijfsprocessen en de applicaties die de bedrijfsprocessen ondersteunen. Er zijn twee manieren waarop de processen, waaronder de gegevensverwerkende, beheerst worden:
- gebruikers steunen op het stelsel van administratieve organisatie en interne controle binnen de automatisering(sorganisatie);
- gebruikers steunen niet op het stelsel van administratieve organisatie en interne controle binnen de automatisering(sorganisatie).

In het laatste geval zal binnen de gebruikersorganisatie een stelsel van compenserende maatregelen van interne controle aangebracht moeten zijn, zodat onder andere de betrouwbaarheid van de geautomatiseerde gegevensverwerking beheerst wordt.

Niet alle IT-infrastructuren behoeven derhalve aan dezelfde eisen onderworpen te zijn. Bij SFNB zal voor nagenoeg alle bedrijfsprocessen sprake (dienen te) zijn van een situatie waarin wordt gesteund op het stelsel van administratieve organisatie en interne controle binnen de automatisering(sorganisatie). Gebruikers, er zijn er bij SFNB slechts weinigen, controleren de invoer niet zelfstandig op betrouwbaarheid (dit kunnen zij waarschijnlijk ook niet), zij laten deze controles over aan de applicaties en de automatiseringsorganisatie. Indien het management een beheerste (controlled) omgeving wenst, en dat is op zijn minst gezegd verstandig, dan zullen general ICT controls van een dusdanige opzet moeten zijn, dat gewaarborgd is dat de GIS op een betrouwbare wijze de gegevens verwerken en dat de geprogrammeerde toepassingscontroles juist worden uitgevoerd.

Gebruikers controleren veelal niet (zelfstandig) de betrouwbare werking van de computercontroles.

Indien goed opgezet en geïmplementeerd hebben general ICT controls een belangrijke invloed op de effectiviteit van de automatiseringsorganisatie en haar functies en waarborgen dat de geautomatiseerde gegevensverwerking in een beheerste omgeving



Figuur 1. Samenhang onderzoek general ICT controls en toepassingscontroles.

plaatsvindt ([IIAR91]). De general ICT controls vormen derhalve de basis voor de kwaliteit van de toepassingscontroles.

Toepassingscontroles

Toepassingscontroles zijn gericht op de beheersing van de betrouwbaarheid van de [Jenk92])
- invoer in de GIS:
  invoercontroles waarborgen de volledige en juiste vastlegging van geautoriseerde transacties en identificeren geweigerde, uitgestelde en dubbele invoer;
- gegevensverwerking in en door de GIS:
  controles op de verwerking waarborgen de volledige en juiste verwerking van geautoriseerde transacties;
- uitvoer door de GIS:
  uitvoercontroles waarborgen dat een volledig en juist audit trail van de uitkomsten van de verwerking wordt gerapporteerd aan de juiste individuen voor controledoeleinden.

Voorbeelden van toepassingscontroles zijn:
- logische toegangs- en autorisatiecontroles binnen de applicaties;
- waarschijnlijkheids- en redelijkheidscontroles;
- bestaanscontroles;
- verbandscontroles;
- integriteits- en aansluitingscontroles (subadministraties en netwerk van controletotalen);
- juistheidscontroles;
- volledigheidscontroles.

Opgemerkt wordt dat naast toepassingscontroles ook de rekenregels binnen de applicaties op een juiste wijze dienen te zijn geprogrammeerd voor een betrouwbare gegevensverwerking door GIS.

Op basis van een risicoanalyse en afhankelijkheidsanalyse brengt het management van een organisatie het stelsel van beheersmaatregelen aan binnen de applicaties en automatiseringsorganisatie alsmede binnen de gebruikersorganisatie. De EDP-auditor zal de toepassingscontroles dienen te onderzoeken teneinde vast te stellen dat de beheersing van de betrouwbaarheid van de regelkring in de systemen (vanuit management-controloptiek) adequaat is.

Toepassingscontroles kunnen in de applicaties zijn geprogrammeerd, maar kunnen ook door de gebruikers handmatig worden uitgevoerd. Geprogrammeerde controles kunnen leiden tot gebruikerscontroles, bijvoorbeeld bij exception reports (uitzonderingsrapportages), die door de gebruikers verder zullen moeten worden afgehandeld.

Samenhang general ICT controls en toepassingscontroles

De samenhang tussen de general ICT controls en toepassingscontroles in het kader van de controle van de jaarrekening kan als afgebeeld in figuur 1 worden weergegeven:
Zoals uit deze figuur naar voren komt zal, indien in de controle wordt gesteund op toepassingscontroles, de voortdurende juiste werking van general ICT controls moeten worden gecontroleerd. Hiervoor is reeds gesteld dat de general ICT controls het fundament vormen voor de juiste werking van de toepas-

singscontroles, waarbij met name change management belangrijk is. Het onderzoek naar de kwaliteit van de general ICT controls zal derhalve ieder jaar moeten plaatsvinden. Indien blijkt dat de kwaliteit van de general ICT controls ontoereikend is, zal bij de controle van de jaarrekening geen gebruik gemaakt kunnen worden van de EDP-controles (general ICT controls en toepassingscontroles) en zal inderdaad de reeds hiervoor weergegeven 'audit around the computer' noodzakelijk zijn. In de casus SFNB zal dit betekenen dat geen goedkeurende verklaring afgegeven kan worden vanwege het ontbreken van voldoende alternatieve controlemiddelen.

De EDP-audits op de geprogrammeerde toepassingscontroles zullen moeten plaatsvinden bij implementatie van nieuwe GIS. Indien systemen stabiel zijn en niet verder worden ontwikkeld, zal na de nulmeting geen noodzaak bestaan voor het verrichten van een onderzoek naar de geprogrammeerde toepassingscontroles. Overigens worden hierbij adequate change-managementprocedures (organisatie van de systeemontwikkeling en het onderhoud) als voorwaarde gesteld. Indien de GIS worden gewijzigd of vernieuwd zal altijd een (her)beoordeling van de juiste opzet en het bestaan van toepassingscontroles moeten plaatsvinden. Dit kan worden geïnitieerd vanuit de beoordeling van de change-managementprocedures. De door de gebruikers uitgevoerde toepassingscontroles zullen wel dienen te worden onderzocht op voortdurende juiste werking. In dit artikel wordt hiervan op een enkele uitzondering na geabstraheerd, vanwege het feit dat het artikel zich richt op organisaties die in hoge mate zijn geautomatiseerd.

Samenvatting objecten van onderzoek

Samenvattend kunnen de volgende objecten van onderzoek van de EDP-audit worden genoemd: general ICT controls en toepassingscontroles: invoercontroles, verwerkingscontroles en uitvoercontroles. Ten aanzien van general ICT controls zijn met name van belang (omschreven in terminologie van de accountantscontrole): functiescheiding, logische toegangsbeveiliging, change-management- en systeembeheerprocedures en rekencentrumprocedures. Al deze controles dienen ervoor zorg te dragen dat de gegevens op de saldibalans betrouwbaar zijn.

AANPAK VAN DE EDP-AUDIT

Voorafgaand aan de beschrijving van de aanpak zelf worden eerst de randvoorwaarden geformuleerd.

Randvoorwaarden voor audit

Alvorens de EDP-auditor een oordeel afgeeft bij een post op de saldibalans zal hij een deugdelijke grondslag dienen te verkrijgen. Ten aanzien van het verkrijgen van een deugdelijke grondslag zijn de volgende randvoorwaarden van toepassing:

- de kwaliteit van de controles moet objectief meetbaar zijn;
- de controlemethoden en -technieken moeten voldoende controle-informatie verstrekken;
- de uitkomsten van het onderzoek naar de kwaliteit van de controles moeten (in bepaalde mate) vertaalbaar zijn naar de kwantitatieve normen van de accountantscontrole.

Bij de beoordeling van de uitkomsten van de uitvoering van de audit moet door de EDP-auditor getoetst worden of aan deze randvoorwaarden is voldaan.

Fasen en onderdelen van de EDP-audit

De uitvoering van de accountantscontrole is doorgaans op de volgende wijze gefaseerd: strategie, planning, uitvoering, afsluitende beoordeling, rapportage en evaluatie. Ten behoeve van de effectiviteit (het bijdragen van controle-informatie) en de efficiency van de EDP-audit is het noodzakelijk dat de EDP-auditor zijn werkzaamheden afstemt op de controleaanpak, zoals deze door de accountant wordt geselecteerd. Met name de risico-inschatting ten aanzien van het inherente risico en het internecontrolerisico alsmede de maatstaf voor de materialiteit van posten in de saldibalans zijn van belang.

Bij de EDP-audit van SFNB zal dit een ander karakter krijgen vanwege de verregaande automatisering. In dit artikel, waarin wordt gerefereerd aan de casus van SFNB, is de inzet van de EDP-auditor, die nu het merendeel van de controlewerkzaamheden uitvoert ten behoeve van het vaststellen van de betrouwbaarheid van de gegevens op de saldibalans, vooral van belang in de eerste vier fasen van het controleproces.

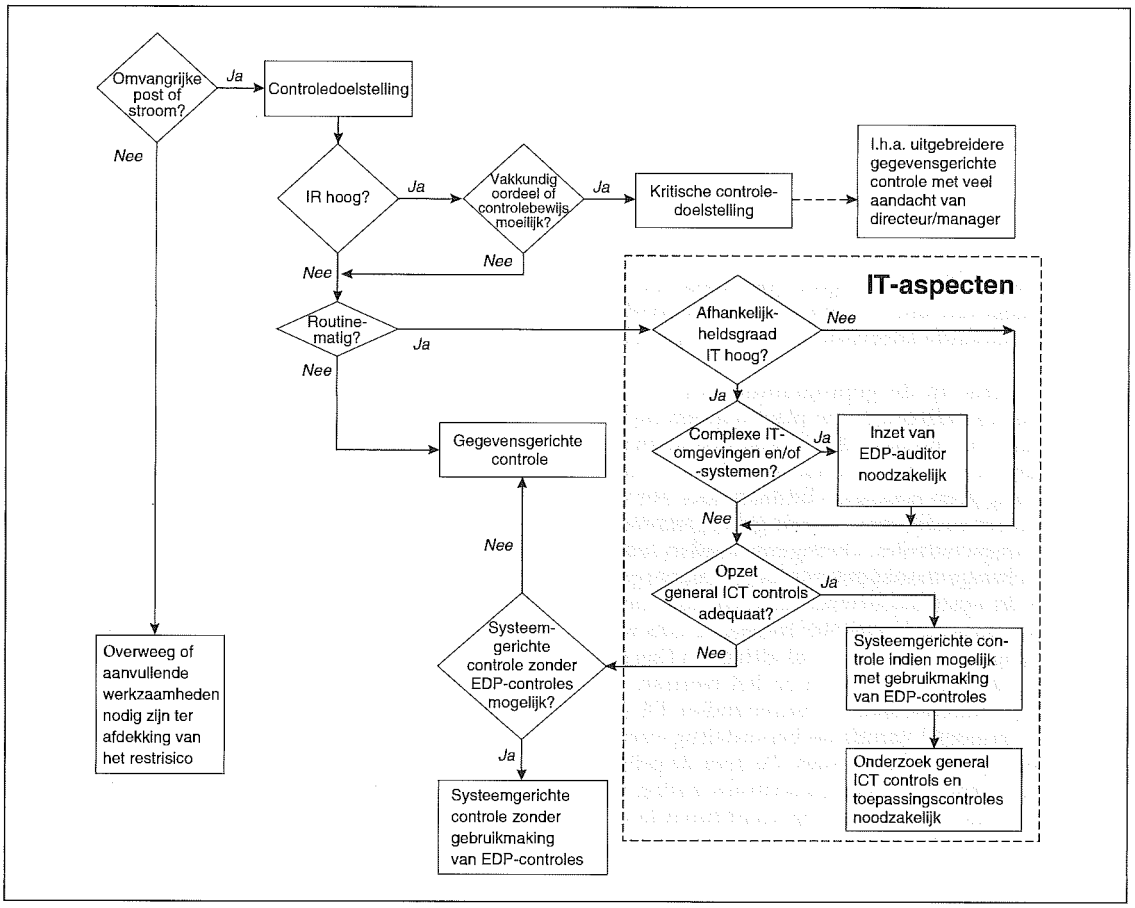
In figuur 2 worden de te volgen beslissingsmomenten in het controleproces weergegeven welke de controleaanpak bepalen; hierbij zijn de vraagstukken die direct een relatie hebben met de IT in een grijs kader weergegeven. Deze beslissingsboom is afgeleid van de KPMG Audit Service methodiek ([KPMG94]). Het schema opent met de vraag of de desbetreffende post of stroom in de jaarrekening omvangrijk is. Gezien het feit dat de posten en stromen voortkomen uit bedrijfsprocessen is het met het oog op de efficiency raadzaam deze beslissingsboom per bedrijfsproces (dus een bundeling van posten en stromen, die het bedrijfsproces genereert) door te lopen, omdat een bedrijfsproces veelal door één informatiesysteem wordt ondersteund, en elk systeem derhalve in de EDP-audit als afzonderlijk onderdeel onderzocht wordt.

Zoals hiervoor is gesteld, richt de EDP-auditor zich bij het onderzoek naar de betrouwbaarheid van de posten in de saldibalans op de general ICT controls en de beheersingsmaatregelen omtrent de invoer in, de verwerking in en de uitvoer van gegevens uit de GIS (toepassingscontroles).

De EDP-auditor voert het merendeel van de controlewerkzaamheden uit voor het vaststellen van de betrouwbaarheid van de saldibalans.

In de strategie- en planningsfase zullen de opzet, het bestaan en de werking van de general ICT controls

Figuur 2. Beslissingsboom bepaling controle-aanpak.



Tabel 1. Fasen en onderdelen van de EDP-audit.

Fase	Onderdeel onderzoek
Strategie/planning	Inzicht verkrijgen in processen en systemen welke posten in de jaarrekening genereren, bepalen van afhankelijkheidsgraad van IT en uitvoeren van risicoanalyse op de processen.
Strategie/planning	Normen formuleren ten aanzien van de te onderzoeken general ICT controls en toepassingscontroles.
Planning	Beoordelen van general ICT controls en evalueren uitkomsten voor de controleaanpak.
Planning/uitvoering	In kaart brengen en beoordelen van aanwezige stelsel van beheersingsmaatregelen op de juiste invoer, verwerking, uitvoer en bewaring van gegevens (beoordelen van toepassingscontroles) en evalueren van de uitkomsten van het onderzoek voor de betrouwbaarheid van de gegevens op de saldibalans.
Planning/uitvoering	Rapporteren aan accountant.

alsmede de opzet van de toepassingscontroles worden onderzocht. Het onderzoek naar de voortdurende juiste werking van de general ICT controls kan pas worden afgerond op balansdatum, dus als het boekjaar is afgesloten. Het bestaan van toepassingscontroles wordt vastgesteld hetzij reeds in de planningsfase hetzij in de uitvoeringsfase. De rapportage van de EDP-auditor vindt plaats in de uitvoeringsfase.

Op basis van het bovenstaande kunnen ten aanzien van de EDP-audit de in tabel 1 genoemde onderdelen worden onderscheiden.

Inzicht verkrijgen in processen en systemen

Inzicht in processen en systemen is noodzakelijk voor het plannen van de noodzakelijke werkzaamheden in de EDP-audit. Er zal inzicht moeten worden verkregen in de onderstaande aspecten:

- de primaire bedrijfsprocessen en bijbehorende informatiestromen en -bestanden;
- het karakter per bedrijfsproces (sturend of ondersteunend, routinematig of niet-routinematig);
- welke bedrijfsprocessen belangrijk/kritisch zijn voor de cliënt;
- welke risico's verbonden zijn aan de belangrijke/kritische bedrijfsprocessen;
- welke geautomatiseerde systemen de belangrijke/kritische bedrijfsprocessen ondersteunen en in hoeverre de organisatie afhankelijk is van de IT;
- welke IT wordt gebruikt;
- het profiel van de automatiseringsorganisatie;
- de mate van betrokkenheid van gebruikers bij IT-ontwikkelingen.

Hierbij kan gebruik worden gemaakt van beschrijvingen van de processen en de administratieve organisatie en interne controle alsmede functie- en taakbeschrijvingen. Tevens kunnen indien noodzakelijk inlichtingen worden gevraagd aan de gecontroleerde (interviews) ten behoeve van het in kaart brengen van bovenstaande aspecten. Hulpmiddelen voor de vastleggingen van een en ander kunnen worden gevonden in schematechnieken en matrices waarin processen, functies en taken en bevoegdheden met elkaar in relatie worden gebracht.

Het in kaart brengen van bovenstaande (IT-)aspecten wordt doorgaans in samenwerking met de accountant uitgevoerd. Hiermee wordt bereikt dat in het vervolg van het onderzoek duidelijk is dat bepaalde aspecten diepgaander worden beoordeeld (de kritische IT-infrastructuur en GIS) en bepaalde aspecten minder diepgaand of in het geheel niet. Deze aspecten zullen in de planningsfase worden uitgewerkt, waarna de controleaanpak afgestemd kan worden op de uitkomsten van dit onderzoek.

Het vaststellen van de afhankelijkheid is in dit artikel gericht op betrouwbaarheid. Van de eisen ten aanzien van beschikbaarheid, effectiviteit, wettelijke bepalingen en brancherichtlijnen wordt in dit artikel geabstraheerd. De mate van afhankelijkheid geeft een indicatie voor het belang van de beheersingsmaatregelen gericht op de betrouwbaarheid. De vaststelling van de afhankelijkheid ten aanzien van het kwaliteitsaspect betrouwbaarheid komt tot stand nadat de procesanalyse is uitgevoerd. De EDP-auditor vormt zich zelfstandig een oordeel over de afhankelijkheid en zal dit afstemmen met het management van de gecontroleerde organisatie en met de accountant.

