# COMPACT WINTER

EDP-AUDITING EN ACCOUNTANTSCONTROLE

1993/4

KWARTAALBLAD EDP-AUDITING

*Compact ®*
*Jaargang 20, nummer 4*
*Een uitgave van KPMG Klynveld EDP Auditors en Samsom BedrijfsInformatie, werkmaatschappij van Wolters Kluwer NV.*
*Het blad verschijnt 4 x per jaar.*

*Redactie*
*D. Steeman RE RA*
*(hoofdredacteur)*
*drs. R.G.A. Fijneman RE RA*
*prof. A.W. Neisingh RE RA*
*drs. P. Veltman RE RA*

*Redactiesecretariaat*
*Mw. A.M.F. Hofland,*
*KPMG Klynveld EDP Auditors,*
*K.P. van der Mandelelaan 41,*
*3062 MB Rotterdam*
*Tel.: 010 - 453 47 40*
*Fax : 010 - 453 47 77*

*Vormgeving*
*Bureau Karakter, Delft*

*Aan dit nummer werkten mee*
*drs. J.J. van Beek RE RA*
*J.C. Boer RE RA*
*drs. L.H. Dam RA*
*mw.mr.drs. A.W. Duthler*
*drs. R.G.A. Fijneman RE RA*
*drs. R. Oudega*
*drs. G.J.W.C. Vankan*
*drs. P. Veltman RE RA*

*Abonnementen*
*f 135,- per jaar incl. BTW. Losse nummers f 45,- 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.: 01720 - 6 68 00*
*Fax: 01720 - 7 59 33*
*Adreswijzigingen - ook tijdelijke - moeten minstens 8 weken voor de verschijningsdatum bekend zijn.*



*Uitgever*
*J.R.M. Masselink*

*Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU*

*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 èn advies, zoals: • beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacy-wetgeving • computercriminaliteit en nieuwe regelgeving.*

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



*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 het secretariaat verkrijgbaar is.*

Het winternummer van Compact dat u nu heeft opgeslagen, markeert een periode.

De trouwe lezer weet dat dit blad als een intern blad over automatisering en controle in 1973 werd gestart: Computer en accountant; Compact. In 1986 werd ter gelegenheid van het twaalfeneenhalf-jarig bestaan het boek *24 over EDP-auditing* gepubliceerd. Dit jaar maakt Compact zijn twintigste jaargang vol.

Samenhangend met de oprichting van de beroepsvereniging NOREA en de uitgave van het blad de EDP-Auditor, heeft de redactie zich beraden over de positie en de functie van Compact. Een in februari van dit jaar gehouden lezersonderzoek heeft een zeer positief beeld opgeleverd omtrent de betrokkenheid van de lezers bij het blad en de appreciatie ervan.

Mede naar aanleiding van het lezersonderzoek en ter markering van het twintigjarig bestaan, staat in dit nummer het thema 'accountant en automatisering' centraal. Terug naar de oorsprong dus: wat betekent de automatisering voor de accountantscontrole.

Dit onderwerp is van belang, omdat veel EDP-auditors in hun werk regelmatig met accountants in aanraking komen en in veel gevallen ook deel uitmaken van een interne accountantsafdeling of een externe accountantspraktijk.

De brede opvatting over het vakgebied van EDP-auditing mag er niet toe leiden dat vraagstukken van betrouwbaarheid, vertrouwelijkheid en continuïteit in relatie tot accountantscontrole naar de achtergrond verdwijnen; uiteindelijk stonden deze aspecten aan de wieg van EDP-auditing.

In dit nummer worden deze vraagstukken opnieuw aan de orde gesteld. De leidraad in de artikelen is de noodzaak tot systeemgerichte controle. Absoluut geen nieuw onderwerp, maar de constatering is op zijn plaats dat in de systeemgerichte controle de automatiseringsaspecten nog steeds onderbelicht zijn, althans naar de mening van EDP-auditors.
De schrijvers van de eerste drie artikelen doen een poging om de materie opnieuw onder de aandacht te brengen. Wellicht leidt dit tot reacties der accountants.

Naast deze drie thematische artikelen wordt aandacht besteed aan nauw verwante onderwerpen. Dit zijn: operational auditing, computerverzekeringen, de samenwerking tussen accountant, EDP-auditor en jurist, en het altijd ook voor de accountant van belang zijnde onderwerp geautomatiseerde betalingen.

Al met al weer een goed gevuld nummer voor rond de kerstdagen, waarvan de redactie van Compact hoopt dat u ze in goede harmonie zult doorbrengen.

*D. Steeman RE RA*

# Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving

Drs. R.G.A. Fijneman RE RA

**IT wordt door certificerende accountants nog te defensief benaderd. Het ontlenen van concrete audit evidence aan het beoordelen van de general IT controls geschiedt nog fragmentarisch.**
**Vanuit een gestructureerde benadering van IT en de juiste inpassing hiervan in het controleprogramma kan IT een 'opportunity' zijn voor de accountant.**

## INLEIDING

De accountant richt zich in zijn certificerende functie op de financiële gegevens en in meerdere of mindere mate op het proces van verwerking van deze gegevens. Het primaire doel van de accountantscontrole is het vaststellen of de informatie in een jaarrekening een getrouw beeld geeft van de werkelijkheid, of deze informatie voor de gebruikers van de jaarrekening toereikend is en of zij is opgesteld conform wettelijke voorschriften. De accountant kan bij het inrichten van zijn controlewerkzaamheden in hoofdlijnen een tweetal verschillende benaderingen kiezen, namelijk gegevens- of systeemgericht. De verschillen in benadering worden als invalshoek gebruikt om te kunnen aangeven welke invloed de geautomatiseerde gegevensverwerking (IT) heeft of zou moeten hebben op de accountantscontrole. Dit artikel zal niet expliciet ingaan op motieven van praktische of theoretische aard, die ten grondslag kunnen liggen aan de keuze voor één van beide benaderingen.

Bij een gegevensgerichte controle richt de accountant zich rechtstreeks op het object van onderzoek, zijnde de financiële gegevens, dat moet worden gecertificeerd. De systeemgerichte benadering richt zich daarentegen op het proces van verwerking van het object van onderzoek. Daarbij staat de vraag centraal in welke mate de accountant bij het controleren van de betrouwbaarheid van de posten in de jaarrekening gebruik kan maken van de beheersingsstructuren in een organisatie en welke invloed dit heeft op de door hem te verrichten werkzaamheden. De systeemgerichte benadering zal in het artikel verder worden gevolgd. De vraag welke aandacht voor IT minimaal benodigd is bij een gegevensgerichte controle-aanpak wordt, hoe interessant ook, niet behandeld.

Het bij de systeemgerichte controlebenadering te beoordelen proces van verwerking verandert door de introductie van IT. Gegevensverwerkende processen zijn in overwegende mate geautomatiseerd. 'Application controls' worden in gegevensverwerkende processen opgenomen ter waarborging van de betrouwbaarheid van de uitkomsten. De goede werking van deze controls dient te worden onderzocht. Daarnaast wordt als het ware een meta-proces ter beheersing van het proces van de application controls geïntroduceerd, de 'general IT controls'. Deze veranderingen worden in dit artikel behandeld, waarbij met name zal worden ingegaan op de betekenis van de general IT controls voor de accountantscontrole en de te volgen controlestrategie. Uit de literatuur blijkt dat niet eenduidig over de invloed van IT op de accountantscontrole wordt gedacht, hetgeen de verder gaande discussie over deze materie alleen maar interessanter maakt. Overigens is het evident dat deze veelal vaktechnische discussies onder beroepsgenoten dienen te leiden tot helderheid naar de afnemers van het accountantsprodukt, zijnde het management van de organisatie en het maatschappelijk verkeer.

## MODERNE VISIE OP ADMINISTRATIEVE ORGANISATIE

De laatste jaren is de betekenis van administratieve organisatie en interne controle verruimd. In het verleden werden zij in de praktijk direct gelieerd aan de betrouwbaarheid van de gegevensverwerking en de verslaglegging. Uit recente publikaties omtrent administratieve organisatie en interne controle blijkt nadrukkelijker dat het beheersingsvraagstuk betrekking heeft op de algehele kwaliteit van de organisatie, de processen en de produkten. Het begrip management control doet hierbij zijn intrede. Om als management grip te hebben op en sturing te kunnen geven aan de algehele kwaliteit is interne controle noodzakelijk. Interne controle is door Starreveld al gedefinieerd als controle door of namens de leiding. In de brede kwaliteitsbetekenis wordt het begrip interne controle gedefinieerd als een proces, ingevuld door het management en de overige werknemers, gericht op het verkrijgen van redelijke zekerheid omtrent het bereiken van doelstellingen met betrekking tot:

- de effectiviteit en efficiëntie van de bedrijfsprocessen;
- de betrouwbaarheid van de financiële rapportage;
- de overeenstemming met relevante wet- en regelgeving.