Basis voor normen voor EDP-audit

De EDP-auditor zal bij de uitvoering van de audit op de betrouwbaarheid van de gegevens op de saldibalans, zijnde de output van GIS, de normen in acht dienen te nemen die worden gesteld door de accountant. De accountant is eindverantwoordelijke voor de af te geven accountantsverklaring en zal de eisen die aan de betrouwbaarheid van de gegevens van de saldibalans worden gesteld, formuleren (de controletolerantie). De controletolerantie wordt vervolgens door de accountant verdeeld over de posten in de jaarrekening (standen en stromen); de verdeelde tolerantie wordt omschreven als evaluatietolerantie ([Aren91]).

Daarnaast baseert de accountant zijn controleaanpak mede op de inschatting van het inherente risico en het internecontrolerisico. Dit is van belang voor het onderzoek naar de general ICT controls en toepassingscontroles. Hiervoor is reeds aangegeven, dat de keuze systeemgericht te controleren met gebruikmaking van de controles in de automatisering mede afhankelijk is van het beheersingsconcept van het management (het al dan niet steunen op maatregelen van interne controle in de automatisering(sorganisatie)).

De EDP-auditor zal zijn audit richten op de general ICT controls en de toepassingscontroles, welke op basis van een risicoanalyse en afhankelijkheidsanalyse door het management van de gecontroleerde organisatie zijn geïmplementeerd.

De normen voor de audit van de EDP-auditor dienen te zijn afgeleid van de normen voor de controle van de jaarrekening.

Normen voor general ICT controls
De normen die gesteld worden ten aanzien van de general ICT controls zijn afhankelijk van enerzijds het inherente risico als zodanig en anderzijds de inschatting ('waardering' in het risicoanalysemodel) van het internecontrolerisico door de accountant. Indien de accountant bij de controle van de betrouwbaarheid van een post in de jaarrekening wenst te steunen of zelfs moet steunen (zie casus SFNB) op de administratieve organisatie en interne controle, waarbij gebruikgemaakt wordt of zelfs moet worden (zie casus SFNB) van computercontroles, dan zullen de (kwaliteits)normen ten aanzien van de general ICT controls ten aanzien van de betrokken IT-infrastructuur op een hoger niveau liggen dan in het geval dat de accountant bij de controle geen gebruik maakt van de computercontroles. Daarnaast zal door de accountant een afweging gemaakt worden omtrent de mate van toepassing van gegevensgerichte maatregelen om het detectierisico af te dekken. Bij onvoldoende mogelijkheden voor gegevensgerichte maatregelen (waaronder cijferanalyses en detailcontroles) betekent dit dat de normen ten aanzien van het internecontrolerisico op een hoger niveau zullen liggen (zie casus SFNB), immers het internecontrolerisico zal lager dienen te zijn om het accountantscontrolerisico op een acceptabel niveau te krijgen.

Er is een aantal normenkaders geformuleerd waaraan bij de uitvoering van de EDP-audit kan worden gerefereerd. Te noemen zijn onder andere: CobiT, ITIL, Code voor Informatiebeveiliging, NIVRA-geschriften in de serie Automatisering en controle en NIVRA Studierapport 34.

Vooraf is in de risicoanalyse van de accountant aangegeven welke norm ten aanzien van het inherente risico en het internecontrolerisico geldt. Op basis van deze inschatting én van vakkundige oordeelsvorming maakt de EDP-auditor een schatting van het minimaal noodzakelijke niveau van de general ICT controls.

Normen voor toepassingscontroles
De normen die gesteld worden ten aanzien van de toepassingscontroles zijn enerzijds afhankelijk van de inherente risico's in de bedrijfsprocessen (wat kan er zoal fout gaan in de uitvoering van de bedrijfsactiviteiten) en anderzijds afhankelijk van de inschatting van het internecontrolerisico en van de controletolerantie en evaluatietolerantie (foutenkans die niet wordt afgedekt door toepassingscontroles) door de accountant. Hierbij geldt hetzelfde betoog als bij de general ICT controls.

De normen ten aanzien van toepassingscontroles zullen specifiek per bedrijfsproces dienen te worden bepaald op basis van de risicoanalyse en gestelde controletolerantie en evaluatietolerantie.

De toepassingscontroles zijn specifiek gericht op de betrouwbaarheid van de posten in de saldibalans. De controletolerantie en evaluatietolerantie per post in de saldibalans zijn kwantitatief van aard. De controletolerantie en evaluatietolerantie kunnen derhalve worden gekwalificeerd als maatlat, waartegen de werkelijkheid kan worden afgemeten. De toepassingscontroles dienen ervoor zorg te dragen dat geen fouten in de posten op de saldibalans groter dan de controletolerantie en evaluatietolerantie voorkomen. Dit betekent dat de toegestane fout per transactie vermenigvuldigd met het aantal transacties onder de gestelde toleranties dient te blijven.

Conclusies hanteren van normen
Geconcludeerd wordt dat de normen die gesteld worden aan de general ICT controls en de toepassingscontroles, afhankelijk zijn van:

- Het inherente risico.

- De door de accountant gekozen controleaanpak, die de inschatting ('waardering' in het risicoanalysemodel) van het internecontrolerisico bepaalt. Het wel of niet toepassen van gegevensgerichte controlemaatregelen beïnvloedt de eis ten aanzien van het internecontrolerisico. Dit lijkt op het eerste gezicht een omgekeerde wereld; het detectierisico bepaalt het internecontrolerisico. Het is echter mogelijk vanwege een hogere efficiency van gegevensgerichte maatregelen toch de nadruk te leggen op gegevensgerichte controles.

- De gestelde toleranties ten aanzien van posten in de jaarrekening, welke mede voortkomen uit posten op de saldibalans zijnde de uitkomsten van de GIS (met name van belang voor toepassingscontroles).

De normen zullen per specifieke situatie bepaald moeten worden.

De formulering van de normen ten aanzien van de general ICT controls en de toepassingscontroles dient te berusten op de vakkundige oordeelsvorming (veronderstelt specifieke deskundigheid) van de EDP-auditor, waarbij als randvoorwaarde is gesteld de door de accountant aangegeven controletolerantie en evaluatietolerantie per post in de jaarrekening, welke wordt gevormd door één of meer posten in de saldibalans eventueel aangevuld met voorafgaande journaalposten. De EDP-auditor dient zijn oordeelsvorming omtrent de normen ten aanzien van de general ICT controls en de toepassingscontroles te overleggen en af te stemmen met de accountant alvorens het onderzoek wordt uitgevoerd, dit om discussies bij de evaluatie van de uitkomsten van het onderzoek te voorkomen. Het verdient derhalve aanbeveling de accountant het normenkader schriftelijk te laten bevestigen.

In dit artikel wordt verder geen aandacht besteed aan de specifieke invulling van de normen.

Onderzoek general ICT controls

Het onderzoek naar de general ICT controls dient uitsluitsel te geven over de vraag of een systeemgerichte controle met gebruikmaking van EDP-controles mogelijk is.

Gezien de reikwijdte wordt in dit artikel niet inhoudelijk ingegaan op de aspecten die moeten worden onderzocht bij de genoemde onderdelen van de general ICT controls. Voor het vaststellen van de opzet en in een aantal gevallen ook tegelijkertijd het bestaan zal gebruikgemaakt worden van:
- interviews met de betrokken medewerkers in de gebruikers-, systeemontwikkelings- en verwerkings- en transportorganisatie;
- kennisnemen van procedurebeschrijvingen van de systeemontwikkelings- en verwerkings- en transportorganisatie en uitvoeren van lijncontroles;
- kennisnemen van de mogelijkheden en de toepassing van de mogelijkheden (maatregelen van interne controle) van de aanwezige besturings- en toegangsbeveiligingsprogrammatuur alsmede het databasemanagementsysteem, en vaststellen van het bestaan van de maatregelen van interne controle.

De werking van de general ICT controls wordt vastgesteld door middel van het uitvoeren van proceduretests op die aspecten/maatregelen van interne controle waaraan de controle-informatie ten behoeve van de onderbouwing van de controleaanpak (systeemgericht met gebruikmaking van EDP-controles) wordt ontleend. Hieruit kan worden afgeleid dat de werking van de general ICT controls zichtbaar moet zijn om achteraf de juiste uitvoering te kunnen vaststellen. Indien controles niet zichtbaar zijn zal geen uitspraak gedaan kunnen worden over de werking, tenzij de EDP-auditor permanent aanwezig is ter vaststelling van de werking, hetgeen een irrationele controle impliceert (zeer hoge kosten).

Evaluatie general ICT controls voor controleaanpak
De uitkomsten van het onderzoek naar de opzet, het bestaan en de werking van bovengenoemde general ICT controls zijn objectief meetbaar. De normen zijn vastgelegd in de voorgaande fase. In deze fase wordt getoetst aan de vastgelegde norm.

De EDP-auditor zal na afronding van de beoordeling van de opzet en het bestaan een tussenrapportage verstrekken aan de accountant ter onderbouwing van de controleaanpak. Na afronding van het onderzoek naar de general ICT controls (op zijn vroegst om 0.00 uur van de eerste dag van het nieuwe boekjaar) zal de EDP-auditor de accountant kunnen rapporteren over de voortdurende juiste werking van de general ICT controls gedurende het gehele boekjaar. Een voortdurende juiste werking stelt hoge eisen aan de automatiseringsorganisatie (toereikende zichtbare en verifieerbare controles).

De rapportage van de uitkomsten van het onderzoek naar de opzet van de general ICT controls zal de accountant uitsluitsel dienen te geven dat de gekozen controleaanpak (systeemgericht met gebruikmaking van EDP-controles) mogelijk is of niet. Er zal een antwoord gegeven moeten worden op de vraag of de general ICT controls adequaat zijn van opzet. Nadat de juiste opzet is vastgesteld, zal het onderzoek naar de voortdurend juiste werking worden uitgevoerd.

Indien bij het onderzoek van de general ICT controls blijkt dat een systeemgerichte controle met gebruikmaking van EDP-controles niet mogelijk is, zal de

EDP-auditor hierover direct aan de accountant rapporteren. De EDP-auditor zal de (onbevredigende) uitkomst met de accountant bespreken en de gevolgen voor de controleaanpak aangeven. In de situatie van de casus van SFNB zal de conclusie luiden dat de jaarrekening van SFNB niet controleerbaar is vanwege het ontbreken van een 'adequaat' stelsel van administratieve organisatie en interne controle. De accountant zal in dit geval met redenen omkleed het management van SFNB rapporteren, dat geen goedkeurende verklaring afgegeven kan worden. In dit artikel wordt verder geabstraheerd van het probleem of sprake is van subjectieve verhindering.

Onderzoek toepassingscontroles

Op basis van de uitgevoerde risicoanalyse en het oordeel over de opzet van de general ICT controls zal door de EDP-auditor onderzocht dienen te worden op welke wijze de beheersingsmaatregelen in de applicaties zijn aangebracht (geprogrammeerd) of op welke wijze de beheersingsmaatregelen in de gebruikersorganisatie zijn getroffen.
Hiervoor is reeds onderscheid gemaakt tussen de volgende toepassingscontroles:
- invoercontroles (inclusief autorisatiecontroles);
- verwerkingscontroles;
- uitvoercontroles.

Figuur 3 licht de plaats en het belang van toepassingscontroles nader toe.

De EDP-auditor maakt bij zijn onderzoek naar de opzet en het bestaan van de toepassingscontroles onder andere gebruik van de volgende controlemethoden en -technieken:
- kennisnemen van organigram, taken en bevoegdheden medewerkers, administratieve procedures en de daarin vervatte maatregelen van interne controle;
- kennisnemen en beoordelen van systeemdocumentatie van de GIS;
- kennisnemen en beoordelen van beschrijving informatiearchitectuur en de daarbij aangegeven eigenaren van data;
- interviews met systeemontwikkelaars/projectleider;
- interviews met (kern)gebruikers;
- kennisnemen van testrapportages (systeem- en gebruikerstests);
- uitvoeren van lijncontroles van transacties door de GIS.

Het meten van de effectiviteit en de toereikendheid van de toepassingscontroles (bijdrage aan de controle-informatie voor de onderbouwing van de grondslag voor de af te geven accountantsverklaring) berust op vakkundige oordeelsvorming van de EDP-auditor. De EDP-auditor zal hiervoor over voldoende kennis van administratieve organisatie en interne controle dienen te beschikken.

Voorop staat dat de fouten die in posten op de saldibalans voorkomen, tezamen in omvang niet de gestelde controletolerantie en evaluatietolerantie per post te boven mogen gaan. De toepassingscontroles zullen dit moeten waarborgen.

Mochten bovenstaande werkzaamheden onvoldoende controle-informatie opleveren, dan zal de EDP-auditor zijn eigen werkzaamheden moeten uitbreiden. Hierbij kan gedacht worden aan het uitvoeren van eigen testwerkzaamheden en het zelfstandig controleren van de juiste werking van verbandscontroles.

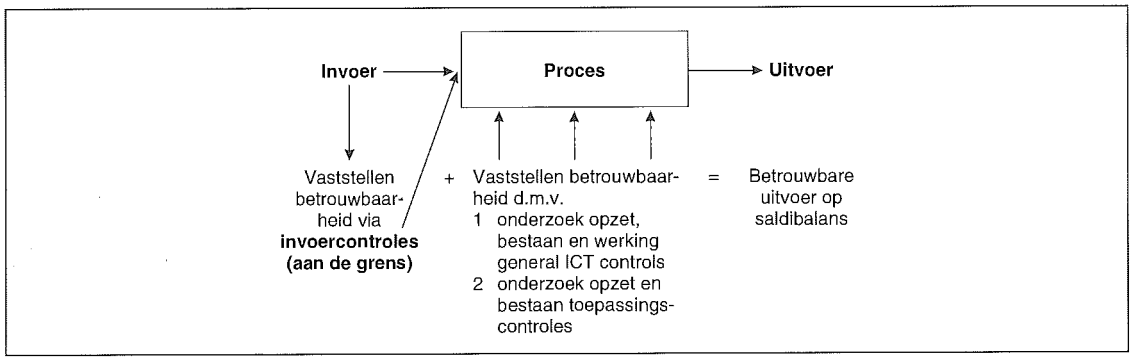
Hieronder wordt een aantal aandachtspunten weergegeven ten aanzien van bovengenoemde toepassingscontroles (van gebruikerscontroles wordt geabstraheerd).

Invoercontroles zijn veelal onvervangbare maatregelen van interne controle.

Invoercontroles
De EDP-auditor stelt vast dat de invoercontroles zekerheid geven omtrent volledigheid, juistheid en tijdigheid van de registratie van de invoer van geaccepteerde en uitgevoerde transacties.

In het in figuur 3 weergegeven schema is aangegeven dat invoercontroles dienen te bewerkstelligen, dat de registratie van de geaccepteerde en uitgevoerde transacties betrouwbaar plaatsvindt. Derhalve zal bij het onderzoek naar de toepassingscontroles de nadruk worden gelegd op invoercontroles.

Ten behoeve van het vaststellen van de volledigheid van invoer zal aan de onderstaande aspecten inhoud moeten zijn gegeven en zullen deze derhalve door de EDP-auditor moeten worden beoordeeld. De beoordeling zal zich richten op het toetsen aan de gestelde (kwantitatieve) normen, welke zijn afgeleid van de controletolerantie en evaluatietolerantie.



Figuur 3. Overzicht controleaanpak voor vaststelling betrouwbaarheid uitvoer.

Tezamen met de andere toepassingscontroles mogen geen fouten in de posten van de saldibalans onontdekt blijven door de GIS, welke tezamen de toleranties overschrijden. Aan de volgende aspecten zal invulling moeten zijn gegeven:
- beschikbaarheid van logginginformatie van aan de GIS aangeboden en door de GIS geaccepteerde en uitgevoerde transacties;
- alle geaccepteerde en uitgevoerde transacties zullen in een invoerbestand beschikbaar dienen te blijven als 'brondocumenten';
- eenmaal in de GIS ingevoerde en door de GIS geaccepteerde en uitgevoerde transacties (dus in overeenstemming met de autorisatiestructuur in de administratieve organisatie) mogen niet meer verwijderd en ongeautoriseerd gewijzigd kunnen worden.

De controles die deze aspecten afdekken, kunnen worden bestempeld als onvervangbare interne controles. Achteraf is zonder de noodzakelijke (betrouwbare) basisinformate niet meer vast te stellen of de uitkomsten van de GIS betrouwbaar zijn weergegeven.

Als de casus SFNB hierbij betrokken wordt, zal een soort elektronisch postontvangstregistratiesysteem noodzakelijk zijn voor het vaststellen van de volledigheid van de registratie van de via Internet ontvangen geaccepteerde en uitgevoerde transacties. Indien geen zekerheid verkregen wordt omtrent de betrouwbaarheid van de registratie van geaccepteerde en uitgevoerde transacties zal de EDP-auditor zich – bijvoorbeeld door middel van verbandscontroles – geen oordeel kunnen vormen omtrent de output van de GIS en zal de accountant derhalve geen controle-informatie ontvangen, welke kan dienen als deugdelijke grondslag voor het afgeven van een goedkeurende verklaring.

De EDP-auditor zal verder invoercontroles die de juistheid en accuratesse van de (schone) invoer bewerkstelligen, beoordelen. Deze invoercontroles kunnen zijn:
- waarschijnlijkheids- en redelijkheidscontroles;
- bestaanscontroles;
- juistheidscontroles;
- volledigheidscontroles.

Tot slot zal de EDP-auditor de aanwezigheid vaststellen van controles die controleren dat alle ingevoerde transacties in het invoerbestand door de GIS zijn verwerkt.