*Management control zal veel centraler in het controleprogramma van de accountant komen te staan.*

Deze verruimde betekenis van interne controle heeft ook haar weerslag op de door de accountant te verrichten werkzaamheden in zijn fungeren ten behoeve van de leiding van de gecontroleerde huishouding. De interne controle om te komen tot betrouwbare financiële informatie vormt een integraal onderdeel van de gehele kwaliteitsbeheersing. Met andere woorden, de management control-benadering zal veel centraler in het controleprogramma van de accountant worden geplaatst. Dit geldt eveneens voor de situaties waarbij de accountant nadrukkelijk gebruik zal maken van de betrouwbaarheidswaarborgen in de IT. Voordat hierop verder zal worden ingegaan, dient allereerst de accountantscontrole als zodanig nader te worden belicht.

## ACCOUNTANTSCONTROLE

Zoals vermeld heeft de accountantscontrole tot doel vast te stellen of de informatie in een jaarrekening een getrouw beeld geeft van de werkelijkheid, of deze informatie voor de gebruikers van de jaarrekening toereikend is en of zij is opgesteld conform de wettelijke voorschriften. Om te kunnen vaststellen dat de informatie inderdaad een getrouw beeld geeft, stelt de accountant een onderzoek in naar de posten van de balans en de verlies- en winstrekening.

### Totstandkoming jaarrekening

Een jaarrekening komt via een aantal fases tot stand, namelijk de eerste vastlegging van transacties aan de grens tussen de organisatie en de buitenwereld, de verwerking van de primaire vastleggingen uitmondend in een saldibalans, de omwerking van de saldibalans naar jaarrekeningposten en de feitelijke totstandkoming van de jaarrekening inclusief toelichting. De eerste twee fases kenmerken zich veelal door routinematige verwerking van bulktransacties (het verwerken van inkoopbestellingen, het plaatsen van verkooporders). Echter, dit kan per organisatie natuurlijk variëren. Het is eveneens goed denkbaar dat in dit proces ook niet-routinematige transacties (bijvoorbeeld de verwerking van specifieke financieringsconstructies en sale and lease back-constructies van vaste activa) zich voordoen. Dit verschil in routinematige en niet-routinematige transacties heeft invloed op de risico-inschattingen van de accountant. De inherente risico's bij niet-routinematige transacties zullen vanuit audit-perspectief veelal hoger worden ingeschat dan de risico's bij routinematige transacties. De accountant dient zich af te vragen waar gezien de door hem uit te voeren taken de grootste risico's te onderkennen zijn, waarbij een aansluiting op de management control-benadering zoveel mogelijk wordt nagestreefd. De mate waarin risico-afwegingen ondersteund kunnen worden met risico-analysemethoden is binnen de accountantswereld overigens volop onderwerp van discussie. Hieraan wordt in dit artikel voorbijgegaan.

De eerste twee fases van het proces van totstandkoming van een jaarrekening hebben directe relaties met de bedrijfsprocessen in een organisatie en de daarbij gehanteerde beheersingsstructuren. Zo zal het inkoopproces in een organisatie onder andere leiden tot het ontstaan van voorraad- en verplichtingenposities, die al dan niet juist, volledig en tijdig in het informatieproces (met als laatste vertaalslag de jaarrekening) tot uitdrukking komen. Automatisering ofwel IT vervult in dit informatieproces een steeds dominantere rol.

### Relatie met administratieve organisatie

Om waarde te kunnen ontlenen aan de beheersing van het informatievoorzieningsproces dient de accountant zich te verdiepen in de administratieve organisatie van dit informatieproces en de daarbij gehanteerde IT. Het is van belang dat inzicht verkregen wordt in de wijze waarop relevante posten in de jaarrekening tot stand komen door middel van geautomatiseerde informatiesystemen. Vervolgens dient te worden beschreven binnen welke technische infrastructuur deze informatiesystemen operationeel zijn. De te onderkennen IT-objecten (apparatuur, besturingsprogrammatuur, applica-

ties en organisatie) kunnen in meerdere of mindere mate als onderdeel van de certificerende activiteiten van de accountant onderwerp van onderzoek zijn. Dat IT tevens een hulpmiddel kan zijn bij het uitvoeren van het controleprogramma in plaats van object van onderzoek, is evident. Op het gebruik van audit-software wordt in dit artikel echter niet verder ingegaan (zie daarvoor het artikel over Audit automation elders in deze Compact).

In het licht van de moderne visie op administratieve organisatie en interne controle kan worden gesteld dat de beheersing van de bedrijfsprocessen een management-vraagstuk is. Eén van de deelaspecten daarbij is het waarborgen van de betrouwbaarheid van de financiële rapportage. Echter, de beheersing inclusief de te treffen maatregelen van administratieve organisatie en interne controle wordt in principe vanuit een integrale benadering door het management ingesteld, waarbij de relatie met het door de accountant primair gestelde betrouwbaarheidsvraagstuk niet altijd eenduidig is te leggen. Zeker in een geavanceerde IT-omgeving dient de accountant de samenhang tussen de beheersingsmaatregelen in en rondom IT en de uitwerking daarvan op de betrouwbaarheid van de posten in de jaarrekening veelal zelf in beeld te brengen. Dat hierbij voor zover mogelijk aansluiting wordt gezocht bij de management control-benadering is niet alleen om efficiëntieredenen verstandig, maar sluit ook aan bij de verwachtingen van het management. Natuurlijk worden deze activiteiten zoveel mogelijk uitgevoerd in samenspraak met de te controleren organisatie, eventueel ondersteund door gespecialiseerde EDP-auditors.

## RELATIE IT EN ACCOUNTANTSCONTROLE

Door de introductie van IT verandert de controlefunctie van de accountant niet. Geen enkele methodiek van gegevensverwerking kan op zichzelf de zekerheid verschaffen dat de jaarrekening een getrouw beeld geeft. Derhalve zal de accountant die gebruik maakt van de management control-procedures zelfstandig controle dienen uit te voeren. Aangezien de integratie van IT in de bedrijfsprocessen en het daarbij behorende informatieproces echter voortschrijdt, verandert wel de wijze van uitvoering van de accountantsfunctie.

Het beoordelen van de betrouwbaarheid en in beperkte mate de continuïteit van IT als onderdeel van de accountantscontrole wordt algemeen geaccepteerd. Slechts in beperkte mate is het denkbaar dat IT als een 'black box' kan worden benaderd, waarbij de accountant nog in staat is volledig onafhankelijk van IT zijn controleprogramma uit te voeren. De consequenties van de toenemende betekenis van IT voor de accountantsfunctie worden nader belicht.

Zoals in de Inleiding is gesteld, maakt de accountant bij de systeemgerichte benadering gebruik van de beheersingsmaatregelen in het proces van verwerking van het object van onderzoek. In een omgeving met IT zijn deze maatregelen te onderscheiden naar:

- *Application controls.*

In [Jenk92] worden deze controls omschreven als procedures gericht op het adequaat bewaren van de financiële gegevensbestanden en op het zeker stellen dat alleen geautoriseerde transacties juist, volledig en tijdig worden verwerkt en vastgelegd. Deze procedures omvatten zowel geprogrammeerde controles alsook in het verlengde daarvan handmatige handelingen.
Het is van belang te benadrukken dat in deze definitie de application controls de user controls omvatten. Deze definitie is ontleend aan de Angelsaksische benadering van dit begrip, in Nederland worden de application en user controls soms nog separaat behandeld. User controls hebben dan de betekenis van onafhankelijk van de automatisering uitgevoerde controlehandelingen. Deze situatie doet zich steeds minder voor.

- *General IT controls.*

Activiteiten van interne controle om redelijk zeker te stellen dat de geprogrammeerde functies, inclusief controles, in een applicatie adequaat worden ontworpen, geïmplementeerd, onderhouden en verwerkt.
Deze activiteiten hebben betrekking op:
- ontwikkeling en onderhoud van applicaties;
- toegangsbeveiliging;
- rekencentrumprocedures;
- aanschaf en onderhoud van besturingsprogrammatuur.