Toegangscontroles
De toegangscontroles zijn noodzakelijk voor de beveiliging van de integriteit van data en applicaties. De EDP-auditor stelt vast dat de toegangscontroles in de applicaties op een adequate wijze zijn ingevuld. Hiertoe zal hij gebruikmaken van de faciliteiten die het ontwikkeltool waarmee de GIS zijn ontwikkeld, biedt. Hij zal hierbij, indien deze aanwezig is, gebruikmaken van de functiematrix waarin gebruikers worden gekoppeld aan functies of modules. Indien deze functiematrix ontbreekt zal de EDP-auditor op een alternatieve wijze de inrichting van de toegangscontrole dienen vast te stellen. Bij de beoordeling van de general ICT controls is reeds invulling gegeven aan de logische toegangsbeveiliging tot de data en systemen in het algemeen.

De norm (maatlat) voor de beoordeling van de toegangscontroles is zodanig dat niet afgeweken mag worden van de bevoegdhedenstructuur, zoals deze is vastgelegd in de administratieve organisatie. Er dient derhalve minimaal aan deze norm te zijn voldaan. Functiescheidingen mogen niet worden doorbroken in de applicaties.

Verwerkingscontroles
De verwerkingscontroles moeten de betrouwbaarheid van de verwerking van transacties waarborgen. De EDP-auditor stelt vast dat de geprogrammeerde maatregelen in de GIS een adequaat stelsel vormen. Hierbij zal met name gebruik kunnen worden gemaakt van verbandscontroles (netwerk van controletotalen), audit trails en foutverslagen, welke geproduceerd worden van tijdens de verwerking geweigerde transacties. Verbandscontroles (vergelijking van output met input in totalen) dienen te bewerkstelligen dat geen mutaties verloren gaan tijdens de verwerking. Tevens kan gebruikgemaakt worden van een vergelijking van de telling van het aantal transacties aangeboden ter verwerking en het aantal verwerkte transacties met eventueel het aantal geweigerde transacties in een wachtbestand.

Van alle fouten die tijdens de verwerking zijn opgetreden, zullen uitzonderingsrapportages uit de GIS verkregen dienen te worden. De uitzonderingsrapportages zullen door de gebruikers afgewerkt moeten worden. Deze uitzonderingsrapportages zullen doorlopend genummerd en na afwerking op een centrale plaats gearchiveerd dienen te worden, zodat van deze maatregelen van interne controle het bestaan en de juiste werking vastgesteld kunnen worden. De handmatige correctieprocedures rondom de verwerking zullen door de EDP-auditor worden beoordeeld.

De interfaces tussen de diverse GIS (indien geen sprake is van één geïntegreerd GIS) zullen door de EDP-auditor op betrouwbaarheid (en controleerbaarheid) dienen te worden beoordeeld.

De norm (maatlat) voor bovenstaande beoordelingen wordt gevormd door de controletolerantie en evaluatietolerantie, die aan de posten in de saldibalans zijn toegekend. De fouten (het totaalbedrag aan fouten) die door de verwerkingscontroles niet worden ontdekt (tezamen met de overige toepassingscontroles) mogen in omvang de gestelde toleranties niet overschrijden.

Naast de genoemde werkzaamheden gericht op het vaststellen van de toereikendheid van de verwerkingscontroles zal specifiek aandacht dienen te worden geschonken aan memoriaalboekingen in de financiële administratie. Memoriaalboekingen kunnen worden gekarakteriseerd als niet-routinematig. Omdat een memoriaalboeking een post in de saldibalans kan raken welke systeemgericht wordt gecontroleerd, is onderzoek naar de juistheid en autorisatie van memoriaalboekingen echter wel noodzakelijk. Een memoriaalboeking kan doorbreking van functiescheiding en bevoegdheden, zoals deze in de organisatie en in de GIS aanwezig zijn, inhouden. De memoriaalboekingen worden doorgaans door de financiële administratie direct in het grootboek verwerkt. Met behulp van bestandsanalyse zullen deze

transacties op een efficiënte wijze kunnen worden achterhaald en vervolgens op juistheid (en autorisatie) worden gecontroleerd (eventueel uit te voeren door de accountant).

Uitvoercontroles
Uitvoercontroles dienen te waarborgen dat alle verwerkte transacties worden bijgewerkt in de (uitvoer)bestanden. Het databasemanagementsysteem zal hiertoe functionaliteiten kunnen bieden. Indien de verwerking onjuist is verlopen of indien de verwerking is vastgelopen, zal teruggegaan moeten kunnen worden naar de situatie voor de transactie (zogenaamde rollback); de (referentiële) integriteit van de bestanden dient te zijn gewaarborgd. Verder kan gebruikgemaakt worden van verbandscontroles zoals weergegeven bij de verwerkingscontroles.

Voor de norm voor de uitvoercontroles kan worden verwezen naar de andere toepassingscontroles. Tezamen met de andere toepassingscontroles mogen geen fouten in de posten van de saldibalans voorkomen die de toleranties overschrijden.

Rekenregels
Rekenregels binnen de applicaties van de GIS vormen het hart van de gegevensverwerking. Met behulp van de rekenregels worden gegevens omgezet van invoer naar uitvoer. Het zal derhalve duidelijk zijn dat de EDP-auditor geen uitspraak kan doen omtrent de betrouwbaarheid van de uitkomsten van de GIS op de saldibalans indien hij de rekenregels niet heeft beoordeeld op juistheid. De beoordeling van de rekenregels vergt kennis van de bedrijfseconomie (het berekenen van de financiële consequenties van transacties) en de bedrijfsadministratie (wijze van verslaglegging van de financiële consequenties in de financiële administratie) en indien relevant de financiële rekenkunde en levensverzekeringswiskunde.

Mogelijkerwijs kan de accountant hierbij ondersteuning bieden. De EDP-auditor zal zich zelfstandig een oordeel moeten vormen omtrent de juistheid van de rekenregels. Indien hij hiertoe niet in staat is zal hij geen uitspraak kunnen doen omtrent de uitkomsten van de GIS. In de GBRE zijn geen bepalingen opgenomen omtrent de samenwerking met andere deskundigen voor deelonderzoeken, zoals het onderzoeken van rekenregels. Er wordt derhalve aansluiting gezocht bij de Richtlijnen voor de Accountantscontrole (Richtlijn 620).

Evaluatie/conclusies onderzoek toepassingscontroles voor betrouwbaarheid saldibalans
De kwaliteit van de toepassingscontroles (met name invoercontroles zijn van belang) en de juistheid van de rekenregels is meetbaar. De toetsing van de kwaliteit van de toepassingscontroles, die dienen te waarborgen dat aan de kwantitatieve normen die gelden voor fouten in posten op de saldibalans is voldaan, is mogelijk. Indien is vastgesteld dat het opgezette stelsel (samenstel) van toepassingscontroles adequaat is en rekenregels juist zijn geprogrammeerd, indien daarnaast is vastgesteld dat de controles bestaan (juist zijn geprogrammeerd en gebruikerscontroles juist worden uitgevoerd) en indien deze controles geplaatst zijn in een betrouwbare (stabiele) geautomatiseerde omgeving (general ICT controls zijn adequaat), dan bestaat voldoende zekerheid omtrent de betrouwbaarheid van de uitkomsten van de GIS op de saldibalans.

Overigens wordt nogmaals benadrukt dat de beoordeling van de toereikendheid van de general ICT controls en toepassingscontroles berust op vakkundige oordeelsvorming van de EDP-auditor; de normen zijn met een zekere mate van subjectiviteit bepaald. Aangegeven is dat de normen vooraf afgestemd moeten worden met de accountant. Het gaat om de mate van acceptabel restrisico (ontdekkingsrisico), hetgeen is vastgelegd in de normen zoals hiervoor is omschreven.

De EDP-auditor zal de uitkomsten van de controlewerkzaamheden toetsen aan de normen ten aanzien van het controlerisico, de controletolerantie en evaluatietolerantie, zoals deze door de accountant zijn gesteld, en vervolgens zijn rapportage (de mededeling) opstellen, verstrekken en toelichten aan de accountant.

De volgende oordelen van de EDP-auditor zijn mogelijk ten aanzien van het onderzoeksobject, de saldibalans ([Velt95]):

- Goedkeurend, indien geen materiële tekortkomingen in de opzet, het bestaan en de werking van de general ICT controls en de opzet en het bestaan van de toepassingscontroles zijn geconstateerd of materiële onderzoeksonzekerheden ten aanzien van deze controles zijn blijven bestaan.

- Goedkeurend met beperking, indien er sprake is van een materiële tekortkoming en/of materiële onderzoeksonzekerheid. Tekortkomingen kunnen betrekking hebben op de werking van general ICT controls en/of de opzet en het bestaan van toepassingscontroles (eventueel van werking van door gebruikers uitgevoerde toepassingscontroles).

- Oordeelonthouding. Dit oordeel zal in praktijk overigens niet van toepassing zijn voor dit type audit. Er zal geen sprake zijn van onzekerheid. Indien een omissie is vastgesteld of indien geen zekerheid kan worden verkregen over de opzet en het bestaan van de administratieve organisatie en interne controle, dan voldoet de administratieve organisatie en interne controle niet aan de daaraan te stellen eisen: een afkeurend oordeel of oordeel met beperking zijn dan de mogelijkheden.

- Afkeurend, indien de EDP-auditor tot het oordeel is gekomen dat de general ICT controls en/of de toepassingscontroles niet voldoen aan de gestelde criteria, zodat geen zekerheid verkregen kan worden omtrent de betrouwbaarheid van de output van de GIS. Er is sprake van een combinatie van tekortkomingen van wezenlijk belang.

De accountant zal zich zelfstandig een oordeel moeten kunnen vormen omtrent de uitkomsten van het onderzoek van de EDP-auditor.

De accountant zal op basis van het oordeel van de EDP-auditor in staat moeten zijn, zijn oordeel over de getrouwheid van de jaarrekening (voor wat betreft de beweringsaspecten die zijn onderzocht door de EDP-auditor) te vormen. De accountant zal zich overigens zelfstandig een oordeel moeten kunnen vormen omtrent de uitkomsten van het onderzoek van de EDP-auditor.

In de casus SFNB heeft de accountant geen mogelijkheid voor het uitvoeren van detailcontroles zodat geen of onvoldoende controle-informatie op een alternatieve wijze kan worden verkregen (gegevensgerichte controle). Dit impliceert dat de accountant de mededeling van de EDP-auditor, onder voorbehoud dat in het traject saldibalans naar jaarrekening geen tekortkomingen worden geconstateerd, direct kan vertalen naar de accountantsverklaring. Het verdient derhalve de voorkeur de mededeling van de EDP-auditor op een soortgelijke wijze op te stellen als een accountantsverklaring.

SAMENVATTING

De vraagstelling binnen dit artikel heeft plaatsgevonden in het kader van het verkrijgen van controle-informatie ten behoeve van de controle van de jaarrekening van organisaties met verregaand geautomatiseerde informatiesystemen (GIS), waarbij controle met behulp van brondocumenten rondom de computer niet meer mogelijk of niet meer efficiënt is. De accountant beschikt vanuit zijn deskundigheidsgebied in deze gevallen veelal niet meer over controlemiddelen om zelfstandig tot oordeelsvorming omtrent de getrouwheid van een jaarrekening te komen. De accountant zal daarom gebruik kunnen maken van de deskundigheid van de EDP-auditor. Dit artikel geeft uitsluitsel over de vraag aan welke voorwaarden moet zijn voldaan voordat een EDP-auditor een uitspraak over de betrouwbaarheid van de uitkomsten van de GIS op de saldibalans (object van onderzoek) kan doen in omgevingen met verregaand GIS.

De accountant zal doorgaans zelfstandig het totstandkomingstraject van saldibalans naar jaarrekening controleren vanwege het ontbreken van een adequaat stelsel van maatregelen van interne controle en de aard van de uitgevoerde journaalposten (niet-routinematig en veelal schattingsposten).

De Richtlijnen voor de Accountantscontrole schrijven voor dat de accountant altijd zelfstandig nog eigen controlewerkzaamheden dient te verrichten bij het verkrijgen van controle-informatie, hij moet altijd zelfstandig tot een oordeel komen. Vanuit het risicoanalysemodel zal de EDP-auditor met name de inschatting van het inherente en het internecontrolerisico kunnen onderbouwen door middel van het uitvoeren van een EDP-audit. De noodzaak voor de inzet van de EDP-auditor in de jaarrekeningcontrole is situatieafhankelijk, de complexiteit van de GIS en de deskundigheid van de accountant zijn hier bepalende factoren. Voorop staat, dat de accountant zich zelfstandig een oordeel kan vormen omtrent de uitkomsten van de werkzaamheden van de EDP-auditor.

De normen voor de EDP-audit op de betrouwbaarheid van de uitkomsten van de GIS op de saldibalans (verder te noemen de EDP-audit) zijn afhankelijk van de bepaling van de materialiteitsgrenzen die door de accountant zijn gesteld ten aanzien van de te controleren jaarrekening. Tevens zal het controlerisico (afhankelijk van het inherente risico en het internecontrolerisico) medebepalend zijn voor de normstelling bij de EDP-audit. De normen zullen voordat de EDP-audit wordt uitgevoerd door de EDP-auditor, worden afgestemd met de accountant.

De betrouwbaarheid van (de uitkomsten van) een GIS wordt grotendeels bepaald door computercontroles met een algemeen karakter, de general ICT controls, en computercontroles die zich richten op de werking van een specifieke applicatie, toepassingscontroles. General ICT controls hebben invloed op het inherente risico en het internecontrolerisico. Toepassingscontroles hebben invloed op het internecontrolerisico. Toepassingscontroles kunnen worden onderverdeeld naar invoercontroles, toegangscontroles, verwerkingscontroles en uitvoercontroles. Daarnaast zal de juistheid van de rekenregels binnen de GIS vastgesteld moeten worden. Al deze controles dienen ervoor zorg te dragen dat de gegevens op de saldibalans betrouwbaar zijn; de EDP-auditor zal de deugdelijke grondslag aan deze controles moeten ontlenen.

Ten aanzien van de uitvoering van de EDP-audit is een aantal randvoorwaarden van toepassing: de kwaliteit van de controles moet objectief meetbaar zijn, de methoden en technieken moeten voldoende controle-informatie verstrekken en tot slot moeten de uitkomsten van het onderzoek naar de kwaliteit van de controles (in bepaalde mate) vertaalbaar zijn naar de kwantitatieve normen van de accountantscontrole. Indien aan één of meer van deze randvoorwaarden niet voldaan is, kan geen sprake zijn van een deugdelijke grondslag voor het afgeven van een mededeling.

De aanpak van de EDP-audit kan als volgt worden weergegeven:

1. inzicht verkrijgen in processen en systemen die posten in de jaarrekening genereren, bepalen van afhankelijkheidsgraad van IT en uitvoeren van risicoanalyse op de processen;
2. normen (maatstaf voor hoeveel procent zekerheid kan worden verkregen ten aanzien van het inherente en internecontrolerisico) formuleren ten aanzien van de te onderzoeken general ICT controls en toepassingscontroles;
3. beoordelen van general ICT controls en evalueren uitkomsten voor de controleaanpak;
4. in kaart brengen en beoordelen van het aanwezige stelsel van beheersingsmaatregelen op de invoer, verwerking, uitvoer en bewaring van gegevens (beoordelen van toepassingscontroles) en evalueren van uitkomsten onderzoek voor de betrouwbaarheid van de gegevens op de saldibalans;
5. rapporteren uitkomsten van onderzoek aan accountant.

In dit onderzoek is vastgesteld dat bij de EDP-audit kan worden voldaan aan de hiervoor gestelde randvoorwaarden voor het verkrijgen van een deugdelijke grondslag voor het afgeven van een mededeling over de betrouwbaarheid van de uitkomsten van de

GIS. Met name de controle op de betrouwbaarheid van de registratie van geaccepteerde en uitgevoerde transacties zal in de audit aandacht dienen te krijgen.

CONCLUSIES

De accountant blijft eindverantwoordelijke voor het afgeven van de verklaring over de getrouwheid van de jaarrekening en zal daartoe zelfstandig controlewerkzaamheden dienen te verrichten.

Een EDP-auditor kan een uitspraak doen over de beweringen volledigheid, bestaan en accuratesse (kwaliteitsaspect: betrouwbaarheid) van één of meer posten in de saldibalans of de gehele saldibalans afhankelijk van de wijze van inrichting van de administratieve organisatie en interne controle, en van de toepassing van IT. Het object van onderzoek zal hierbij vooraf met de accountant worden afgesproken. De in de applicaties opgenomen rekenregels kunnen door de accountant worden beoordeeld op juistheid.

Er zijn in de uitvoering van de EDP-audit enkele zaken waarbij vakkundige oordeelsvorming van de EDP-auditor onontbeerlijk is. De accountant zal zich zelfstandig een oordeel moeten kunnen vormen omtrent de uitkomsten van de EDP-audit. Daarnaast kan de accountant ten aanzien van de uitvoering van de EDP-audit zekerheid ontlenen aan het feit dat de EDP-auditor als lid is ingeschreven in het Register van de Nederlandse Orde van Register EDP-Auditors (NOREA).

Het is een geruststelling dat jaarrekeningen ook in de toekomst bij voortschrijdende automatisering kunnen blijven worden gecontroleerd, mits is voldaan aan de voorwaarden die zijn gesteld ten aanzien van de administratieve organisatie en interne controle alsmede de toepassing van IT. Ongetwijfeld is hiermee de discussie over de inzet van EDP-auditors in de controle van de jaarrekening niet beëindigd; wellicht kan echter met dit artikel weer een stap worden gezet in de goede richting.

LITERATUUR

[Aren91] Prof. A.A. Arens en J.K. Loebecke, *Auditing an integrated approach*, Prentice-Hall International Editions, Englewood Cliffs, 1991.