*Door de introductie van IT verandert de wijze van uitvoering van de accountantscontrole.*

De betrouwbaarheid van de verantwoordingsinformatie kan dus worden gewaarborgd door een combinatie van geprogrammeerde en handmatige controles en general IT controls. Het begrip betrouwbaarheid behoeft hierbij wellicht nog enige toelichting. Betrouwbaarheid in relatie tot gegevens heeft betrekking op aspecten als juistheid en volledigheid. Betrouwbaarheid in relatie tot application controls betreft de vraag of de toepassingsprogrammatuur, inclusief de hierin opgenomen geprogrammeerde controles, en de handmatige gegevensverwerkende activiteiten naar behoren functioneren. Dit laatste wil zeggen in overeenstemming met de specificaties, volgens de voorgeschreven procedures, etc. Hierbij moeten de specificaties en procedures aan daaraan te stellen eisen voldoen (zoals te ontlenen aan de leer van de administratieve organisatie). In relatie tot de general IT controls houdt betrouwbaarheid eveneens in het functioneren volgens voorgeschreven specificaties, die dienen te voldoen aan bepaalde eisen.

## BEOORDELEN APPLICATION CONTROLS

Het is van belang dat, voordat applicaties worden onderzocht op aspecten van interne controle, een grondige analyse plaatsvindt van de relatie tussen de posten in de jaarrekeningen en de diverse applicaties. De kritische en risicovolle applicaties, gezien vanuit de invalshoek van de controlerend accountant, dienen te worden onderkend.

*Audit evidence is in toenemende mate te ontlenen aan IT.*

Deze analyse wordt nog te beperkt uitgevoerd, waardoor het interpreteren van de uitkomsten van een betrouwbaarheidsonderzoek in termen van de voor de accountant relevante posten in de jaarrekening nog moeilijk is [Fijn93]. Over de aard en aanpak van een onderzoek naar de betrouwbaarheid van een applicatie is al regelmatig gepubliceerd. In het artikel van Fijneman [Fijn93] is een stapsgewijze aanpak beschreven. Per onderkende functie in de applicatie worden heldere normen geformuleerd ten aanzien van de betrouwbaarheid. Deze normen worden door de accountant als leidraad gebruikt voor het inventariseren van de gerealiseerde application controls (volgens Angelsaksische definitie inclusief de handmatige procedures). Het evalueren of de aangetroffen set van application controls afdoende is voor de controlerend accountant is sterk situatie-afhankelijk. Echter, voor een aantal applicatiegebieden (zoals grootboek, debiteuren, crediteuren) is redelijke consensus bereikt over de minimaal te realiseren application controls als basis om te komen tot een positieve beoordeling. Het metaproces (de general IT controls) ter beheersing van de application controls is nog te weinig gestructureerd behandeld.

De verdere aandacht in het artikel gaat uit naar de behandeling van de general IT controls in het kader van de accountantscontrole.

## BEOORDELEN GENERAL IT CONTROLS

De vraag kan worden gesteld welke 'evidence' een onderzoek naar de betrouwbaarheid van een proces oplevert ten aanzien van de betrouwbaarheid van het produkt ervan. Voor de procescontroles (zijnde application controls) is hierover enige consensus bereikt. Ten aanzien van de metaprocescontroles (de general IT controls) is de discussie nog gaande. Dat de metaprocescontroles echter evidence kunnen opleveren ten aanzien van de betrouwbaarheid van het produkt lijkt aannemelijk. Door het realiseren van bepaalde algemene beveiligingsmaatregelen worden de processen in een gecontroleerde omgeving uitgevoerd. Hierdoor is niet alleen een voorwaarde geschapen om de procescontroles te kunnen uitvoeren maar kunnen ook zekerheden over het produkt worden verkregen. Door het installeren van toegangsbeveiligingssoftware bijvoorbeeld kunnen toegangsbeveiligingsmaatregelen voor alle applicaties worden gerealiseerd. Als onderdeel van het controleprogramma dient het juist functioneren van deze algemene software continu te worden vastgesteld. Zodoende kan extra zekerheid worden verkregen over de betrouwbaarheid van de geïmplementeerde autorisatietabellen voor de diverse processen en in het verlengde hiervan over de handhaving van de functiescheidingen in de geautomatiseerde omgeving. Let wel, gesproken wordt over extra zekerheid, hetgeen impliceert dat nog altijd een mix van controlemaatregelen dient te worden ingezet. Het alleen beoordelen van de general IT controls zal niet afdoende blijken te zijn, om tot aanvaardbare uitspraken over het object van onderzoek te komen.

Aangezien het accountantsonderzoek gericht is op het beperken van risico's of anders gezegd het vergaren van zekerheid, past hierbij aandacht voor de general IT controls. De kans op het optreden van een fout in de gegevens en gegevensverwerking in een omgeving met beperkte general IT controls is namelijk groter dan de kans hierop in een omgeving met voldoende management-aandacht hiervoor.

De centraal te beantwoorden vraag is of de general IT controls voor de te onderzoeken organisatie acceptabel zijn, rekening houdend met de grootte en complexiteit van en risico's in een organisatie. Hieruit blijkt direct dat er niet één stelsel van normen en maatregelen is op het gebied van de general IT controls, dat voor elke organisatie op dezelfde wijze dient te worden gerealiseerd. Ook in een relatief kleine organisatie (met bijvoorbeeld twee IT-medewerkers) moet het mogelijk zijn in het kader van de accountantscontrole te steunen op de kwaliteit van de general IT controls. In het artikel van De Munck [Munc93] is al eerder gesignaleerd dat de controlerend accountant wellicht te snel besluit om van deze waarborgen geen gebruik te maken.
General IT controls hebben betrekking op de systeemontwikkelings-, onderhouds- en verwerkingsomgeving. De general IT controls hebben tot doel te waarborgen dat informatiesystemen effectief worden ontwikkeld en geïmplementeerd en dat gegevens en programma's adequaat worden beschermd. Algemene procedure- en beleidsuitspraken ter beheersing van de IT en functiescheidingen in de gebruikersorganisatie en tussen de IT-afdeling en de gebruikers dienen voorhanden te zijn. Deze algemene procedures worden geconcretiseerd in de al eerder genoemde vier gebieden ontwikkeling en onderhoud van applicaties, toegangsbeveiliging, rekencentrumprocedures en aanschaf en onderhoud van besturingsprogrammatuur.

Zonder de intentie te hebben in dit artikel een volledig controleprogramma voor het beoordelen van de general IT controls te beschrijven zal een aantal relevante aandachtspunten per onderkend gebied worden toegelicht.

### Algemene procedures

De algemene procedures liggen specifiek op het terrein van het algemeen management. Voor het beoordelen van deze procedures is het van belang om een beeld te krijgen van de planning van IT, de management-verantwoordelijkheden ten aanzien van IT, de verantwoordelijkheden van de IT-afdeling, de beveiligingsprocedures en de invulling van de security-functie. Audit evidence is onder andere te ontlenen aan het opvragen van het informatie- en automatiseringsbeleid, het automatiseringsplan, de budgetten (over meerdere jaren ten behoeve van trendanalyses), de verslagen van relevante management-bijeenkomsten, het beveiligingsbeleid, de organisatiestructuur en taakstellingen en de security-verslagen. De noodzakelijke audit evidence kan variëren met de grootte van de organisatie. In een kleinschalige omgeving kan ondanks het ontbreken van formele procedures toch worden geconcludeerd dat het management de IT voldoende beheerst.

### Functiescheidingen

De functiescheidingen hebben betrekking op het vaststellen van de traditionele functiescheidingen tussen de gebruikers en de IT-afdeling en de verdere functiescheidingen binnen de IT-afdeling. Aan de hand van de organisatieschema's, de taakbeschrijvingen, het beveiligingsbeleid en de operationele verantwoordingen kan hiervan een beeld worden gevormd. Indien geconstateerd wordt dat de functiescheiding tussen de gebruikers en de IT-afdeling niet aanwezig is (bijvoorbeeld het PC-netwerk en de applicatie worden beheerd door de controller), behoeft dit nog geen problemen op te leveren. Het is denkbaar dat in die organisatie alleen een standaardpakket wordt gebruikt, dat niet zelfstandig door de controller kan worden aangepast. De risico's van het ontbreken van de functiescheiding nemen dan duidelijk af.