[Donk95] Ir. J.A.M. Donkers, M. Groesz RE en ir. J.A. Verstelle RE, *Informatietechnologie, management control van de geautomatiseerde informatievoorziening*, Kluwer Bedrijfswetenschappen, 1995.

[Frie91] Prof. dr. A.B. Frielink RA en prof. H.J. de Heer RA, *Leerboek Accountantscontrole 2A: De algemene controle, typologie accountantscontrole in het kader van de accountantscontrole*, Stenfert Kroese, Leiden-Antwerpen 1991.

[Jenk92] B. Jenkins MA FCA, P. Cooke Bsc FCA, P. Quest MA FCA, *An Audit Approach to Computers*, The Institute of Chartered Accountants in England and Wales, Chartered Accountants' Hall, London 1992.

[Koed96] Drs. M.J.A. Koedijk RA en W.A. de Munck RA, *System Review Services*, Compact 1996/3, p. 21-28.

[KPMG94] *Handboek KPMG Audit Service*, KPMG, Amsterdam 1994.

[Munc95] W.A. de Munck RA, *Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering*, Compact 1995/3, p. 3-10.

[NIVR96] Koninklijk NIVRA, *Richtlijnen voor de Accountantscontrole*, Amsterdam 1996.

[IIAR91] The Institute of Internal Auditors Research Foundation, *Systems Auditability and Control, Module 2, Audit and Control Environment*, Altamonte Springs 1991.

[Velt95] Drs. P. Veltman RE RA, *Third party review en -mededeling bij uitbesteding van IT-services*, Compact 1995/3, p. 20-37.

W. de Korte RE RA
Is sedert 1990 werkzaam bij KPMG, gedurende een aantal jaren in de controlepraktijk, momenteel als senior EDP audit manager. Hij is verantwoordelijk voor de ontwikkeling van de general EDP audit practice van KPMG EDP Auditors in Rotterdam. Hierbij richt hij zijn aandacht onder andere op EDP-auditwerkzaamheden in het kader van de controle van de jaarrekening.

Het beheersen van risico's op het gebied van informatie-beveiliging: de visie van een klant

Mr. P. van Dijken

Het gebruik van de Code voor Informatiebeveiliging bij organisaties kan een goede basis zijn voor de general IT controls. Een beschouwing van een klant.

INLEIDING EN SAMENVATTING

Zowel externe accountants als hun klanten en gebruikers van informatietechnologie (IT) hebben een gemeenschappelijk probleem: hoe de betrouwbaarheid van de IT-infrastructuur vast te stellen, een infrastructuur waarvan de bedrijfsprocessen voor een groot deel afhankelijk zijn. Het leveren van goederen en diensten, het betalen van rekeningen, besluitvorming omtrent investeringen, kennisuitwisseling met collega's, dit alles wordt ondersteund door een steeds complexer wordende technologie. Het managen van de bedrijfsrisico's die hiermee samenhangen is een zorg voor zowel klanten als accountants, zoals dagelijks is te zien aan de openbare discussie over de vraag of bedrijven hun capaciteit om tijdig over te kunnen schakelen naar het jaar 2000 aan zouden moeten geven. In dit artikel[1] zal ik één aspect van deze gemeenschappelijke uitdaging nader behandelen: het managen van risico's omtrent de informatiebeveiliging.

Ik definieer informatiebeveiliging op de klassieke manier als het beveiligen van de betrouwbaarheid, integriteit en beschikbaarheid van informatie, in wat voor vorm ook. Een beveiligingsrisico is voor mij de mate van waarschijnlijkheid dat door mensen veroorzaakte schadelijke voorvallen optreden. Hier horen ook gebeurtenissen bij die niet door menselijke fouten zijn veroorzaakt, maar wel een zeer schadelijk effect kunnen hebben (bijvoorbeeld bomaanslagen). Ik zal dit gemeenschappelijke territorium nader bekijken door de volgende punten te behandelen:

- de strategische aspecten van IT zoals toegepast door de klant voor wie ik werk;
- de ontwikkelingen in beveiliging die relevant zijn voor deze klant; en
- de gekozen aanpak om de daaruit voortvloeiende risico's te beheersen.

In het laatste deel wordt de rol behandeld die interne en externe IT-beveiligingsspecialisten (ook wel EDP-auditor geheten) kunnen spelen om alle aandeelhouders te verzekeren dat 'alles onder controle is'.

1 Dit artikel is de weergave van een lezing, door de auteur gehouden op de KPMG EDP Audit Conference van 17 en 18 november 1997 te Barcelona.

IT-STRATEGIE

Sommige mensen beweren dat een bedrijfsstrategie op het gebied van IT niet bestaat: men zou het eerder moeten hebben over de bedrijfsstrategie die door IT mogelijk wordt gemaakt. De Koninklijke Nederlandse/Shell Groep (de eigenaar van mijn bedrijf) liet dit punt enige tijd geleden achter zich, toen de verantwoordelijkheid voor IT-zaken in handen werd gegeven van lijnmanagers, die met IT net zo om dienen te gaan als met andere bedrijfsinvesteringen. Dit principe is nog niet veranderd, maar er is in de loop der tijd wel een belangrijke aanpassing in aangebracht, naar aanleiding van de grote invloed van IT in de wereldwijde werkterreinen van de bedrijven van Shell. Een goed voorbeeld van deze aanpassing is het bestaan van de functie van corporate Chief Information Officer in de nieuwe Shell-organisatie. Deze functionaris houdt zich bezig met IT-aspecten die binnen de hele Groep veel voorkomen. De individuele bedrijven (downstream of upstream) hebben hun eigen IT-strategieën. Samen maken zij het geheel uit van de manier waarop de Groep IT gebruikt.

Waarom is deze IT-strategie voor de hele Groep opgezet? Het antwoord is: het inzicht dat kennis, know-how en informatie de kern zijn van wat we doen. IT, als het belangrijkste voertuig voor archiveren, communicatie, opvragen, en het transformeren en presenteren van kennis, moet alles mogelijk maken. Daarom zijn overkoepelende normen noodzakelijk voor de IT-infrastructuur, zodat kennis en informatie vrij en tegelijkertijd veilig kunnen worden uitgewisseld. De strategische doelstelling is dus:

De Groep moet een wereldwijde informatie-infrastructuur hebben, alleen daar gedifferentieerd waar noodzakelijk voor de behoeften van de bedrijven.

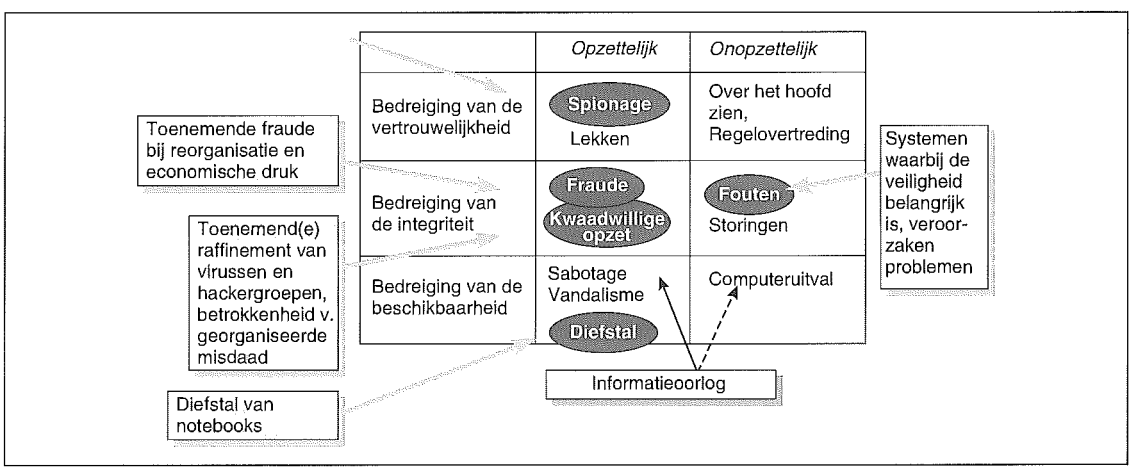
Door deze infrastructuur kan personeel binnen de Groep (onder andere) elektronisch samenwerken en zo specialismen verstevigen en 'best practices' uitwisselen. Het stelt de bedrijven van de Groep verder in staat veilig elektronisch zaken te doen met klanten, leveranciers, en onderling. Maar bovenal moedigt het aan om te leren, als een noodzaak om te overleven. Een artikel in het september/oktobernummer van Harvard Business Review geeft inzicht in de drijvende krachten binnen de olie-industrie, vanuit een onafhankelijk, gezaghebbend oogpunt, namelijk de Chief Executive Officer van British Petroleum, John Browne. Volgens Browne is leren de basis van het vermogen van een bedrijf om zich aan te passen aan een snel veranderende omgeving. Om meerwaarde te genereren voor de aandeelhouders moet het bedrijf vooral béter leren dan de concurrenten, en die kennis sneller en wijder inzetten (een voorbeeld: in 1995 waren er gemiddeld 100 dagen voor nodig om een diepzeebron te boren; nu nog slechts 42). Eén van de belangrijkste middelen om een voorsprong te creëren op concurrenten (om kennis te verkrijgen en kennis door te geven) is IT. Vanuit het oogpunt van deze capaciteitsvergroting betekent IT dat men oude opvattingen zoals het scheiden van netwerken vanuit 'de behoefte om overzicht te hebben' op moet geven. Er is niet veel ruimte over voor wat ik 'beveiligingsstokpaardjes' zou willen noemen, ofwel beveiligingsregels die niet zijn opgesteld met het oogmerk om bij te dragen aan bovengenoemde strategische IT-doelstellingen.

Wat is er nodig om dit te bereiken? Belangrijke elementen van de Shell Group-infrastructuur zijn een wereldwijd netwerk, het Group intranet ('ShellWideWeb'), elektronische berichtgeving, standaarddesktops en -servers, een gezamenlijke Groepsdirectory, en natuurlijk een aantal beleidsregels omtrent informatiebeveiliging, die de veiligheid van de informatieactiva van de Groep waarborgen. Dit beveiligingsbeleid moet voldoen aan:

- de Code of Practice for Information Security Management (British Standard BS7799, van februari 1995, meer hierover verderop);
- de aanwezigheid van een firewall die voldoet aan de technische normen van de Groep (die ik hier niet bespreek), namelijk wanneer netwerken zijn verbonden met niet-betrouwbare domeinen;
- het gebruik van goedgekeurde cryptografische technologie om zeer gevoelige zakelijke informatie te beschermen (valt ook buiten dit artikel).

TRENDS IN (IT-) BEVEILIGINGSRISICO'S

Binnen Shell zien wij geen verschil tussen de gevaren voor het bedrijf in het algemeen en gevaren voor de veiligheid van de IT-infrastructuur. De laatste gevaren kunnen wel technisch complexer zijn, bijvoor-



Figuur 1.
Soorten bedreigingen.

beeld in het geval van een samenzwering om een zwakke plek in het Electronic Funds Transfer-systeem uit te buiten. Maar de gevarenbron is dezelfde: crimineel gedrag van mensen. In deze paragraaf wordt met 'wij' bedoeld: de adviseur van de Shell International Group Security, en mijzelf: adviseur in de Information Security Services. Een goed voorbeeld in dit verband is diefstal van notebooks: stelen is een fysieke daad, verbonden met direct geldverlies. Als het notebook gevoelige bedrijfsinformatie bevat kan het resulterende verlies veel groter zijn dan de directe schade. Het verloren notebook kan ook een potentiële achterdeur zijn voor hackers, als ermee via het openbare net ingebeld kan worden.

Sinds het einde van de koude oorlog doen zich drie belangrijke ontwikkelingen voor in beveiligingsrisico's:

1. grotere onvoorspelbaarheid en instabiliteit van de veiligheid;
2. grotere risico's met betrekking tot informatie;
3. meer mogelijkheden voor misbruik van IT-systemen.

De gevarenbronnen die we kunnen onderscheiden zijn:

– *Nationale veiligheidsdiensten* verzamelen informatie om de concurrentiepositie van hun binnenlandse bedrijven te verstevigen. Gebruikte technieken zijn bijvoorbeeld: interceptie van communicatie, computer hacking, fysieke inbraak, werven van personeel/aannemers, afluisteren met onder andere audiomiddelen, en afkijken.

– *Illegale information brokers* (die bijvoorbeeld aannemers helpen opdrachten binnen te slepen) vormen een bekend verschijnsel in de olie-industrie. De gebruikte technieken omvatten het werven van personeel/aannemers, fysieke inbraak en afluisteren.

– *Agressieve bedrijfsspionagebureaus* worden steeds vaker ingehuurd om achter bepaalde bedrijfsinformatie te komen. Dit soort bureaus heeft soms voormalig veiligheidsdienstpersoneel in dienst, met uitgebreide spionagevaardigheden. Onder de toegepaste technieken vallen bijvoorbeeld het werven van personeel/aannemers, het zich voordoen als headhunters, computer hacking, fysieke inbraak, en audio-afluistertechnieken.

– *Militante activisten* staan erom bekend dat ze vooral geïnteresseerd zijn in informatie op het gebied van het milieu, en in personeelsgegevens zodat ze individuele medewerkers kunnen bestoken. Onder de toegepaste technieken zijn het werven van personeel/aannemers, en fysieke inbraak.

– *Militante extremisten* kunnen bomaanslagen plegen of 'denial-of-service'-aanvallen plegen op computers, dit om de bedrijfsactiviteiten te verstoren.

– *Criminelen*, meestal in georganiseerde groepen of opererend voor andere geïnteresseerde partijen, kunnen het op de PC-uitrusting gemunt hebben, en vooral op notebook computers. Poging tot afpersing is een andere techniek, met als pressiemiddel bijvoorbeeld virussen die gegevens ontoegankelijk maken, of andere aanvallen die het computersysteem verstoren.

– *Hackergroepen*, gebruiken vaak zeer geraffineerde middelen om in computers in te breken. Ze kunnen deze middelen toepassen vanuit het oogmerk van financieel gewin, om politieke redenen, of gewoon om de uitdaging. Computer hackers worden soms door derden ingehuurd (waaronder bovenstaande groepen).

– *Kwaadaardige software* zoals PC-virussen kunnen per ongeluk of expres in een systeem terechtkomen. Dit gevaar is toegenomen, bijvoorbeeld door de toename van de Internet mail file attachments en de groei in elektronische document managing systems, maar ook door de toegenomen mogelijkheden tot toegang op afstand in netwerken, systemen en toepassingen.

– *Natuurrampen of rampen veroorzaakt door mensen*, zoals brand, kunnen informatie vernietigen en IT-systemen onbruikbaar maken.

Tot slot: In zichzelf onschuldige daden, zoals het doorgeven van een waarschuwing over een e-mailvirus, kunnen een stortvloed van berichten veroorzaken, waardoor een netwerk overbelast kan raken. En, nu we het informatietijdperk binnengaan zal onze informatie onvermijdelijk kwetsbaarder worden voor de gevaren die ik hierboven heb genoemd, wegens de volgende ontwikkelingen:

– Onze bedrijfsactiviteiten worden steeds afhankelijker van de doorlopende beschikbaarheid van IT-diensten.

– Wereldwijde IT-netwerken bieden nieuwe mogelijkheden om toegang te krijgen tot computersystemen, of gegevens of wachtwoorden te onderscheppen vanaf verafgelegen locaties.

– Bedrijfsactiviteiten zoals kennismanagement en samenwerking van teams via computers, zullen ertoe leiden dat bedrijfsinformatie beter en makkelijker beschikbaar wordt.

– Technieken en instrumenten om ongeautoriseerd toegang te krijgen tot computers worden steeds veelzijdiger, beter toegankelijk en makkelijker te gebruiken.

– Nieuwe technologieën zijn moeilijker te beveiligen, te beheersen en te controleren.

Samenvattend: Als typische 'gebruikersindustrie' zijn we een tijdperk binnengegaan waarin de kunst om informatiebeveiligingsrisico's te beheersen een eerste vereiste is geworden.

HET BEHEERSEN VAN INFORMATIEBEVEILIGINGSRISICO'S

Sinds 1991 hebben de bedrijven van Shell hun aanpak in het managen van informatiebeveiligingsrisico's gebaseerd op het baseline security concept. Donn Parker (van S(tanford) R(esearch) I(nternational)) heeft dit concept opgesteld, en heeft het grootste deel van zijn loopbaan als adviseur gewijd aan het verzamelen, analyseren en documenteren

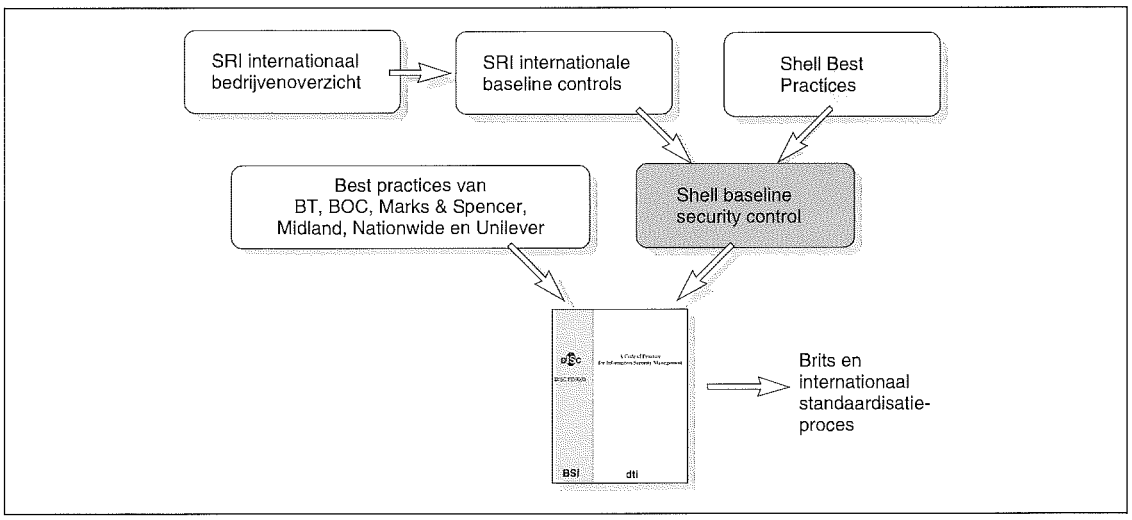
van baseline controls van veel toonaangevende bedrijven (dit behoort als kernmateriaal toe aan het International Information Integrity Institute, of I-4). De baselines zijn nooit gepubliceerd, maar wel door ons gebruikt om onze eigen versie te ontwikkelen. Deze aanpak heeft zich voor ons bewezen, omdat we er met de tijd door leerden hoe een gewone, technologieonafhankelijke referentiestandaard kon worden gebruikt voor een breed spectrum van bedrijfsomgevingen en IT-infrastructuren (van mainframes tot notebooks).