### Ontwikkeling en onderhoud van applicaties

Met betrekking tot het ontwikkelen en onderhouden van applicaties spelen een rol:
- het specificeren van de eisen en wensen;
- het bepalen van prioriteiten voor het aanpassen en/of ontwikkelen van applicaties;
- de ontwikkelingsmethode;
- de test-, acceptatie- en overdrachtsprocedures;
- de gebruikerstraining en het opstellen van de documentatie;
- de wijze van implementatie;
- de behandeling van noodprocedures (ad hoc-aanpassingen in de applicaties).

In het artikel van Van Beek wordt op deze aandachtspunten verder ingegaan.

Bij het aanschaffen van standaardpakketten dienen bovenstaande aandachtsgebieden anders te worden geëvalueerd dan bij ontwikkeling van applicaties in eigen huis. Mogelijke controlehandelingen zijn onder meer het beoordelen van de testverslagen, het inventariseren van de inhoud van de produktie-omgeving en het beoordelen van de library software. De certificerende accountant zal zich overigens primair richten op de test-, acceptatie- en overdrachtsprocedures. Het is van belang te onderkennen dat bij het adequaat uitvoeren van de test-, acceptatie- en overdrachtsprocedures de application controls worden getest. Indien aansluitend de applicaties op een juiste wijze worden geïmplementeerd en beveiligd in de operationele omgeving functioneren de application controls in principe naar behoren. Lijncontroles op de change management-procedures dienen dan wel in het controleprogramma te worden gedefinieerd.

*Onbekend maakt onbemind*
*geldt zeker voor*
*de general IT-controls.*

### Toegangsbeveiliging

De relevante onderwerpen ten aanzien van het inrichten van de logische toegangsbeveiliging betreffen het identificeren van risicovolle gegevens en applicaties, het scheiden van de ontwikkel/test- en produktie-omgevingen, het gebruik van user-identificaties en passwords, het al dan niet benutten van menubeveiliging, de netwerkbeveiliging en het registreren en beheren van de gehele logische toegangsbeveiliging. Mogelijke controlemaatregelen zijn het beoordelen van de logging-informatie, de parameterinstelling van de toegangsbeveiligingssoftware, de interfaces tussen de systeemsoftware en de applicaties, de actuele autorisatietabellen, de autorisatieprocedures, het personeelsbestand in relatie tot de autorisatietabel en de security-verslagen. Vele variaties op de te treffen maatregelen afhankelijk van de grootte van de organisatie maar ook van de stand van de techniek zijn denkbaar. De audit-risico's dienen per situatie te worden afgewogen, waarbij onder andere rekening dient te worden gehouden met de complexiteit van de IT-omgeving en het belang van de gegevensstromen die kunnen worden beïnvloed.

### Rekencentrumprocedures

Als aandachtspunten zijn te noemen de capaciteitsplanning en het beheer daarvan, de planning van de verwerking, de documentatie van de verwerkingsprocedures (met name ook de behandeling van uitzonderingen en storingen) en het netwerkbeheer. In het controleprogramma kan aandacht worden gevraagd voor onder andere de beoordelingen van de implementatieprocedures van hardware- en netwerkcomponenten, de actualiteit van de registratie van het netwerk, de inhoud van de onderhoudscontracten, de service levels, de vastlegging van de performance en storingen, en de operating instructies. Het verkrijgen van inzicht in de operationele gegevensverwerking staat daarbij

centraal, waarbij de mate van complexiteit sterk varieert per soort IT-omgeving. Ook hier geldt wederom dat de accountant aansluiting zoekt bij de interne procedures ter beheersing van het rekencentrum.

**Aanschaf en onderhoud van besturingsprogrammatuur**

De betekenis van besturingsprogrammatuur voor het creëren van een betrouwbare verwerkingsomgeving neemt duidelijk toe. De verschillende componenten van de besturingsprogrammatuur dienen te worden geïdentificeerd en met name dient te worden bepaald welke betrouwbaarheidsmaatregelen door deze componenten worden afgedekt. Zo kunnen diverse toegangsbeveiligingsmaatregelen en integriteitsmaatregelen (ter ondersteuning van de application controls) in een database management-systeem zijn gerealiseerd. De change management-procedures ten aanzien van belangrijke componenten van de besturingsprogrammatuur, gericht op het onderkennen van de security-consequenties, dienen te worden beoordeeld. De contracten met de leveranciers en de oplossingen van geconstateerde operationele problemen ('temporary fixes') dienen eveneens te worden beoordeeld.

**Uitwerken controleprogramma general IT controls**

Feitelijk dient de accountant een concreet controleprogramma ten aanzien van de general IT controls uit te werken, waarbij naast het vaststellen van de opzet en het bestaan van maatregelen tevens de werking van bepaalde essentiële maatregelen wordt getoetst. Audit software kan daarbij worden aangewend voor het verkrijgen van evidence omtrent de werking (zie daarvoor het artikel Audit automation), waarbij het 'multi-purpose'-karakter van geautomatiseerde controletoepassingen de nodige efficiëntie kan opleveren. De accountant moet

*Minimumeisen ten aanzien van beheersingsmaatregelen gericht op IT moeten worden gedefinieerd.*

in zijn controleprogramma een samenhangend geheel controlehandelingen gericht op de general IT controls beschrijven, waarbij tevens de raakvlakken met de application controls inzichtelijk worden gemaakt. Met andere woorden, indien bij de uitvoering van het controleprogramma bepaalde omissies in de general IT controls worden geconstateerd, dient het effect daarvan op de application controls en het uiteindelijke object van onderzoek (de financiële gegevens) te kunnen worden bepaald.

## PRAKTISCHE PROBLEMEN BIJ BEOORDELEN GENERAL IT CONTROLS

In het voorgaande is een benaderingswijze voor de accountant met betrekking tot de general IT controls uiteengezet. Bij de praktische uitwerking hiervan blijkt zich toch een aantal problemen voor te doen.
Het uitwerken van een controleprogramma voor het beoordelen van de general IT controls in een concrete IT-omgeving vergt de nodige aandacht. Hoewel de te hanteren normen voor het beoordelen van de betrouwbaarheid van de general IT controls veelal gelijk kunnen zijn, blijkt dat te weinig aandacht bestaat voor de variëteit aan maatregelen. Bij de beoordeling worden mogelijke maatregelen te veel tot normen verheven, waardoor in vele situaties (met name in kleinschalige omgevingen) een negatief oordeel wordt afgegeven. De relatie met de algemene management control-benadering is soms ook te beperkt onderkend, zodat uitspraken te veel worden gebaseerd op technische feiten zonder rekening te houden met de organisatorische structuur en aansturing van een organisatie. Het beoordelen van de general IT controls kan dan ontaarden in een vakgebied van en voor technical EDP-auditors, waarbij de controlerend accountant als primaire afnemer van de uitkomsten van een dergelijke beoordeling te veel aan de zijlijn staat.

De aansluiting tussen de te controleren financiële gegevens, de applicaties en de gehanteerde IT-infrastructuur wordt in een aantal controleprogramma's te weinig inzichtelijk gemaakt. Het is van belang te onderkennen welke delen van de IT-omgeving (en dan met name de applicaties) van belang zijn in relatie tot de relevante posten in de jaarrekening, zodat bij het beoordelen van de IT-omgeving ook rekening kan worden gehouden met de mogelijke audit-risico's. Een samenhangend geheel van audit-objecten ontbreekt nog te vaak.

Al eerder is de vraag gesteld welke audit evidence kan worden ontleend aan het beoordelen van de general IT controls. In welke mate kan een positief oordeel over de betrouwbaarheid van het metaproces (general IT controls) zekerheid opleveren voor de betrouwbaarheid van het proces (application controls) en de daarin tot stand komende produkten (de financiële gegevens).
Hoewel hierover in de accountantswereld nog geen consensus is bereikt, lijkt de algemene tendens te zijn dat het ontlenen van audit evidence aan het beoordelen van de general IT controls voor de certificerende activiteiten wordt geaccepteerd.

Afsluitend dient bij de toenemende aandacht voor de management control-benadering te worden bedacht dat de accountant, indien hij aansluiting zoekt bij deze benadering, wordt geconfronteerd met de gehele beheersingssystematiek gezien vanuit het management. De accountant dient binnen de kaders van de financiële controle vast te stellen welke betrouwbaarheidsmaatregelen in de management control zijn ingebed. Vanuit de leer van de administratieve organisatie dienen de mini-

mumeisen gericht op de betrouwbaarheid van de gegevens en processen te worden vastgesteld. De geïnventariseerde maatregelen dienen te worden geëvalueerd aan de hand van deze minimumeisen.