Tegelijkertijd promoten externe auditorganisaties hun eigen aanpak van dit probleem. Deze aanpak vertoonde natuurlijk wel opvallende overeenkomsten met de I-4 adviesrichtlijnen (bijna alle Big Six waren lid op dat moment), hetgeen te verwachten was. Maar de verwerking van al deze ervaringen verschilde: in mijn regio verdween het controleren van computeractiviteiten als specialisme ('Wat is zo bijzonder aan het werken met computers'). De meeste auditbureaus zagen echter de kans schoon om hun eigen concepten en beveiligingscontrolenormen op de markt te brengen, waarbij zij zich onderscheidden van concurrenten. Ik heb de afgelopen jaren verscheidene malen Shell IT-managers in verschillende landen met externe auditors zien worstelen over IT-controleproblemen (als een (duur) gevolg daarvan). De auditors propageerden hun normen, de Shell IT-manager de Shell baseline controls. Beiden hadden natuurlijk gelijk. De directie van Shell had de indruk dat het implementeren van de baselines (voorzien van step-outs voor hogere of lagere risico's) hen uit de gevarenzone hield. Externe auditors hadden geen bekend referentiekader om de inspanningen van Shell te beoordelen (en propageerden derhalve hun eigen normen).

Een initiatief van het Britse Ministerie van Handel en Industrie om ons samen met zes andere bedrijven uit te nodigen (elk bedrijf uit een verschillende industriële branche) brak het ijs in 1993. In een sfeer van openheid en mededeelzaamheid droeg elk bedrijf bij aan de Code of Practice for Information Security Management (eerst uitgegeven als DISC PD0003, om in 1995 aangenomen te worden als de Britse Standaard 7799; in Nederland met steun van het Ministerie van Economische Zaken vertaald en uitgegeven door het Nederlands Normalisatie Instituut in Delft als de Code voor Informatiebeveiliging, een leidraad voor beleid en implementatie). Doordat bij het opstellen en uitgeven alleen 'gebruikers-bedrijven' waren betrokken, kon dit proces relatief snel verlopen. Zoals te verwachten duurde het langer voordat partijen die er niet bij waren betrokken, zoals leveranciers of EDP-auditororganisaties, de Code accepteerden. Op basis van deze ervaringen drong het team dat de Code naar het Nederlands vertaalde erop aan dat vertegenwoordigers uit de informatiebeveiligingsbranche in de feedbackcyclus werden opgenomen. Tijdens dit latere stadium van het opstellen van de Code verzamelden we kwalitatief goede feedback. De Code ging zijn eigen weg door het internationale normeringsproces, en werd DIS 14980. De Code is door een aantal landen binnen en buiten Europa geadopteerd, en wordt gebruikt in andere landen (bijvoorbeeld de Verenigde Staten) (zie NIST Special Publication 800-14, pagina 12).

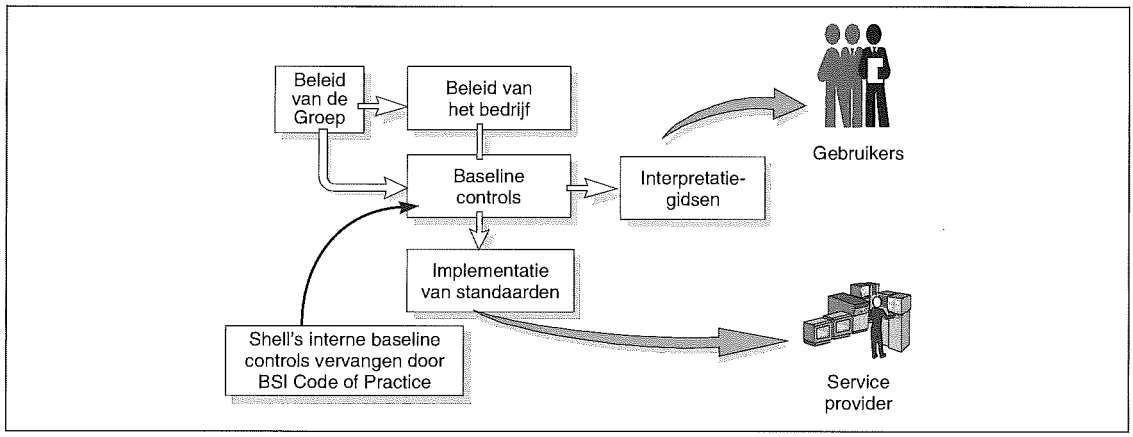
De positieve ontvangst van de Code bij Nederlandse beveiligingsexperts in de overheidssector, gebruikersindustrieën en particuliere adviesbureaus kweekte de juiste voedingsbodem om een stap verder te gaan met de Code. Dit mondde uit in het 'ACB-project', gesponsord door het Nederlandse Ministerie van Economische Zaken, dat ten doel had het eerste 'Schema voor zelfbeoordeling en certificatie van informatiebeveiliging volgens BS7799' op te stellen. Het behoeft geen betoog dat Shell hier graag aan meewerkte. Mijn bedrijf (Shell Information Services B.V. & Ltd) ontving het certificaat op 1 september 1997 uit handen van KPMG Certification, die zojuist de status had verworven om als certificerende instantie op te treden voor de BS7799.

Wat betekent dit nu in termen van het beheersen van informatiebeveiligingsrisico's? Zal een BS7799-certificaat het risico verkleinen dat een hacker ons netwerk binnendringt? Het antwoord is ja, maar niet op een directe manier. Het certificaat dwingt ons om een toezichtkader op te zetten en te onderhouden, waarmee dit soort risico's actief onderkend wordt, of in beveiligingstermen: wat ons waakzaam houdt. Niet het document maar het proces om het document te verkrijgen is belangrijk. De nauwe samenwerking met een Big Four bedrijf is in meerdere opzichten nuttig gebleken: auditors van KPMG



Figuur 2. An International Pedigree.

Mr. P. van Dijken
Is werkzaam als manager information security services bij Shell Services International B.V. te Rijswijk (Z.H.). Hij is verantwoordelijk voor diensten en producten inzake informatiebeveiliging voor Shell-maatschappijen wereldwijd.



Figuur 3. Control Infrastructure.

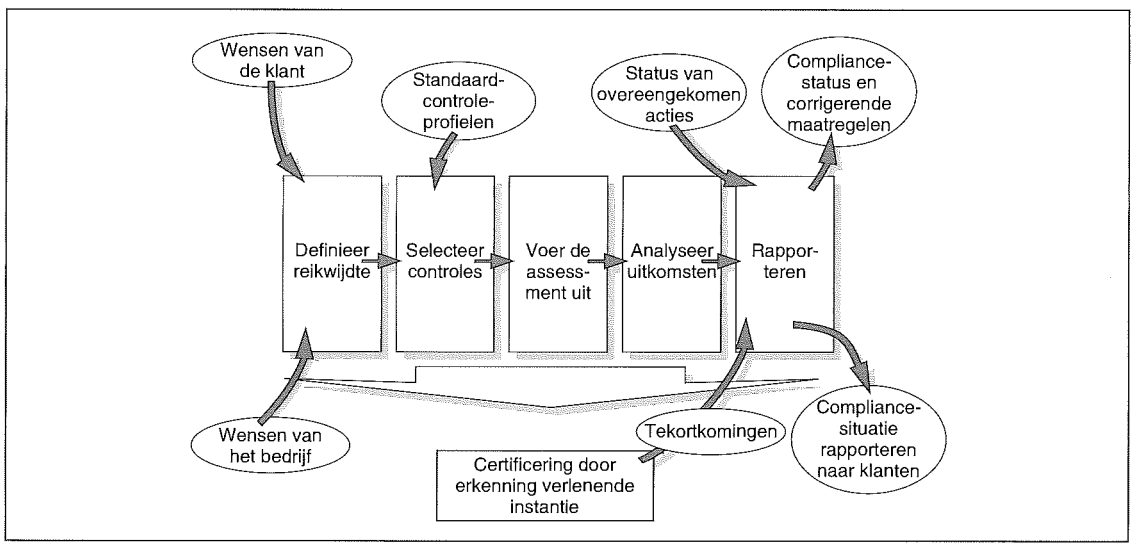
EDP die voor andere onderdelen van de Koninklijke/Shell werken zien mogelijkheden om het certificaat elders binnen de organisatie te hergebruiken. De voordelen: potentiële kostenbesparingen voor de auditing van IT controls binnen en buiten mijn bedrijf. Onze (interne) klanten waren enthousiast: certificering door onafhankelijke externe experts voor een internationale, openbare standaard betekent meer voor hen dan interne pogingen om aan interne regels te voldoen. Binnen het nieuwe Shell is deze manier om aan klanten tegemoet te komen de sleutel tot succes.

Een voorbeeld (uit Shell) is weergegeven in figuur 4.

TOT SLOT

Het managen van informatiebeveiligingsrisico's is cruciaal voor bedrijven. De keuze die in het verleden was gemaakt voor de baseline control-aanpak veroorzaakte geschilpunten, vooral tussen Shell IT-managers en EDP-auditexperts, over de hele wereld. De groeiende aanvaarding van gebruikersondersteunende, gecodificeerde, openbare en internationale security baselines heeft dit beeld veranderd. KPMG Certification en KPMG EDP Auditors hebben hier professioneel op ingespeeld en de uitdaging geaccepteerd om zich als certificerende instantie op te werpen. Binnen Shell managen we nog steeds onze eigen risico's, maar het proces kan worden verantwoord, en kostenbesparingen zijn mogelijk gemaakt. De certificering onder BS7799 opent deuren om het IT-gebruik naar andere niveaus te tillen (bijvoorbeeld de implementatie van nieuwe netwerkbeveiligingsconcepten, waarmee wereldwijde toepassingen worden ondersteund). Ik zie een succesvolle samenwerking voor me, in plaats van vruchteloze discussies over de installatie van bepaalde beveiligingsvoorzieningen op standaard Windows NT-computers.

Figuur 4. Certification Maintenance Process.



TER AANVULLING

GEBRUIK VAN DE CODE VOOR INFORMATIEBEVEILIGING VOOR DE GENERAL ICT CONTROLS

Dr.ir. P.L. Overbeek

Wat is de Code

De afhankelijkheid van organisaties van informatie, computers en netwerken neemt steeds meer toe. Tegelijkertijd neemt ook de kwetsbaarheid van de informatie in de IT-infrastructuur toe, bijvoorbeeld vanwege de toename van het aantal samenwerkingsverbanden, en, meer algemeen, vanwege de toegenomen distributiegraad van informatie. Daarom moet binnen een organisatie, of – in het geval van informatie-uitwisseling – ook tussen organisaties, een stelsel uniforme spelregels voor de informatiebeveiliging worden gehanteerd. De Code voor Informatiebeveiliging voorziet hierin in de vorm van een eenvoudig managementraamwerk en een evenwichtig stelsel maatregelen die een 'baseline' (basisniveau) vormen voor informatiebeveiliging. Veel bedrijven hanteren de Code als uitgangspunt voor hun informatiebeveiliging.

De Code in relatie tot de general ICT controls
De controls in de Code, daar veelal beveiligingsmaatregelen genoemd, zijn weliswaar anders omschreven, maar omvatten de general ICT controls geheel. Het is eenvoudig mogelijk de audit van de general ICT controls uit te voeren door middel van een audit naar geselecteerde controls (maatregelen) uit de Code.

Audits op basis van de Code

Audits in het kader van de jaarrekeningcontrole kennen een specifieke aanpak. Hieronder wordt een uiteenzetting gegeven.

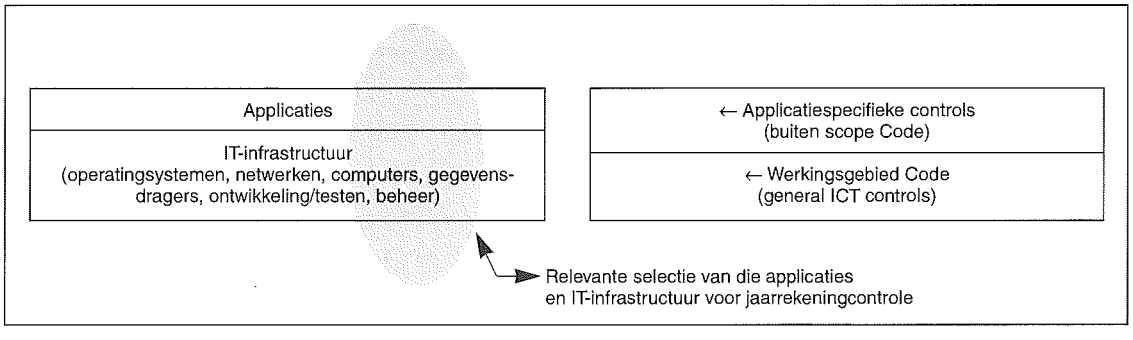
Specifieke jaarrekeningaudit
Indien een audit specifiek in verband met jaarrekeningcontrole plaatsvindt, zal deze gericht zijn op die afdelingen en/of die informatie en systemen die van belang zijn in verband met de jaarrekeningcontrole. Zo'n audit kan gebaseerd worden op de Code, waarbij de controls voor de desbetreffende objecten dienen te worden vastgesteld.

Steunen op interne auditresultaten
Voor bedrijven die de Code als beleidsuitgangspunt hanteren, kan in de jaarrekeningcontrole tevens worden gesteund op de resultaten van de in de Code voorgeschreven interne 'self assessments'. Deze self assessments zijn eigen beoordelingen (en dus niet onafhankelijk) en de resultaten hiervan dienen derhalve van onafhankelijke zijde te worden gecontroleerd, bijvoorbeeld door een steekproef uit te voeren op de resultaten van de self assessments. Soms vindt reeds een eerste review plaats door de interne auditors, in welk geval hun resultaten mede in de beeldvorming kunnen worden betrokken. Ook hiervoor geldt dat de resultaten moeten worden geverifieerd.

Afbakening: wat is de Code wel en wat niet in relatie tot de jaarrekeningcontrole
Figuur 1 toont gearceerd een selectie van de IT-infrastructuur die van specifiek belang is voor de EDP-audit in verband met de jaarrekeningcontrole, bijvoorbeeld een financieel-administratief informatiesysteem, met de infrastructuur waar dit systeem gebruik van maakt (computers, netwerken, operatingsystemen en applicaties). De onderste helft van de figuur is het werkingsgebied van de general ICT controls, die, zoals hierboven betoogd, kunnen worden ingevuld door de Code. Specifiek voor de EDP-audit ten behoeve van de jaarrekeningcontrole hoeft dus alleen dit gedeelte geaudit te worden met de Code als normenkader. De bovenkant van de figuur vertegenwoordigt een groep van de applicatiespecifieke controls (die, bijvoorbeeld, toegangsrechten binnen de applicatie regelen). Deze vallen buiten het werkingsveld van de Code en worden op de gebruikelijke wijze geaudit.

Certificatie op basis van de Code voor Informatiebeveiliging

Een belangrijke trend is de opkomst van certificatie van beveiliging op basis van de Code (BS7799-certificatie. Deze certificatie geeft bedrijven meer zekerheid dat het vereiste niveau van beveiliging ook *blijvend* wordt geboden, aangezien certificatie vergezeld gaat van periodieke controle-audits. In Nederland zijn momenteel twee partijen erkend door de Raad voor Accreditatie als certificerende instantie voor dit certificatieschema. De audits worden op basis van de regels van de Raad voor Accreditatie uitgevoerd. De eisen die de Raad stelt aan de auditors zijn andere eisen dan door NOREA worden gesteld. Het certificatieschema schrijft voor dat de auditors ten minste vier jaar ervaring in de IT en ten minste twee jaar in de beveiliging hebben. Tevens wordt aantoonbare auditervaring vereist. Het certificatieschema schrijft



Figuur 1.

Dr.ir. P.L. Overbeek is senior manager bij KPMG EDP Auditors.

echter niet voor dat de audits worden uitgevoerd door Register EDP-auditors (RE's), die gebonden zijn aan de NOREA-gedragsregels. De nu erkende certificeerders geven hier dan ook een andere invulling aan.

Voor de beeldvorming van de accountant kan worden gesteund op certificatie op basis van de Code, indien rekening wordt gehouden met de verschillen tussen certificatie-audits en audits in het kader van de jaarrekening. Verschillen tussen de BS7799-certificatieonderzoeken en audits in het kader van de jaarrekening bestaan namelijk, en zijn relevant. De belangrijkste verschillen zijn:

- BS7799-certificatieonderzoeken richten zich op de volle breedte van de Code (binnen de scope van het onderzoek) en voeren daarbinnen steekproeven uit. Jaarrekeningaudits richten zich doorgaans alleen op specifiek voor de jaarrekening interessante systemen. Derhalve moet worden geverifieerd dat de voor de jaarrekening relevante systemen recent geaudit zijn.