## ONTWIKKELINGEN EN OPLOSSINGSRICHTINGEN

Het nadenken over en beschrijven van de invloed van IT op de accountantscontrole is geen nieuw onderwerp. De tijd voor het vinden van antwoorden lijkt echter aangebroken. Bijvoorbeeld door de introductie van de Wet computercriminaliteit is de noodzaak hiervan nog eens benadrukt. Volgens deze wet dient de accountant zijn bevindingen ten aanzien van de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking te vermelden in zijn verslag aan de raad van commissarissen en aan het bestuur. Een juiste interpretatie van deze passage betekent dat de accountant slechts die bevindingen behoeft te rapporteren die hem in het kader van zijn controle-activiteiten duidelijk zijn geworden. Een aanvullend onderzoek naar de betrouwbaarheid en continuïteit van IT hoeft niet te worden ingesteld. Echter, ter voorkoming van misverstanden moet de accountant met zijn cliënt communiceren over de wijze waarop de accountant in het kader van zijn controle-activiteiten omgaat met IT. De invloed van IT op de accountantscontrole is daarbij een belangrijk vraagstuk.

De noodzaak om aandacht te schenken aan IT in het kader van de accountantsfunctie blijkt ook uit het IFAC-rapport 'Impact of Information Technology on the Accountancy Profession' [Kamp93]. Door de geautomatiseerde informatiesystemen worden andere beheersingsmaatregelen en in het verlengde daarvan andere vormen van audit evidence voor de accountant geïntroduceerd. Als uitvloeisel hiervan wordt in NIVRA-verband gewerkt aan een controlerichtlijn om meer aandacht te schenken aan administratieve organisatie en dus ook aan IT. Dezelfde tendens is waarneembaar in de nieuwe cursusnota administratieve organisatie [Nimw93]. Het beheer van IT dient in het algemeen veel meer vanuit een informatie-management-invalshoek te worden benaderd dan vanuit technologisch perspectief. Deze benadering sluit volledig aan bij de eerder beschreven moderne visie op administratieve organisatie (de management control-benadering).

De Stuurgroep EDP-auditors van het NIVRA heeft zich ook gebogen over de vraag wat de invloed van de kwaliteit van de automatisering op het controleprogramma van de accountant is [Kooi93]. Alhoewel nog geen definitieve standpunten zijn ingenomen, zijn toch denklijnen ontwikkeld die vermeldenswaard zijn. Minimumeisen ten aanzien van de beheersingsmaatregelen (normen en standaarden) gericht op IT zijn ondanks de verscheidenheid aan typologieën, wisselende technieken en verschillen in bedrijfsomvang te formuleren. In principe is er materiaal genoeg om deze normen en standaarden nader uit te werken. Een andere denklijn is dat bij het optreden van ernstige gebreken in de general IT controls de accountant de efficiëntie en effectiviteit van de controle niet zonder meer kan vergroten door het intensiever toepassen van gegevensgerichte controles. Gebreken in de general IT controls kunnen namelijk leiden tot onzekerheid over de volledigheid van het transactievolume en de handhaving van functiescheidingen, hetgeen directe gevolgen zou moeten hebben voor de af te geven verklaring.

Ten slotte is vermeldenswaard dat de Commissie Automatiseringsvraagstukken van het NIVRA actief met deze materie bezig is. Een werkgroep is ingesteld, die in het kader van de zogeheten eerstelijns EDP-auditing (EDP-auditing ten behoeve van de controlerend accountant) een minimumpositie voor de betrouwbaarheid en continuïteit van IT in de vorm van normen en standaarden probeert te definiëren. De general IT controls staan hierbij centraal. In een nadere uitwerking van één van de door de Stuurgroep EDP-auditors gedestilleerde denklijnen wordt dus al voorzien.

Een verschil met de in dit artikel eerder beschreven uitgangspunten lijkt te bestaan. Gesteld is dat de general IT controls niet alleen voorwaardenscheppend zijn voor de goede uitvoering van het proces, maar ook audit evidence kunnen opleveren voor de betrouwbaarheid van het produkt. Het definiëren van een minimumpositie, zoals nu vanuit het NIVRA wordt gepoogd, is hiervoor slechts een eerste stap. De aanduiding minimumpositie wijst erop dat het afgeven van een goedkeurende verklaring bij enige gebreken in deze positie een moeilijke zo niet onmogelijke zaak wordt. Tijdige communicatie met de opdrachtgever om tot oplossingen voor de geconstateerde problemen te komen is dan ook onontbeerlijk. Het is denkbaar dat de minimumpositie in de vorm van normen en standaarden wordt uitgewerkt, die met behulp van verschillende maatregelen afhankelijk van de organisatie kunnen worden afgedekt. Hopelijk wenst het NIVRA ook de vervolgstappen te definiëren, waardoor de general IT controls niet meer alleen een randvoorwaardelijke betekenis vervullen. De minimumpositie zou slechts een opstap moeten vormen naar een volwaardige integratie van de general IT controls en in het verlengde daarvan de application controls, in de controleprogramma's van de certificerende accountant.

## TEN SLOTTE

De betekenis van de general IT controls voor de accountantscontrole heeft in dit artikel centraal gestaan. Dat het accountantsberoep geen statisch beroep is of zou moeten zijn, is uit bovenstaande uiteenzetting genoegzaam gebleken. Het beheer van IT en de consequenties daarvan voor de controlerend accountant vragen om duidelijke antwoorden. Het accountantsprodukt wordt aangeboden in een sterk veranderende markt, door sommigen ook wel aangeduid als een 'buyers market'. In deze markt waar de klant en niet de accountant koning

*Drs. R.G.A. Fijneman RE RA Is sinds 1986 werkzaam bij KPMG Klynveld EDP Auditors. Zijn audit-ervaring ligt met name op het gebied van administratieve organisatie, automatiseringsorganisaties en informatiesystemen. Hij is docent van cursussen op het gebied van automatisering en controle.*

is, wordt het steeds belangrijker niet alleen duidelijkheid te scheppen over de accountantsfunctie als zodanig maar ook over de wijze van uitoefening van het beroep. Dat IT als object van onderzoek daarbij niet meer is weg te denken staat niet ter discussie. De beoordeling van de general IT controls levert in veel controle-omgevingen toegevoegde waarde op voor de accountant. De beoordeling van de general IT controls kan goed in de risico-aanpak worden ingepast.

Geconstateerd is dat de wijze van behandeling en beoordeling van de general IT controls nog verdere uitwerking behoeft. De praktische vertaling in een controleprogramma dient nadrukkelijk aandacht te krijgen. Het vinden van concrete antwoorden op de gestelde praktische en deels ook theoretische problemen moet mede gezien het zich verder ontwikkelende EDP-auditing-vakgebied mogelijk zijn. Accountants en EDP-auditors moeten daartoe de handen ineenslaan en bereid zijn de controleprogramma's daadwerkelijk te enten op de controle-omgevingen voorzien van moderne IT. IT is daarbij voor de accountant veel eerder een 'opportunity' dan een 'threat'.

## LITERATUUR

[Bakk93] W. Bakker, *De bijdrage van de EDP-auditor aan de jaarrekeningcontrole,* de EDP-auditor, 2e jaargang nr. 1.

[Brou93] J. Brouwer en W.J. de Vries, *Beheersing van geautomatiseerde gegevensverwerking,* in: Update on EDP & Accountancy, VERA studiereeks nr. 3, 1993.

[COSO92] *Internal Control - Integrated Framework,* Rapport van Committee of Sponsoring Organizations of the Treadway Commission, september 1992.

[Else93] A. Elsenaar, *Informatietechnologie; Kans of bedreiging,* BIKMAG special 1993, Bestuurlijk Informatiekundig Magazine Tilburg.

[Fijne93] R.G.A. Fijneman en E.P.R. van Vroenhoven, *Systeembeoordeling op basis van risico-analyse,* in: Update on EDP & Accountancy, VERA Studiereeks nr. 3, 1993. Dit artikel is een bewerkte versie van een eerder in Compact 1992/2 verschenen artikel.

[Hart92] P.A. Hartog, A. Molenkamp en J.H.M. Otten, *Kwaliteit van de administratieve dienstverlening,* Kluwer Bedrijfswetenschappen, 1992.