- BS7799-certificatieonderzoeken kunnen worden uitgevoerd door 'auditors' met beperkte ervaring (vier jaar) die niet gebonden zijn aan de NOREA-richtlijnen. Daarom moet worden geverifieerd dat RE's betrokken zijn bij het onderzoek en dat volgens de NOREA-richtlijnen is gewerkt.

- De minimale diepgang van BS7799-certificatieonderzoeken is in technische zin minder dan wat normaal is bij jaarrekeningonderzoeken. In de praktijk hoeft dit geen probleem te zijn omdat het BS7799-certificatieonderzoek steunt op self assessments en technical compliance audits, die naar verwachting wel de gewenste diepgang hebben.

- Tot slot: de Code bevat geen uitgebreide applicatiespecifieke controls, die veelal wel voor de jaarrekeningcontrole van belang zijn.

De volgende gedragsregels kunnen dienen indien de accountant of EDP-auditor in zijn controlewerkzaamheden 'stuit' op een certificaat op basis van de Code (voor deze gedragsregels is een parallel getrokken met het NIVRA-Studierapport Accountant en ISO9000-certificatie).

- Vraag het certificaat en het auditrapport op bij de gecertificeerde organisatie. Toestemming van de gecertificeerde organisatie is nodig omdat de certificatieonderzoeken op basis van de Code met een ander doel worden uitgevoerd dan die voor de jaarrekeningcontrole. Deze toestemming is ook nodig omdat certificaten ook kunnen worden afgegeven en opgevraagd door derde partijen. Vervolgens:
  - verifieer dat de scope van het onderzoek het beoogde object van onderzoek omvat;
  - kijk in het auditrapport of een non-conformity bestaat met betrekking tot het onderzoeksobject en/of de voor de genral ICT controls relevante 'controls' uit de Code. Is dit het geval, dan kan, naar inzicht van de auditor, aanvullend onderzoek nodig zijn. De BS7799-audits laten namelijk ruimte voor een beperkt aantal verbeterpunten;
  - verifieer dat in het certificatieonderzoek het relevante onderzoeksobject ook daadwerkelijk aan bod is gekomen. Het certificatieonderzoek gaat namelijk over een beeld over de gehele organisatie en alle systemen, terwijl in het kader van de jaarrekeningcontrole specifieke systemen van belang zijn.

- Indien deze punten vragen open laten, kan voorts worden gesteund op informatie uit het documentatieonderzoek, waaronder de 'eigen normen' met betrekking tot het onderzoeksobject.

- Vervolgens kan, indien de auditor nog meer informatie nodig heeft, uit het implementatieonderzoek de volgende informatie van de desbetreffende organisatie-eenheid beschikbaar zijn (het is niet verplicht deze informatie aan te houden): self assessments, beveiligingsjaarplannen, en – indien control 10.2 (technical compliance testen) onderdeel is van de eigen norm – de technical audit reports.

- Indien de auditor nog immer onvoldoende informatie heeft, dan is kennelijk een aanvullende audit nodig. Voer deze uit en zorg voor adequate documentatie zodat deze audit in toekomstige BS7799-verificatie-audits kan dienen ter ondersteuning van de implementatie van control 10.2.

Samenvatting

Samenvattend kan worden gesteld:
- de Code voor Informatiebeveiliging vormt een invulling van de general ICT controls en is daarmee goed in te zetten ter ondersteuning van de jaarrekeningcontrole;
- hulpmiddelen voor audits zijn beschikbaar;
- algemene en specifieke audits zijn mogelijk;
- erkende certificeerders mogen certificaten uitgeven voor informatiebeveiliging op basis van de Code;
- vele bedrijven volgen de Code als beleid;
- grote bedrijven verwachten ook van hun zakenpartners dat ze *aantoonbaar* gaan voldoen aan de Code voor Informatiebeveiliging, bijvoorbeeld door middel van certificatie;
- indien de auditor in het kader van de jaarrekeningcontrole op een BS7799-certificaat stuit kan hier onder specifieke voorwaarden gebruik van worden gemaakt.

In de volgende Compact zal een uitgebreid artikel verschijnen over het certificatieschema voor certificatie op basis van de Code voor Informatiebeveiliging.

Accountantscontrole, COSO en CobiT

Mw.drs. A.J.M. Koopman

De vraag waar accountants en IT-auditors mee worstelen bij de beoordeling van IT is aan welke eisen moet worden voldaan om te kunnen stellen dat de IT 'in control' is. De opzet van CobiT is deze vraag te beantwoorden door het definiëren van beheersingsdoelstellingen voor standaard-IT-processen, zodanig dat de kwaliteit van de geproduceerde informatie voldoet aan de door de bedrijfsprocessen gestelde criteria.

INLEIDING

De vraag waar auditors (accountants en IT-auditors) mee worstelen bij de beoordeling van informatietechnologie (IT) is: aan welke eisen moet worden voldaan om te kunnen stellen dat de IT 'in control' is? De opzet van CobiT (Control Objectives for Information and related Technology) is deze vraag te beantwoorden door het definiëren van beheersingsdoelstellingen voor standaard-IT-processen, zodanig dat de kwaliteit van de geproduceerde informatie voldoet aan de door de bedrijfsprocessen gestelde criteria ([ISAC96]).

De ontwikkeling van CobiT hangt samen met de ontwikkeling van nieuwe modellen voor de beheersing van organisaties. Voorbeelden hiervan zijn het COSO-rapport in de Verenigde Staten, het CoCo-rapport in Canada en het Cadbury-rapport in het Verenigd Koninkrijk. In deze rapporten wordt de definitie 'internal control' breder geïnterpreteerd dan voorheen gebruikelijk ([ISAC95]). 'Internal control' behelst het gehele interne beheersingssysteem. CobiT slaat in feite een brug tussen de beheersingsmodellen voor organisaties en de beheersingsmodellen voor IT. Beheersing van de organisatie omvat immers ook de beheersing van de IT.

Er zijn vele modellen ontwikkeld om de beheersing van de IT gestalte te geven en te beoordelen. CobiT geeft echter een globaal en overkoepelend concept voor de IT-ondersteuning van bedrijfsprocessen ([Kord97]). CobiT is een niet-technisch, internationaal bekend referentiekader voor IT-gebonden beheersingsmaatregelen. De bestaande modellen voor de IT-beheersing geven geen totaalconcept voor de ondersteuning van bedrijfsprocessen, zijn technisch georiënteerd en spreken niet de taal van de managers van de organisatie ([Kord97]).

Dit artikel behandelt het gebruik van CobiT als hulpmiddel voor de beoordeling van de beheersing van de IT in het kader van een moderne controleaanpak ten behoeve van een jaarrekeningcontrole door de accountant. Een moderne controleaanpak betekent zowel voor de interne als de externe accountant een verbreding van zijn/haar werkzaamheden. COSO geeft hiertoe een praktische handreiking.

Hierna wordt eerst het COSO-rapport nader toegelicht. Vervolgens worden de uitgangspunten van het CobiT-rapport gedetailleerd besproken. Daarna wordt ingegaan op de wijze waarop het CobiT-framework kan worden gebruikt in de controlepraktijk van de accountant. Hierbij wordt tevens ingegaan op de wijze waarop de werkverdeling tussen de accountant en de IT-auditor gestalte kan krijgen. Vervolgens worden enkele kanttekeningen bij het CobiT-rapport geplaatst. Beveiligingsnormen komen daarna kort aan de orde. Ten slotte wordt de relatie tussen accountantscontrole, COSO en CobiT geëvalueerd.

HET COSO-RAPPORT

In 1987 heeft de 'National Commission on Fraudulent Financial Reporting' (Treadway) bekend gemaakt dat de ondergang van organisaties in de meeste gevallen niet werd veroorzaakt door slecht boekhouden, maar door slechte ethische waarden, corruptie in de top van de organisatie, onbekwaamheid en slechte communicatie. Vanaf dat moment zijn diverse rapporten inzake internal control gepubliceerd (o.a. COSO, Cadbury en CoCo). In deze rapporten werd de definitie 'internal control' breder geïnterpreteerd dan voorheen gebruikelijk ([ISAC95]). Internal control behelst het gehele interne beheersingssysteem. Het COSO-rapport geeft aan dat internal control verder gaat dan het controleren van de betrouwbaarheid van de financiële gegevens waar de aandacht van de accountant zich historisch op richtte. In een moderne controleaanpak, breder dan alleen de handtekening bij de jaarrekening, wordt ook aandacht besteed aan de efficiency en effectiviteit van de processen. Een ander belangrijk element is de naleving van wet- en regelgeving.

'Internal control' behelst het gehele interne beheersingssysteem, waaronder IT.

Voor aandeelhouders en andere belanghebbenden van organisaties is het in toenemende mate een belangrijke vraag of de onderneming 'in control' is of-wel: of de activiteiten en de daarbij behorende risico's in voldoende mate worden beheerst en gestuurd teneinde de continuïteit van de organisatie te kunnen waarborgen ([Paap97]). Hieronder valt natuurlijk ook de beheersing van de IT in de organisatie.

Het begrip internal control moet overigens niet worden verward met management control. Volgens het COSO-rapport is het systeem van interne beheersing een onderdeel van het managementproces (en daarmee van management control). Het bepalen van ondernemingsdoelstellingen, strategische planning en risicomanagement is een voorbeeld van managementactiviteiten die niet tot internal control behoren ([Boer95]). In figuur 1 wordt dit weergegeven.

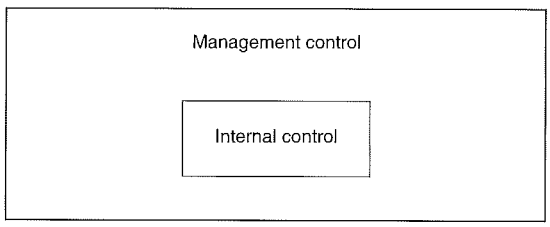
In het COSO-rapport wordt internal control gedefinieerd als een proces (sterk beïnvloed door het management en het personeel van een organisatie) ontworpen om redelijke zekerheid te verkrijgen over het bereiken van doelstellingen op de gebieden:
- effectiviteit en efficiency van bedrijfsprocessen (inclusief beveiliging van activa);
- betrouwbaarheid van financiële verslaggeving (intern en extern);
- naleven van regels en wetten;

Het COSO-framework bestaat uit drie dimensies, die in een kubus kunnen worden weergegeven (zie figuur 2):
1. components;
2. control objectives (effectiviteit en efficiency van bedrijfsprocessen, betrouwbaarheid informatie, naleven van regels en wetten);
3. activity/units (interne beheersing is relevant voor de gehele organisatie en/of elk van haar activiteiten of onderdelen).

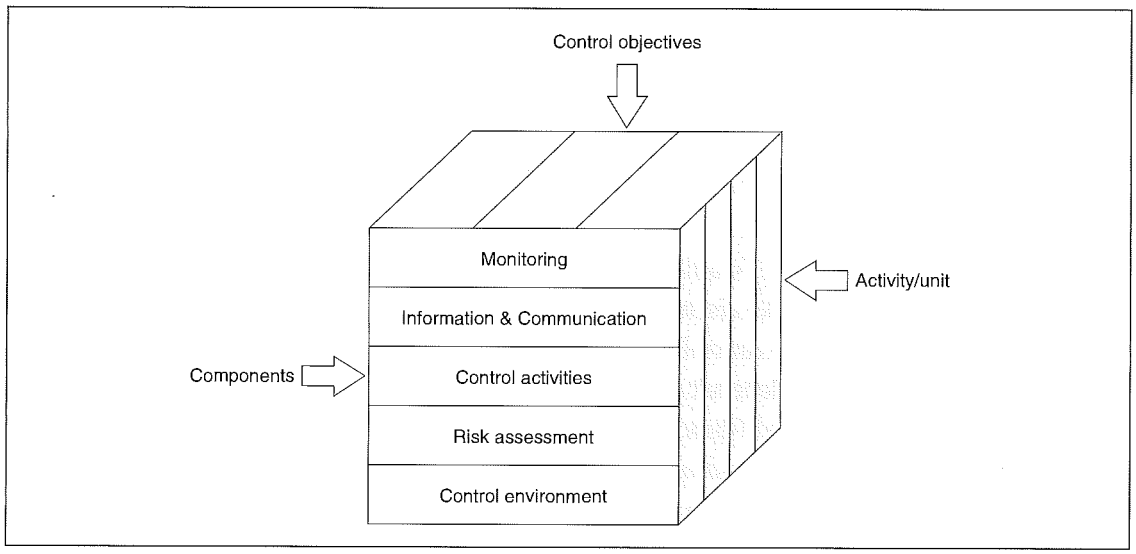
De componenten van de 'COSO-kubus' geven in feite de managementcyclus aan. Onder de vijf componenten wordt het volgende begrepen:

Control environment
De control environment is de algemeen organisatorische fundering voor de interne beheersing. Hierbij is de houding van de top van de onderneming van belang, de invloed van de Raad van Bestuur op het beheersingsproces en de betekenis die zij geven

Figuur 1.
Relatie internal control en management control.



Figuur 2.
'COSO-kubus' ([COSO94]).



aan het interne beheersingsproces. Toegespitst op de automatiseringsorganisatie zijn voorbeelden: integriteit van de leiding, ethische waarden, deskundigheid van personeel, managementfilosofie en human resources. Deze zijn natuurlijk gelijk aan die voor andere onderdelen van de organisatie, al kan de invulling een ander accent hebben.

Risk assessment
Risk assessment is een primaire voorwaarde om een effectieve interne beheersing mogelijk te maken. Relevante interne en externe (IT-)risico's die het bereiken van doelstellingen bedreigen, dienen te worden geïdentificeerd en geanalyseerd. Bedreigingen specifiek voor de IT-omgeving zijn bijvoorbeeld het niet beschikbaar zijn van het netwerk.

Control activities
Onder control activities moeten de specifieke richtlijnen en procedures worden verstaan die zijn geïmplementeerd om de geïdentificeerde risico's te verkleinen. Voorbeelden zijn fysieke en logische toegangsbeveiliging.

Information & Communication
Informatie en de interne en externe communicatie hiervan is een belangrijke component. Hierbij kan een onderscheid worden gemaakt tussen monitoringinformatie en informatie in een bedrijfsproces. Rapportages over responstijden en beschikbaarheid zijn hier voorbeelden van.

Monitoring
Een laatste aspect van interne beheersing is het opzetten en instandhouden van een adequaat 'monitoringsysteem'. De interne beheersingsprocedures moeten niet alleen goed werken nadat ze net zijn ontwikkeld, maar ook nog na langere tijd. De organisatie dient regelmatig de naleving en werking van bestaande richtlijnen en procedures te controleren. Indien dit niet gebeurt verliest het interne beheersingssysteem de beoogde waarde.

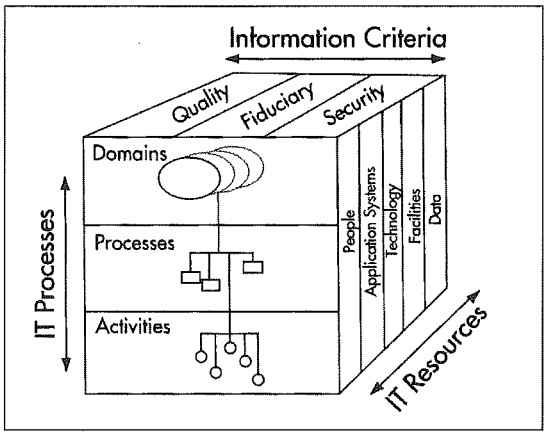
Vanuit onder andere het beheersingsmodel van het COSO-rapport is CobiT ontwikkeld. In de volgende paragraaf worden de uitgangspunten van het CobiT-rapport nader toegelicht. Tevens zal een link worden gelegd tussen de componenten volgens het COSO-rapport en het CobiT-rapport.

HET COBIT-RAPPORT

De doelstelling van het CobiT-rapport is het onderzoeken, ontwikkelen, publiceren en promoten van een gezaghebbende, up-to-date verzameling van algemeen geaccepteerde doelstellingen voor IT-beheersing, welke door managers en auditors kunnen worden gebruikt ([ISAC96]).

Het totale CobiT-rapport bestaat uit vier onderdelen:
1. Executive summary;
2. Framework;
3. Control objectives;
4. Audit guidelines.

Hierna worden het framework, de control objectives en de audit guidelines nader toegelicht.



Figuur 3. 'CobiT-kubus' ([ISAC96]).

Framework

Het CobiT-framework kan worden weergegeven in een kubus (zie figuur 3) die bestaat uit drie verschillende gezichtspunten: de IT Processes (domeinen, processen en activiteiten), de Information Criteria en de IT Resources.

IT Processes
Het CobiT-framework gaat ervan uit dat de IT Resources worden beheerd aan de hand van een geheel van samenhorende en logisch gegroepeerde processen en activiteiten binnen de processen. Domeinen groeperen vervolgens bij elkaar behorende processen op het hoogste niveau binnen het CobiT-framework. De groepering in domeinen sluit in het algemeen aan bij gebieden van verantwoordelijkheid die eenduidig zijn onderkend in een organisatorische structuur. Per domein is een aantal IT-processen gedefinieerd. In totaal zijn voor de vier domeinen 32 IT-processen onderkend. De vier domeinen zijn:

1. Planning & Organisation
Dit domein omvat de strategische en tactische aspecten van IT-beheersing en de identificatie van de beste manier waarop IT kan bijdragen om de doelstellingen van de organisatie te bereiken. Daarnaast moet de realisatie van de strategische visie worden gepland, gecommuniceerd en gestuurd. Ten slotte dient een juiste organisatie en technische infrastructuur te worden geïmplementeerd.

2. Acquisition & Implementation
Om de IT-strategie te realiseren moeten IT-oplossingen worden geïdentificeerd, ontwikkeld of aangeschaft, geïmplementeerd en geïntegreerd in de bedrijfsprocessen. Ook wijzigingen en onderhoud van bestaande systemen vallen binnen dit domein.