[Jenk92] B. Jenkins, P. Cooke en P. Quest, *An audit approach to computers,* The Institute of Chartered Accountants, London 1992.

[Kamp93] H.A. Kampert, *Impact of Information Technology on the Accountancy Profession,* De Accountant nr. 8, april 1993.

[Kooij93] J.L.H. Kooijman, *Resultaten automatiseringsonderzoek en jaarrekeningcontrole,* De Accountant nr. 9, mei 1993.

[Munc93] W. de Munck, *De invloed van automatisering op de accountantscontrole,* in: Update on EDP & Accountancy, VERA studiereeks nr. 3, 1993.

[Nimw93] H. van Nimwegen, *Cursusnota administratieve organisatie,* De Accountant nr. 8, april 1993.

[NIVR80] NIVRA, Deel III, *De invloed van de geautomatiseerde gegevensverwerking op de accountantscontrole,* Kluwer Bedrijfswetenschappen, 1980.

[Poel93] W.G. van der Poel en J. Waardenburg, *Jaarrekeningcontrole en EDP-audit,* MAB, mei 1993.

[Rijn93] J.M.A. van Rijn, *Automatisering; een bedreiging voor de accountant,* BIKMAG special 1993, Bestuurlijk Informatiekundig Magazine Tilburg.

# Aandacht voor interne controle tijdens systeemontwikkeling

Drs. J.J. van Beek RE RA

**Om te voorkomen dat een informatiesysteem wordt opgeleverd met onvoldoende waarborgen voor een betrouwbare gegevensverwerking, kan de accountant of EDP-auditor een participerende rol vervullen bij het ontwikkelproces. Een bijkomend voordeel is dat door participatie veel kennis wordt opgedaan over het administratieve en interne-controlesysteem van de gecontroleerde huishouding.**
**Van Beek schetst vanuit zijn praktijkervaringen een gestructureerde aanpak voor het ontwerpen van een evenwichtig stelsel van interne-controlemaatregelen tijdens het systeemontwikkelingstraject.**

## INLEIDING

Het gebruik van informatietechnologie heeft een onmiskenbare invloed op de wijze waarop binnen organisaties de betrouwbaarheid van de informatievoorziening wordt gewaarborgd. Eén van de belangrijkste gevolgen van de voortschrijdende automatisering is het vervangen van gebruikerscontroles door beheersingsmaatregelen (interne controles in ruime zin) in geautomatiseerde systemen (computer controls). Het grote voordeel van controles opgenomen in het geautomatiseerde systeem is dat deze door de computer altijd worden uitgevoerd. Een door de gebruiker te verrichten controle mist deze zekerheid. Daarnaast kunnen met behulp van het geautomatiseerde systeem op efficiënte wijze preventieve controles worden uitgevoerd, zodat fouten in de gegevensverwerking en tijdrovende correctieprocedures worden voorkomen.

Een stelsel van interne-controlemaatregelen (IC-maatregelen) kan slechts effectief zijn indien de getroffen maatregelen een samenhangend geheel vormen. Om de gewenste samenhang tussen de maatregelen te bereiken, is het noodzakelijk dat tijdens de ontwikkeling van het informatiesysteem expliciete aandacht wordt besteed aan de benodigde IC-maatregelen. Daarnaast is het uit het oogpunt van efficiëntie gewenst in een vroeg stadium van de systeemontwikkeling aandacht te besteden aan het inbouwen van de IC-maatregelen. De kosten van het herstellen van geconstateerde gebreken in een informatiesysteem nemen immers aanzienlijk toe naarmate de gebreken later in het ontwikkeltraject van het systeem naar voren komen.

In de praktijk blijkt dat het realiseren van IC-maatregelen tijdens systeemontwikkeling niet de gewenste aandacht krijgt. Dit is onder meer het gevolg van het ontbreken van een gestructureerde aanpak, gebrek aan kennis en tijdsdruk. Als het management wel aandacht besteedt aan de benodigde IC-maatregelen zal het veelal een accountant of een EDP-auditor de opdracht geven de IC-maatregelen voor het informatiesysteem op te stellen. Afgezien van een specifieke opdracht van het management kan het voor de accountant vanuit zijn certificerende functie als controleur van de jaarrekening gewenst zijn in een vroeg stadium betrokken te zijn bij de systeemontwikkeling.

In dit artikel wordt allereerst ingegaan op de relatie tussen accountantscontrole en systeemontwikkeling. Vervolgens wordt een aantal veel voorkomende knelpunten bij het inbouwen van IC-maatregelen besproken. Tot slot wordt een aanpak beschreven die kan worden gebruikt voor het realiseren van een samenhangend stelsel van beheersingsmaatregelen binnen en rond een geautomatiseerd systeem. Deze aanpak is gebaseerd op de CASA-methode [Koed86] en op praktijkervaringen die binnen KPMG Klynveld met het participeren tijdens het ontwikkelproces zijn opgedaan.

## RELATIE ACCOUNTANTSCONTROLE EN SYSTEEMONTWIKKELING

In het artikel van Fijneman in deze Compact is aangegeven dat de accountant bij het inrichten van zijn controlewerkzaamheden in hoofdlijnen een tweetal verschillende benaderingen kan kiezen, namelijk gegevensgericht of systeemgericht. Als gevolg van de introductie van automatisering is er bij de systeemgerichte controle-aanpak nog een verschil te maken tussen een systeemgerichte aanpak met application controls en een systeemgerichte controle-aanpak met general IT controls.
Bij een systeemgerichte controle-aanpak met application controls is de controle-informatie uit het informatiesysteem het belangrijkste aandachtspunt. De gebruiker kan met behulp van de controle-informatie vaststellen dat de invoer, verwerking en uitvoer van de gegevens juist en volledig is. Hieruit kan worden afgeleid dat de geautomatiseerde application controls naar behoren hebben gefunctioneerd, en niet zijn doorbroken als gevolg van een leemte in de general IT controls.
Bij een systeemgerichte controle-aanpak met general IT controls richt de accountant zich op de processen die moeten waarborgen dat de geautomatiseerde componenten van de application controls naar behoren functioneren, de general IT controls. Logische toegangsbeveiliging met de bijbehorende autorisatiematrix is hierbij het belangrijkste aandachtspunt.

Voor het ontwerpen van een doelmatige en efficiënte controle-aanpak is over het algemeen kennis nodig van het administratieve en interne-controlesysteem van de gecontroleerde organisatie, 'understanding the business'. Hierbij zal tevens een beoordeling moeten plaatsvinden van de opzet en het bestaan van de general IT controls om te bepalen of een systeemgerichte aanpak met general IT controls (inclusief die voor de systeemontwikkeling) mogelijk is. Een belangrijk voordeel van de general IT controls is daarbij dat deze voor meerdere informatiesystemen van toepassing zijn en dus kunnen leiden tot een efficiëntere controle-aanpak. De general IT controls met betrekking tot de systeemontwikkeling zijn de maatregelen die opgenomen zijn in het proces en de structuur van de ontwikkelorganisatie en tot doel hebben te waarborgen dat:
- functionele specificaties voldoen aan de daaraan te stellen eisen;
- functionele specificaties juist en volledig worden vertaald in het produkt, het uiteindelijke informatiesysteem.

*Een belangrijk voordeel van general IT controls is dat deze voor meerdere informatiesystemen van toepassing zijn en dus kunnen leiden tot een efficiëntere controle-aanpak.*

De belangrijkste general IT controls zijn in dit verband:
- functiescheiding tussen systeemontwikkeling en gebruikers;
- functiescheiding tussen systeemontwikkeling en de verwerkings- en transportorganisatie;
- een duidelijke omschrijving van de taken en verantwoordelijkheden in de ontwikkelorganisatie;
- de aanwezigheid van procedures en voorschriften met betrekking tot het ontwikkelen, testen, accepteren en overdragen van systemen en programmatuur;
- een actieve participatie van gebruikers (inclusief de inbreng van specifieke materiedeskundigen);
- de aanwezigheid van voorschriften met betrekking tot de documentatie van het informatiesysteem, inclusief gebruikershandleidingen;
- de aandacht in de voorschriften voor aspecten van interne controle zoals geprogrammeerde controles, verbandscontroles, audit trail en bevoegdheidsaspecten.