3. Delivery & Support
Dit domein is het meest uitgewerkt in CobiT en omvat de feitelijke levering en ondersteuning van de gewenste IT-diensten. Binnen deze diensten bevinden zich de traditionele beveiligings- en continuïteitselementen, maar bijvoorbeeld ook training. Tevens is onder dit domein de verwerking van gegevens opgenomen, inclusief de application controls.

4. Monitoring
Alle IT-processen dienen periodiek te worden beoordeeld op kwaliteit. Hierbij moet worden vastge-

Tabel 1.
CobiT-domeinen en COSO-componenten.

CobiT-domeinen: Specifiek IT-proces	COSO-componenten: Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
Planning & Organisation	■				
PO1: Define strategic plan		■			
PO2: Define information architecture				■	
PO3: Define technological direction				■	
PO5: Manage the investment			■		
PO6: Communicate management aims & direction				■	
PO9: Assess risk		■			
PO11: Manage quality			■		
Acquisition & Implementation	■		■		
Delivery & Support	■		■		
DS11: Manage data				■	
Monitoring					■

steld of de IT-processen nog voldoen aan de vereiste beheersingsdoelstellingen.

In tabel 1 worden de domeinen van CobiT afgezet tegen de componenten volgens het COSO-rapport. Enkele IT-processen zijn expliciet genoemd omdat in die gevallen het IT-proces direct met een COSO-component kan worden vergeleken.

De aspecten die in het COSO-rapport vallen onder de control environment, zijn in het CobiT-rapport in feite van toepassing op bijna alle gedefinieerde IT-processen. Uit tabel 1 blijkt dat de domeinen volgens het CobiT-rapport passen binnen de componenten volgens het COSO-rapport die de managementcyclus weergeven. Het verschil is dat CobiT specifiek gericht is op de beheersingsmaatregelen inzake IT ter ondersteuning van de ondernemingsdoelstellingen.

Information Criteria
Om ondernemingsdoelstellingen te kunnen bereiken moet informatie voldoen aan een reeks van zeven elkaar gedeeltelijk overlappende criteria: effectiviteit, efficiency, vertrouwelijkheid, integriteit, beschikbaarheid, compliance en betrouwbaarheid[1]. Dit is een uitsplitsing van drie categorieën (quality, fiduciary en security) in de 'CobiT-kubus'. De informatiecriteria effectiviteit, efficiency, compliance en betrouwbaarheid stemmen overeen met de genoemde doelstellingen in het COSO-rapport. De aspecten vertrouwelijkheid, integriteit en beschikbaarheid zijn beveiligingsaspecten.

Niet alle beheersingsmaatregelen zullen in dezelfde mate ertoe bijdragen dat de geproduceerde informatie voldoet aan de informatiecriteria. Bij de classificatie van IT-processen (zie figuur 4) is dan ook een onderscheid gemaakt tussen:
- primary impact;
- secondary impact;
- geen impact.

IT Resources
Informatie wordt opgevat als een resultante van de inzet van IT Resources, en wel in hun meest ruime betekenis: mensen, applicatiesystemen (geautomatiseerde en handmatige procedures), informatie- en communicatietechnologie (technologie en faciliteiten) en gegevens.

In figuur 4 worden de IT-processen per domein weergegeven. Dit overzicht geeft in feite het CobiT-framework weer. Voor elk IT-proces is aangegeven of (primair, secundair of geen) de desbetreffende beheersingsmaatregelen ertoe bijdragen dat de geproduceerde informatie aan de diverse informatiecriteria voldoet. Tevens is aangegeven welke IT Resources expliciet betrokken zijn bij een IT-proces.

Control objectives

In het CobiT-framework is voor elk IT-proces volgens een vaste structuur een beheersingsdoelstelling op een hoog niveau gedefinieerd. Voor het IT-proces 'Managing Data' is dit bijvoorbeeld:
'Control over the IT process of managing data
that satisfies the business requirement to ensure that data remains complete, accurate and valid during its input, update and storage
is enabled by an effective combination of application and general controls over the IT operations
and takes into consideration
- media identification, movement and library management
- form design
- source document retention
- data storage and backup management
- input controls
- processing controls
- output controls
- interface controls.'

Vervolgens worden in het onderdeel 'Control objectives' van het CobiT-rapport per IT-proces gedetailleerde beheersingsdoelstellingen weergegeven. Voor elk van de 32 IT-processen zijn variërend 5 tot 25 gedetailleerde beheersingsdoelstellingen gedefinieerd. In totaal zijn 280 beheersingsdoelstellingen geformuleerd die op elke willekeurige organisatie

1. Het begrip betrouwbaarheid in CobiT sluit aan met dat in COSO en heeft betrekking op de toereikende informatievoorziening gezien de uit te voeren taken en verantwoordelijkheden. Integriteit is een beveiligingsaspect en heeft volgens CobiT betrekking op de juistheid en volledigheid van informatie.

SUMMARY TABLE

DOMAIN		PROCESS	Information Criteria: effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	IT Resources: people	applications	technology	facilities	data
Planning & Organisation	PO1	Define a strategic plan	P	S						✔	✔	✔	✔	✔
	PO2	Define the information architecture	P	S	S	S					✔			✔
	PO3	Determine technological direction	P	S								✔	✔	
	PO4	Define organisation and relationships	P	S						✔				
	PO5	Manage the investment	P	P					S	✔	✔	✔	✔	
	PO6	Communicate management aims & direction	P					S		✔				
	PO7	Manage human resources	P	P						✔				
	PO8	Ensure compliance with external requirements	P					P	S	✔	✔			✔
	PO9	Assess risk	S	S	P	P	P	S	S	✔	✔	✔	✔	✔
	PO10	Manage projects	P	P						✔	✔	✔	✔	
	PO11	Manage quality	P	P		P			S	✔	✔			
Acquisition & Implementation	AI1	Identify automated solutions	P	S							✔	✔	✔	
	AI2	Acquire & maintain application software	P	P		S		S	S		✔			
	AI3	Acquire & maintain technology infrastructure	P	P		S						✔		
	AI4	Develop & maintain procedures	P	P		S		S	S	✔	✔	✔	✔	
	AI5	Install & accredit systems	P			S	S			✔	✔	✔	✔	✔
	AI6	Manage changes	P	P		P	P		S	✔	✔	✔	✔	✔
Delivery & Support	DS1	Define service levels	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS2	Manage third-party services	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS3	Manage performance & capacity	P	P			S				✔	✔	✔	
	DS4	Ensure continuous service	P	S			P			✔	✔	✔	✔	✔
	DS5	Ensure systems security			P	P	S	S	S	✔	✔	✔	✔	✔
	DS6	Identify & attribute costs		P					P	✔	✔	✔	✔	✔
	DS7	Educate & train users	P	S						✔				
	DS8	Assist & advise customers	P							✔	✔			
	DS9	Manage the configuration	P				S		S		✔	✔	✔	
	DS10	Manage problems & incidents	P	P			S			✔	✔	✔	✔	✔
	DS11	Manage data				P			P					✔
	DS12	Manage facilities				P	P						✔	
	DS13	Manage operations	P	P		S	S			✔	✔		✔	✔
Monitoring	M1	Monitor the process	P	S	S	S	S	S	S	✔	✔	✔	✔	✔
	M2	Obtain independent assurance	P	P	S	S	S	S	S	✔	✔	✔	✔	✔

Figuur 4. Summary table ([ISAC96]). Overzicht information criteria versus processen en IT resources.

kunnen worden toegepast. Beheersingsdoelstellingen worden overigens gedefinieerd als 'a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity' ([ISAC96]). De definitie van beheersingsdoelstellingen in het CobiT-rapport sluit aan met het COSO-rapport.

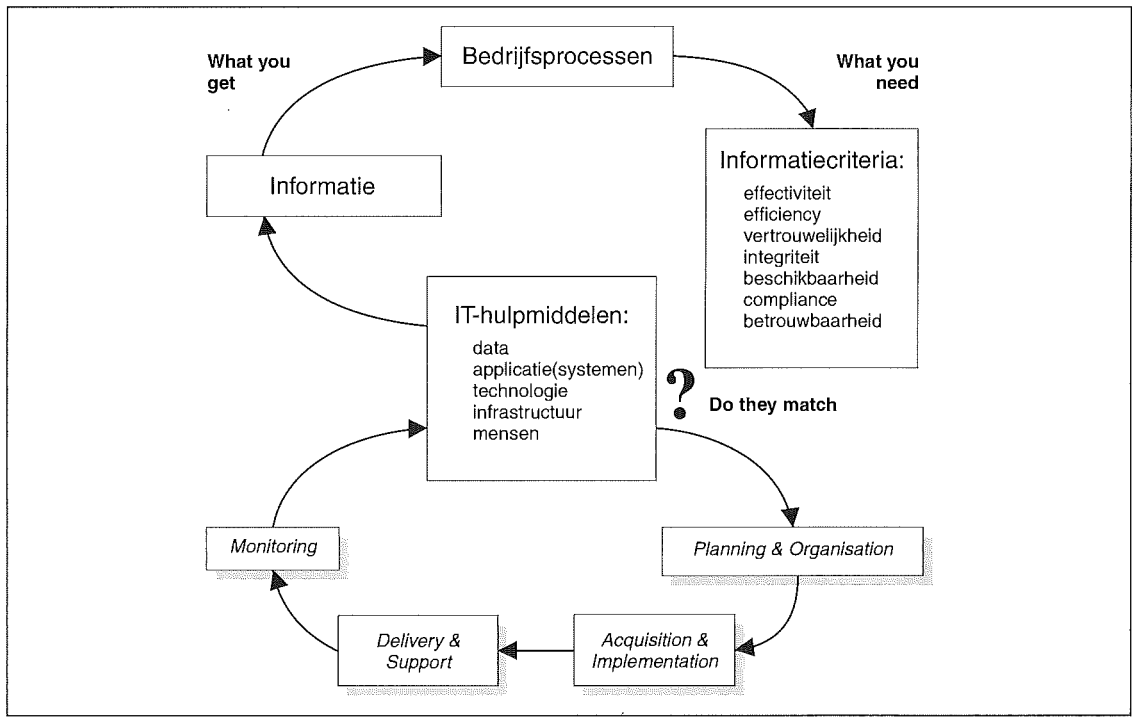
De selectie van beheersingsmaatregelen (ofwel beheersingsactiviteiten) zou volgens CobiT afhankelijk moeten zijn van de beheersingsdoelstellingen waaraan moet worden voldaan. De beheersingsdoelstellingen moeten gericht zijn op de risico's die samenhangen met het realiseren van ondernemingsdoelstellingen. De beheersingsdoelstellingen in het CobiT-rapport zijn toepasbaar voor alle activiteiten binnen de geautomatiseerde informatiesystemen. De onderliggende gedachte van CobiT hierbij is dat de beheersing van IT wordt bereikt door gebruik te maken van de informatie die benodigd is om de bedrijfsprocessen te ondersteunen. Tevens wordt gekeken naar de informatie die daadwerkelijk door de IT Resources wordt gegenereerd. De bedrijfsprocessen zijn gericht op het realiseren van ondernemingsdoelstellingen. In figuur 5 wordt het CobiT-concept weergegeven.

CobiT kan worden gebruikt als leidraad voor de beoordeling van de general IT controls en in beperkte mate voor de application controls. In de praktijk zal het niet zo zijn dat alle IT-processen en alle beheersingsdoelstellingen bij een jaarrekeningcontrole aan de orde komen. Dit is ten behoeve van het beoordelen van de getrouwheid van de jaarrekening niet noodzakelijk en zal budgettair ook niet mogelijk zijn. Het CobiT-rapport voorziet door middel van een standaard audit approach in de behoefte een auditplan op te stellen. Op welke wijze CobiT ingepast kan worden, wordt in de volgende paragraaf nader uitgewerkt.

Audit Guidelines

De audit guidelines stellen de accountant/IT-auditor in staat specifieke IT-processen te beoordelen met behulp van de door CobiT aanbevolen beheersingsmaatregelen. Hiermee kan een oordeel worden verkregen over de effectiviteit van beheersingsmaat-

Figuur 5. CobiT-concept ([ISAC96]).



regelen gericht op IT of kan het management worden geadviseerd waar IT-processen kunnen worden verbeterd. Daarnaast kunnen proceseigenaren zichzelf de vraag stellen: 'Is datgene wat ik doe goed?' 'En zo niet, hoe kan ik het verbeteren?' Het CobiT-framework, de control objectives en de audit guidelines kunnen deze vragen helpen beantwoorden.

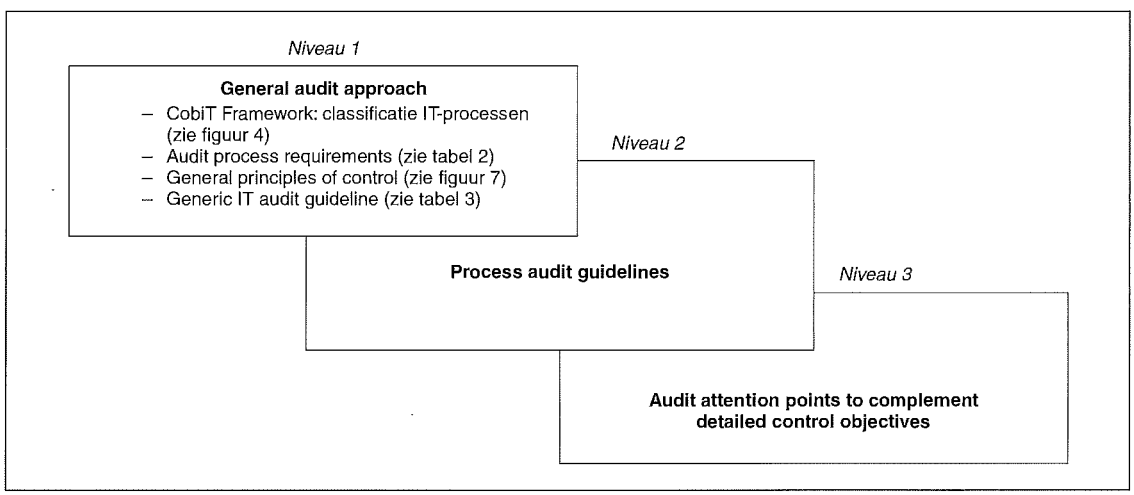
De audit guidelines dienen in feite als een leidraad bij het opstellen van één of meer auditplannen. De guidelines zijn echter niet bedoeld als een kant-en-klaar pakket voor het creëren voor een overall auditplan. Er dient immers ook rekening te worden gehouden met bijvoorbeeld geconstateerde tekortkomingen in het verleden, specifieke risico's van de organisatie, bekende incidenten, nieuwe ontwikkelingen en strategische keuzen. Het doel van de audit guidelines in het CobiT-rapport is te voorzien in een op algemeen geaccepteerde audit practices gebaseerde structuur voor het beoordelen van beheersingsmaatregelen. Doordat individuele auditdoelstellingen en -gebruiken per organisatie verschillen zijn de audit guidelines algemeen en op een hoog niveau gedefinieerd.

De doelstellingen van een onderzoek volgens CobiT (terug te vinden in de structuur van de audit guidelines) zijn:
- het verstrekken van een redelijke mate van zekerheid dat beheersingsdoelstellingen zijn bereikt;
- het onderbouwen van het risico indien significante leemten in de beheersing zijn geconstateerd;
- het management adviseren inzake richtlijnen voor te treffen maatregelen.

Het raamwerk voor het uitvoeren van een audit volgens het CobiT-rapport bestaat uit de in figuur 6 weergegeven drie niveaus.

In dit artikel wordt de standaardstructuur voor de uitvoering van niveau 1 nader toegelicht. Wanneer

Figuur 6. Gefaseerde benadering audit framework CobiT ([ISAC96]).



Fase 1: 'Determine the correct scope of our audit' De eerste fase in het uit te voeren onderzoek is de juiste scope voor de audit te bepalen. Hiertoe dient het volgende te worden geïnventariseerd en geanalyseerd: – de van toepassing zijnde bedrijfsprocessen; – de platformen en informatiesystemen die de bedrijfsprocessen ondersteunen en de relaties die tussen de platformen en informatiesystemen bestaan. De platformen betreffen hardware, het netwerk en besturingsprogrammatuur; – de gedefinieerde taken en functies met betrekking tot IT en de bijbehorende verantwoordelijkheden, inclusief datgene wat is in- of outsourced; – de hiermee samenhangende business risks.
Fase 2: 'Identify the information requirements' Betreft het inventariseren van informatiebehoeften die relevant zijn voor de onderkende bedrijfsprocessen. De bedrijfsprocessen zijn gericht op het bereiken van de ondernemingsdoelstellingen.
Fase 3: 'Identify the inherent IT risks as well as overall level of control' In samenhang met de onderkende bedrijfsprocessen dient het inherente IT-risico en het algehele niveau van beheersing te worden geïdentificeerd. Hiertoe wordt het volgende in kaart gebracht: – recente veranderingen in de organisatieomgeving die een IT-impact hebben; – recente veranderingen in de IT-omgeving; – recente incidenten die van belang zijn voor beheersingsmaatregelen en de bedrijfsomgeving; – de maatregelen om de IT te monitoren, welke worden toegepast door het management; – recente auditrapporten; – recente resultaten van door de organisatie zelf uitgevoerde analyses ('self assessments').
Fase 4: 'Select the relevant CobiT-Processes as well as the resources which apply to them' Op basis van de verkregen informatie kunnen de relevante IT-processen en de IT-resources die daarmee samenhangen worden geselecteerd. Dit zou kunnen betekenen dat bepaalde IT-processen meerdere keren moeten worden onderzocht, elke keer ten aanzien van een ander platform of informatiesysteem. In deze fase dient ook de auditstrategie te worden bepaald op basis waarvan een gedetailleerd auditplan verder zou moeten worden uitgebreid. Het beoordelen van de IT-processen vindt plaats volgens de algemene IT audit guideline (zie hiervoor de fasen 5A tot en met 5D volgens tabel 3).