### Gegevensgericht

Bij de keuze voor een sterk gegevensgerichte controle-aanpak zal de relatie tussen systeemontwikkeling en accountantscontrole beperkt blijven. Alleen ter bepaling van de controle-aanpak zullen de opzet en het bestaan van de general IT controls globaal worden beoordeeld. Dit kan aan de hand van een eenvoudige vragenlijst plaatsvinden. Hierbij wordt opgemerkt dat in het maatschappelijk verkeer steeds vaker de verwachting bestaat dat automatisering, wanneer dit voor de gecontroleerde organisatie van belang is, een integraal onderdeel vormt van de controlebenadering. De recent van kracht geworden Wet computercriminaliteit kan hierbij als voorbeeld worden genoemd. In de Wet computercriminaliteit wordt de accountant verplicht zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking te melden in zijn rapportage aan de raad van commissarissen en aan het bestuur.

### Systeemgericht met application controls

Bij de systeemgerichte controle-aanpak waarbij de controle-informatie uit het informatiesysteem centraal staat, zal de relatie tussen systeemontwikkeling en accountantscontrole in principe ook beperkt zijn. Deze aanpak richt zich immers vooral op de gebruikerscontroles, waarbij zo min mogelijk wordt gesteund op de automatisering. Indien de accountant voor deze benadering kiest zal hij een beoordeling van het informatiesysteem uitvoeren. In de inleiding is echter aangegeven dat organisaties voor de betrouwbaarheid van de gegevensverwerking steeds meer zekerheid ontlenen aan de geautomatiseerde application controls en de general IT controls. Als dit het geval is zal ook het accent

in de controlebenadering door de accountant richting automatisering moeten verschuiven.

**Systeemgericht met general IT controls**

De systeemgerichte controle-aanpak met general IT controls betrekt automatisering meer expliciet in de controlebenadering. Voor de relatie met systeemontwikkeling is hierbij vooral de test-, acceptatie- en overdrachtsprocedure van belang. Vastgesteld zal moeten worden op welke programma's en hierin opgenomen application controls de controle door de accountant zich zal richten. Aan de hand van de aanwezige documentatie kan vervolgens de effectieve werking van de interne acceptatieprocedure worden vastgesteld. Na het uitvoeren van deze beoordeling hoeven in de komende periodes alleen de nieuwe programma's en wijzigingen te worden beoordeeld.

De accountant kan zich ook richten op het systeemontwikkelproces zelf. Het grote voordeel van deze aanpak is dat hiermee de mogelijkheid wordt geboden het ontwikkelproces tijdig bij te sturen. In de praktijk blijken de meeste general IT controls met betrekking tot systeemontwikkeling wel aanwezig, maar waar het aan ontbreekt is juist de expliciete aandacht voor aspecten van interne controle, zoals geprogrammeerde controles, verbandscontroles, audit trail en bevoegdheidsaspecten. Primair betekent dit voor het management van de organisatie het risico dat de betrouwbaarheid van de informatievoorziening niet voldoende is gewaarborgd. Op termijn zal ook de accountant met het informatiesysteem worden geconfronteerd. Onvoldoende aandacht voor IC-aspecten betekent voor de accountant dat mogelijk extra controlerisico's optreden en dat de keuze voor een systeemgerichte controlebenadering niet meer mogelijk is. Denk bijvoorbeeld aan de ontwikkelingen rond EDI. In het NIVRA-studierapport 24 over EDI wordt geconcludeerd dat meer dan ooit geldt dat de accountant in een vroeg stadium betrokken moet zijn bij de systeemontwikkeling en daarop actief moet inspelen. De kans dat men achteraf op grond van (controle- of) accountantseisen de inmiddels gebouwde systemen kan of wil aanpassen, is over het algemeen gering.

Een ander belangrijk voordeel voor de accountant is dat door participatie tijdens de systeemontwikkeling veel kennis wordt verkregen over het administratieve en interne-controlesysteem van de gecontroleerde organisatie. Deze kennis kan worden gebruikt om de jaarrekeningcontrole op verantwoorde en efficiënte wijze in te richten. De accountant zal over het algemeen ten gevolge van het opnemen van interne controles in het informatiesysteem een besparing op zijn controle-arbeid kunnen bereiken door de mogelijkheid de gegevensgerichte controlehandelingen zoveel mogelijk te beperken. In de meeste gevallen zal met betrekking tot de door de accountant voorgestelde IC-maatregelen een kosten/baten-afweging moeten plaatsvinden. Wat zijn de besparingen in de controle-arbeid binnen de organisatie en bij de accountant, versus de kosten die het verwezenlijken van die wensen met zich meebrengt.

Door sommige accountants wordt gesteld dat participatie van de accountant tijdens de systeemontwikkeling de onafhankelijkheid kan ondermijnen. Door te participeren in het ontwikkelproces en zijn wensen met betrekking tot de interne controle in te brengen, bestaat het gevaar dat de beoordeling van het operationele systeem in de knel komt. Een ander risico is dat bij signalering van mogelijke tekortkomingen de accountant mede verantwoordelijk wordt gehouden. De auteur is het op dit punt eens met Hartman [Hart88] dat het evenwel als uiterst ondoelmatig moet worden gekenmerkt als de accountant alleen achteraf beoordelingen wil verrichten. Door tijdig te participeren kan de accountant de toegevoegde waarde van zijn dienstverlening aanzienlijk verhogen. Hierbij wordt opgemerkt dat het primair een verantwoordelijkheid blijft van het management om te beslissen in welke mate voorgestelde IC-maatregelen worden geïmplementeerd.

*Een informatiesysteem zonder een effectief stelsel van IC-maatregelen is voor de organisatie zonder waarde.*

## VEEL VOORKOMENDE KNELPUNTEN BIJ DE REALISATIE VAN IC-MAATREGELEN

Een informatiesysteem zonder een effectief stelsel van IC-maatregelen is voor de organisatie zonder waarde. Dit uitgangspunt zal door de meeste gebruikers en automatiseerders worden onderschreven. Het is echter daarmee in geen geval vanzelfsprekend dat expliciet aandacht wordt besteed aan de benodigde IC-maatregelen. In deze paragraaf wordt een aantal veel voorkomende knelpunten bij de realisatie van IC-maatregelen beschreven.

Het ontwerpen en implementeren van IC-maatregelen voor een informatiesysteem kan op vier manieren plaatsvinden [Bril83]:

1 toevallig;
2 op verzoek van de gebruikers;
3 door het onderkennen van het probleem door de systeemontwikkelaars;
4 door interventie van de accountant.

*Ad 1.*
Het feit dat alleen toevallig, zonder gestructureerde aanpak, aandacht wordt besteed aan interne controle wil niet zeggen dat het ontwikkelde informatiesysteem helemaal geen controles zal bevatten. In de praktijk blijkt soms dat in dergelijke systemen toch nog redelijke controles zijn opgenomen, zonder dat er echt over is nagedacht. In de meeste gevallen evenwel voldoen de systemen die

op deze manier ontwikkeld zijn niet aan de te stellen IC-eisen. Om deze reden is het vanzelfsprekend dat een gestructureerde aanpak de voorkeur verdient.

*Ad 2.*
Als gebruikers nadrukkelijk de eis van adequate interne controles naar voren brengen zullen deze controles normaal gesproken worden gerealiseerd. De meeste aanstaande gebruikers van het informatiesysteem denken echter niet na over interne controles (dat is toch het probleem van de accountants?) of gaan ervan uit dat de automatiseerders ervoor zullen zorgen dat het systeem betrouwbare informatie oplevert. Door deze afstandelijke houding bestaat het risico dat te weinig aandacht aan de controlemaatregelen wordt besteed. De praktijk leert dat wanneer gebruikers tijdig worden gewezen op de gevolgen van te weinig aandacht voor interne controle en vanuit het management worden gemotiveerd hieraan aandacht te besteden, goede resultaten mogelijk zijn. De IC-functionaliteit van een systeem is een onmisbaar onderdeel van het gehele informatiesysteem. Helaas wordt dit door aanstaande gebruikers nog niet altijd direct ingezien.