Tabel 2.
In kaart brengen van de audit process requirements volgens CobiT ([ISAC96]).

bepaald is waar het onderzoek van de IT zich op zal moeten richten, dient de juiste benadering of strategie voor het uitvoeren van de auditwerkzaamheden te worden bepaald. In tabel 2 worden de fasen weergegeven waarmee volgens CobiT de audit process requirements in kaart worden gebracht.

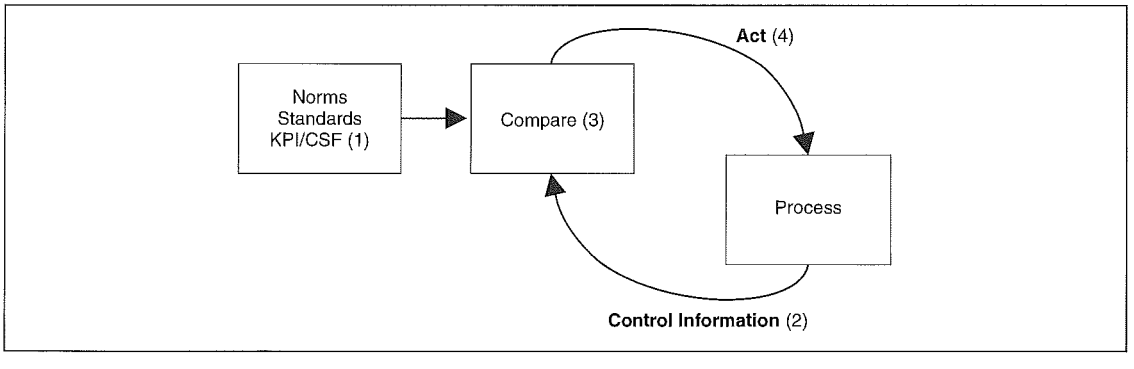
Algemene principes omtrent beheersing kunnen volgens CobiT extra inzicht geven in de wijze waarop de audit guidelines verder gecomplementeerd kunnen worden. Beheersing is vanuit managementoogpunt gedefinieerd als het actief sturen op doelstellingen. Dit betekent dat de performance moet worden geëvalueerd en indien nodig corrigerende maatregelen moeten worden getroffen, zodat de doelstellingen worden bereikt. Het beheersingsproces is weergegeven in figuur 7 en bestaat uit vier stappen:

1. voor een proces dient een norm of gewenste performance (Key Performance Indicators/Critical Success Factors) te worden gedefinieerd;
2. het proces genereert 'control'-informatie, die inzicht geeft in de gebeurtenissen in een proces;
3. de 'control'-informatie wordt vergeleken met een norm of standaard;
4. als de werkelijkheid niet voldoet aan de norm of standaard worden corrigerende maatregelen genomen.

Hierna wordt nader ingegaan op de standaardstructuur van de IT audit guideline; het vierde onderdeel van niveau 1 van de general audit approach (zie figuur 6). Tevens komt aan de orde de werkverdeling tussen accountant en IT-auditor bij de beoordeling van de IT in het kader van de jaarrekeningcontrole.

Gebruik van CobiT in de controlepraktijk

De standaardstructuur voor het in kaart brengen van de audit process requirements (zie tabel 2) ver-



Figuur 7.
Control process ([ISAC96]).

toont overeenkomst met de aanpak die de accountant bij de jaarrekeningcontrole hanteert. De fasen 1 tot en met 3 waarin de audit process requirements worden bepaald, kunnen door een algemeen opgeleid accountant zelf worden uitgevoerd. Fase 3 kan nieuwe elementen in zich hebben, maar er hoeft geen beletsel te zijn die uit te voeren. Bij fase 4 kan een deskundigheidsvraagstuk ontstaan. De accountant zal eventueel bijgestaan door een auditor met IT-deskundigheid (IT-auditor) bepalen welke IT-processen en systemen beoordeeld moeten worden. De beoordeling van de IT-processen zal de IT-auditor uitvoeren. De algemeen opgeleid accountant beschikt hiervoor niet over de benodigde kennis en ervaring. De standaardstructuur waarmee in de audit guidelines de IT-processen kunnen worden beoordeeld, vertoont eveneens overeenkomst met de werkwijze van de accountant. In tabel 3 is de standaard IT audit guideline volgens CobiT weergegeven. De IT-auditor zal overigens voor de werkzaamheden in fase 5A gebruikmaken van de kennis die de accountant hieromtrent al heeft.

De bruikbaarheid van CobiT in het kader van de jaarrekeningcontrole wordt bevorderd doordat de werkwijze waarmee de IT-auditor de IT-processen beoordeelt, overeenkomst vertoont met de werkwijze van de accountant bij het beoordelen van de routinematige bedrijfsprocessen. Door de gefaseerde aanpak (drie niveaus) en de standaardstructuur voor de auditwerkzaamheden wordt de communicatie omtrent de aanpak en de gerapporteerde bevindingen bevorderd. Samengevat zijn de aspecten die pleiten voor het gebruik van de CobiT-methode:

– De uitgangspunten van CobiT sluiten aan op COSO en daarmee bij de ontwikkelingen inzake corporate governance. Deze ontwikkelingen hebben belangrijke invloed op de werkzaamheden van de accountant.

– De structuur van de audit approach, waaronder het bepalen van de audit process requirements en de standaard IT audit guidelines, sluit min of meer aan bij de werkwijze waarmee de accountant de beheersing van routinematige bedrijfsprocessen beoordeelt.

– Het beschikbaar zijn van vaste werkprotocollen is een teken van professionaliteit en heeft tot gevolg dat twee auditors onafhankelijk van elkaar tot hetzelfde oordeel kunnen komen.

– De verantwoordelijk accountant heeft de mogelijkheid een selectie van IT-processen te maken die nader worden onderzocht. De accountant zal hierbij wellicht de deskundigheid van de IT-auditor inschakelen.

– Door het gebruik van standaard-IT-processen worden duidelijkheid en structuur voor de organisatie en de auditor gecreëerd. De communicatie en het wederzijds begrip tussen accountant, management en IT-auditor worden hiermee bevorderd.

– Het CobiT-rapport is geen statisch geheel, maar zal periodiek worden geoptimaliseerd en uitgebreid. Om de gebruiksvriendelijkheid van CobiT in de toekomst nog meer te vergroten, is aangekondigd dat het huidige CobiT-rapport (fase 1) wordt uitgebreid met self assessment guidelines (fase 2) en performance-indicatoren (fase 3).

KANTTEKENINGEN BIJ COBIT

De volgende kanttekeningen kunnen bij het gebruik van CobiT worden geplaatst:

Tabel 3.
De standaardstructuur van de IT audit guideline volgens CobiT ([ISAC96)].

Fase 5A: 'Obtaining and understanding' Door middel van interviews en het bestuderen van documentatie dient inzicht te worden verkregen in de activiteiten die ten grondslag liggen aan de beheersingsdoelstellingen. Daarnaast dienen de bestaande beheersingsmaatregelen te worden geïnventariseerd. Inzicht dient te worden verkregen in: – 'business requirements' en daarmee samenhangende risico's; – organisatiestructuur; – rollen en verantwoordelijkheden; – beleid en procedures; – wet- en regelgeving; – bestaande beheersingsmaatregelen; – managementrapportages (status, performance, actiepunten).
Fase 5B: 'Evaluating the appropriateness of stated controls' De toereikendheid van de beheersingsmaatregelen voor het onderzochte IT-proces wordt geëvalueerd met behulp van de onderkende criteria, normen in de branche en het professional judgement van de auditor. Hierbij beoordeelt de auditor onder andere of de gedocumenteerde processen bestaan, de resultaten ('deliverables') toereikend zijn en de toebedeelde verantwoordelijkheden duidelijk en effectief zijn. Daarnaast dienen eventuele compenserende beheersingsmaatregelen te bestaan.
Stap 5C: 'Assessing compliance' Voor de onderzochte periode dient te worden vastgesteld dat de beheersingsmaatregelen consistent en continu hebben gewerkt zoals beschreven. De auditor bepaalt de hoeveelheid controlewerkzaamheden die nodig is om 'assurance' te kunnen geven dat de beheersing van het IT-proces toereikend is.
Fase 5D: 'Substantiating the risk' Het risico dat de beheersingsdoelstellingen niet worden bereikt, dient te worden onderbouwd door middel van het gebruik van analytische technieken of van alternatieve bronnen. De leemten in de beheersing en bedreigingen en zwakheden als gevolg hiervan dienen te worden gedocumenteerd. Vervolgens moeten de werkelijke en de potentiële impact worden vastgelegd.

– De audit guidelines zijn erg breed, waardoor het risico bestaat dat deze als een allesomvattende checklist worden gehanteerd. In het CobiT-rapport wordt overigens wel duidelijk aangegeven dat de auditor de audit guidelines in het CobiT-rapport indien noodzakelijk dient uit te breiden.

– Het risico bestaat dat een niet-deskundige het CobiT-rapport en dan met name de audit guidelines gebruikt om zelf de beheersing van een IT-proces te beoordelen. De audit guidelines zijn erg breed, maar zijn niet toereikend voor specifieke situaties. Alleen een auditor met IT-deskundigheid kan bepalen welke specifieke beheersingsmaatregelen noodzakelijk zijn en wat de impacts van de controlebevindingen zijn.

– In de audit guidelines wordt geen onderscheid gemaakt tussen general en application controls. Dit behoeft geen probleem te zijn. Echter, bij het beoordelen van de beheersingsmaatregelen dient wel onderkend te worden wat een general of application control is. De general controls ondersteunen immers de blijvende werking van de application controls. Overigens wordt voor wat betreft de application controls alleen een eerste aanzet gegeven. Een beoordelingsmethode van de application controls maakt geen onderdeel uit van CobiT.

BEVEILIGINGSNORMEN

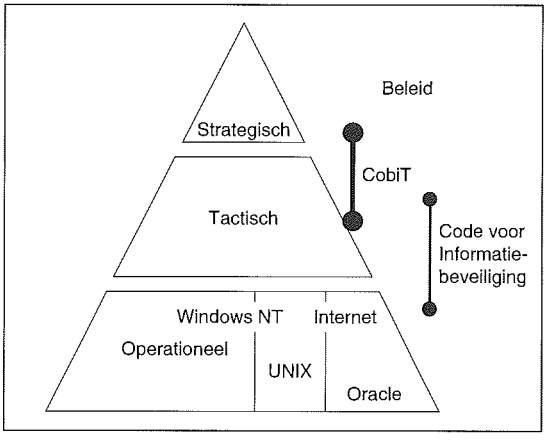
Informatiebeveiliging is een specifiek beheersingsaspect. Met betrekking tot informatiebeveiliging zijn vele normenkaders beschikbaar. In CobiT zijn onder andere normen opgenomen voor beveiliging. In figuur 8 wordt de positie van CobiT weergegeven ten opzichte van andere modellen gericht op informatiebeveiliging. Hieruit blijkt welke niveaus de beheersingsmaatregelen in CobiT betreffen.

In het kader van dit artikel wordt niet verder op het beheersingsaspect informatiebeveiliging ingegaan.

EVALUATIE

De ontwikkeling van het CobiT-rapport hangt samen met de ontwikkeling van nieuwe modellen voor de beheersing van organisaties, zoals COSO. Nieuwe modellen voor de beheersing van organisaties worden mede ontwikkeld als gevolg van de (weer actuele) aandacht voor corporate governance. De accountant wordt hiermee geconfronteerd bij de uitoefening van zijn/haar werkzaamheden. In het COSO-rapport wordt de definitie internal control breder geïnterpreteerd dan voorheen gebruikelijk. Internal control behelst het gehele interne beheersingssysteem, waaronder de beheersing van de IT.

Vele modellen zijn inmiddels ontwikkeld om de beheersing van de IT gestalte te geven en te beoordelen. Wat maakt CobiT nu anders? CobiT slaat in feite een brug tussen de (nieuwe) beheersingsmodellen voor organisaties en de huidige beheersingsmodellen voor IT. CobiT is een niet-technisch, internationaal bekend



Figuur 8.
De plaats van CobiT binnen IT-beveiliging (in de breedste zin).

referentiekader voor IT-gebonden beheersingsmaatregelen, waarin beheersingsdoelstellingen zijn gedefinieerd voor standaard-IT-processen, zodanig dat de kwaliteit van de geproduceerde informatie voldoet aan de door de bedrijfsprocessen gestelde criteria.

De audit guidelines in het CobiT-rapport stellen de IT-auditor in staat specifieke standaard-IT-processen te beoordelen met behulp van de door CobiT aanbevolen beheersingsmaatregelen. De audit guidelines dienen in feite als een leidraad bij het opstellen van één of meer auditplannen. De guidelines zijn overigens niet bedoeld als een kant-en-klaar pakket voor het creëren voor een overall auditplan. Er dient immers ook rekening te worden gehouden met bijvoorbeeld de geconstateerde tekortkomingen in het verleden, specifieke risico's van de organisatie, bekende incidenten, nieuwe ontwikkelingen en strategische keuzen.

De standaardstructuur in CobiT biedt een duidelijke werkverdeling tussen accountant en IT-auditor.

Bij het beoordelen van de beheersing van de IT in het kader van een moderne controleaanpak ten behoeve van de jaarrekeningcontrole is de deskundigheid van de algemeen opgeleid accountant niet geheel toereikend en zal een auditor met IT-deskundigheid (IT-auditor) worden ingeschakeld. De standaardstructuur in het CobiT-rapport voor het beoordelen van de IT biedt de mogelijkheid om een duidelijke werkverdeling tussen accountant en IT-auditor te realiseren. De accountant brengt met behulp van een standaardstructuur de audit process requirements in kaart. De IT-auditor kan vervolgens via vaste werkprotocollen (standaard IT audit guidelines) de door de accountant geselecteerde IT-processen beoordelen. Deze IT-processen kunnen meerdere informatiesystemen betreffen. Doordat de werkwijze van de IT-auditor overeenkomst vertoont met de wijze waarop de accountant de routinematige bedrijfsprocessen beoordeelt, worden een goede communicatie en wederzijds begrip bevorderd.

Bij het gebruik van het CobiT-rapport moet wel worden bedacht dat de audit guidelines erg breed zijn, waardoor het risico bestaat dat deze als een alles-

Mw. drs. A.J.M. Koopman
Is als senior auditor werkzaam bij Audit Fortis Nederland. Dit artikel is deels gebaseerd op de door de auteur geschreven scriptie getiteld: 'Accountantscontrole in een paperless office', in het kader van de postdoctorale accountantsopleiding. In maart 1998 heeft zij deze opleiding aan de Vrije Universiteit te Amsterdam afgerond.

omvattende checklist worden gehanteerd. De audit guidelines dienen 'op maat' te worden gemaakt voor specifieke situaties in een organisatie. Ook moet ervoor worden gewaakt dat het CobiT-rapport door niet-deskundigen wordt gebruikt om de beheersing van IT te beoordelen. De hulp van een IT-deskundige is noodzakelijk om te beoordelen op welke wijze de audit guidelines dienen te worden gecomplementeerd en hoe verstrekkend de gevolgen zijn. Een ander belangrijk aspect is dat het CobiT-rapport met name gericht is op de general IT controls. Voor de application controls wordt alleen een eerste aanzet gegeven. De wijze waarop de specifieke application controls worden beoordeeld, moet door de accountant zelf worden bepaald.

Resumerend kan worden gesteld dat het CobiT-rapport als referentiekader de accountant en de IT-auditor behulpzaam kan zijn bij het beantwoorden van de vraag: 'Aan welke eisen moet worden voldaan, om te kunnen zeggen dat de IT 'in control' is?'

LITERATUUR

[Boer95] H. den Boer en L.C. van Zutphen, *Business control en auditing; recente ontwikkelingen in internationaal verband*, Academic Service, 1995.

[Colb96] J.L. Colbert en P. Bowen, *A comparison of Internal Control: CobiT, SAC, COSO and SAS*, IS Audit & Control Journal, Volume IV, 1996.

[COSO94] Committee Of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework*, Edition in Two Volumes, Author Coopers & Lybrand US, AICPA, New York, July 1994.

[ISAC95] ISACF (Information Systems Audit and Control Foundation), *CobiT: Control Objectives for Information and related Technology*, IS Audit & Control Journal, Volume IV, p. 12 en 13, 1995.

[ISAC96] ISACF, *CobiT: Control Objectives For Information and Related Technology*, released by the CobiT steering committee, the Information Systeems Audit and Control Foundation Research Board and the Information Systems Audit and Control Foundation Standards Board, 1996.

[Jose96] G.W. Joseph en T.J. Engle, *Controlling EDI environments consistent with CobiT and COSO*, IS Audit & Control, Volume IV, 1996.

[Koop98] A.J.M. Koopman, *Accountantscontrole in een paperless office*, Scriptie postdoctorale accountantsopleiding Vrije Universiteit te Amsterdam, 19 februari 1998.

[Kord97] L.J.J. Kordel, *CobiT, een referentiemodel voor de controle van IT*, Informatie, november 1997.

[Lain96] J.W. Lainhart, *Arrival of CobiT Helps Refine the Valuable Role of IS Audit and Control in the Enterprise*, IS Audit & Control Journal, Volume IV, p. 20 t/m 23, 1996.

[Nivr96] NIVRA Studierapport, *Interne beheersing en accountant*; literatuurstudie en synthese, september 1996.

[Paap97] L. Paape en D. Maas, *In Control*, Spotlight nr. 3 1997, p. 25 t/m 31, Coopers & Lybrand.

KPMG EDP Auditors
ten Hagen & Stam Uitgevers