*De meeste aanstaande gebruikers gaan ervan uit dat de automatiseerders ervoor zullen zorgen dat het systeem betrouwbare informatie oplevert.*

*Ad 3.*
Door de meeste automatiseerders wordt het probleem van het ontwerpen van IC-maatregelen niet onderkend. Het is geen expliciet onderdeel van de ontwikkelmethodiek en er zijn geen duidelijke beloningen om aan dit onderwerp aandacht te geven, of sancties als dit niet wordt gedaan. Vaak wordt in de ontwikkelmethodiek verwezen naar eventuele eisen van de accountant. De kennis van systeemontwikkelaars over interne controle is vaak beperkt, omdat hieraan tijdens opleidingen weinig aandacht wordt besteed. Het inbouwen van interne controles brengt daarnaast kosten met zich mee, heeft mogelijk effecten voor de performance en legt beperkingen op aan het systeem. Dit geldt natuurlijk voor de meeste functionaliteit van het systeem, maar IC-functionaliteit wordt daarbij veelal als 'extra' gezien. Met deze achtergrond krijgt interne controle vaak een lage prioriteit bij de automatiseerders. Dit leidt nogal eens tot meningsverschillen tussen gebruikers en systeemontwikkelaars. Een belangrijk punt is ook het communicatieprobleem tussen de opstellers van de IC-eisen en de automatiseerders. De taal van interne controle en die van automatisering sluiten niet zonder meer op elkaar aan.

*Ad 4.*
Zoals in de inleiding is opgemerkt, zal het management in reactie op de geschetste problematiek mogelijk de accountant of EDP-auditor opdracht geven tijdens de systeemontwikkeling actief te participeren. Het probleem daarbij is dat niet alle organisaties intern over de benodigde deskundigheid beschikken en externe deskundigheid aanzienlijke kosten met zich meebrengt. Een ander punt is dat de accountants nog niet altijd de voordelen inzien van betrokkenheid bij de systeemontwikkeling. Op het punt van de onafhankelijkheid is in de vorige paragraaf al ingegaan. Daarnaast heeft dit te maken met het feit dat accountants ten onrechte denken dat voor de participatie veel kennis van automatiseringstechniek noodzakelijk is.

Voor de aanpak die moet worden gevolgd bij het inbouwen van interne controles tijdens systeemontwikkeling kan op basis van de genoemde knelpunten worden geconcludeerd dat in ieder geval de aanpak moet aansluiten bij de gevolgde ontwikkelmethodiek en de hierin onderkende fases. De noodzaak tot veel automatiseringskennis (communicatieprobleem) moet worden vermeden, terwijl aan de andere kant wel een vertaling mogelijk moet zijn richting de produkten van de systeemontwikkeling.

## BESCHRIJVING VAN DE AANPAK

De in deze paragraaf beschreven aanpak geeft de accountant of EDP-auditor een handvat om zijn participatie binnen een SO-project, gericht op het realiseren van een effectief stelsel van IC-maatregelen, te structureren en efficiënt te laten verlopen. De aanpak richt zich specifiek op de IC-aspecten, zoals geprogrammeerde controles, verbandscontroles, audit trail en bevoegdheidsaspecten. Op de benodigde general IT controls zal slechts globaal worden ingegaan.

Bij de uitvoering van de aanpak worden de volgende fases onderscheiden, waarbij in dit artikel wordt uitgegaan van de veelgebruikte SDM-fasering (zie ook figuur 1):
- Fase Definitiestudie:
  bepalen beheersingsfilosofie;
- Fase Basisontwerp:
  opstellen IC-eisen;
- Fase Detailontwerp:
  ontwerpen IC-maatregelen;
- Fase Realisatie:
  bewaken realisatie IC-aspecten;
- Fase Invoering:
  opzetten controlebeleid.

**Fase Definitiestudie:**
**Bepalen beheersingsfilosofie**

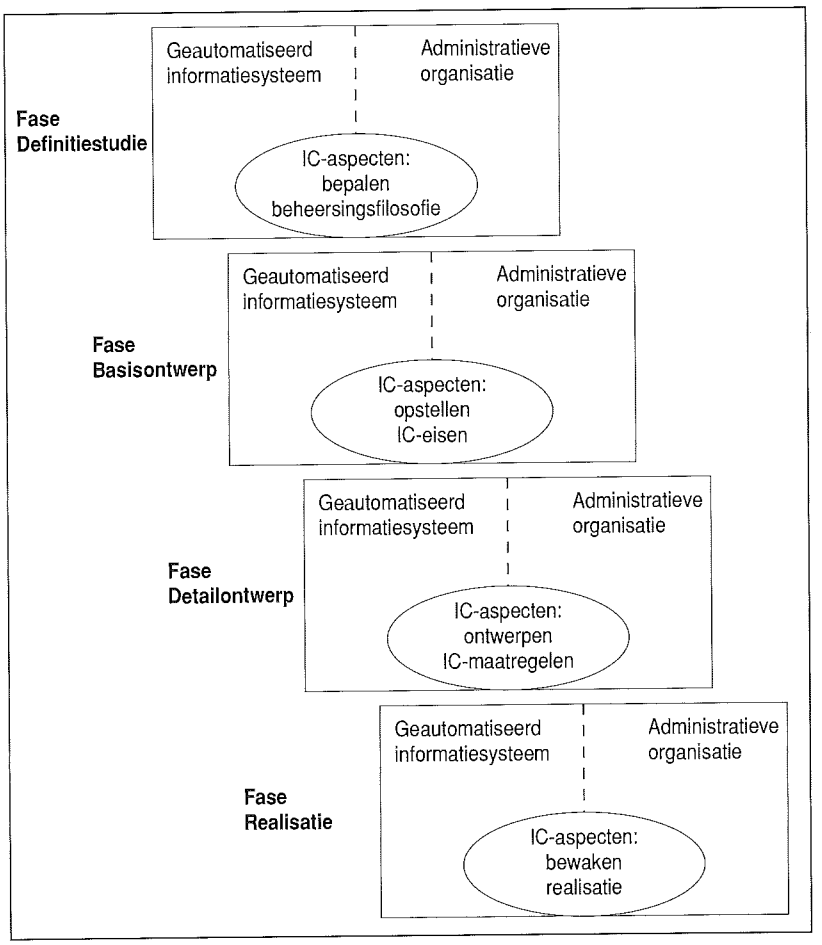
In de fase Informatieplanning/Definitiestudie moet door het management worden aangegeven welke uitgangspunten (beheersingsfilosofie) met betrekking tot de realisatie van de IC-maatregelen worden gevolgd. Hierbij wordt globaal een keuze

gemaakt voor het leggen van een accent op:
- de application controls met de bijbehorende controle-informatie;
- de application controls gewaarborgd door adequate general IT controls.

Hierbij wordt voor de duidelijkheid aangegeven dat de genoemde keuzemogelijkheden als uitersten kunnen worden beschouwd. Feitelijk is een wisselwerking waar te nemen tussen general IT controls en application controls met daarbinnen de gebruikerscontroles. Een matige opzet of werking van bepaalde general IT controls kan worden opgevangen door regelmatige controle of de application controls nog werken of door aanvullende gebruikerscontroles. Bij de keuze voor een bepaalde beheersingsfilosofie geeft het management de leidraad aan waarmee tijdens het ontwikkelproces wordt gewerkt. In de praktijk wordt tijdens de systeemontwikkeling vaak te weinig aandacht besteed aan de gebruikerscontroles. Met name de samenhang tussen de interne controle in het geautomatiseerde systeem en de interne controle in de administratieve organisatie (AO) rond het nieuwe systeem verdient aandacht.

De IC-maatregelen kunnen worden verdeeld in preventieve en repressieve maatregelen. Preventieve maatregelen zijn gericht op beheersing vóóraf, voorkoming van ontsporing (bijvoorbeeld functiescheiding). Repressieve maatregelen zijn specifieke controlehandelingen gericht op de ontdekking en het herstel van ontsporing achteraf (bijvoorbeeld cijferbeoordeling, verbandscontroles en detailcontroles). Een belangrijk aspect van de maatregelen is tevens de tijdigheid van de uitvoering van de controles. Om aan haar doel te beantwoorden moet een adequate combinatie van preventieve en repressieve maatregelen worden getroffen en in het stelsel van interne controle worden opgenomen.
Indien de gebruiker (deels) kan steunen op general IT controls met betrekking tot de automatiseringsorganisatie (zowel verwerkings- en transportorganisatie (VTO) als SO), zal de frequentie van de uitvoering van repressieve gebruikerscontroles kunnen afnemen. Als voorbeeld kan worden gedacht aan een geautomatiseerd systeem voor de berekening en uitbetaling van salarissen. Als niet kan worden gesteund op de ingebouwde controles en de betrouwbare verwerking bij het rekencentrum, betekent dit dat een relatief groot aantal salarisslips ter controle handmatig achteraf moet worden nagerekend. Hierdoor wordt zekerheid over de juiste berekeningen verkregen. Naarmate het systeem meer ingebouwde controles bevat en het rekencentrum waarborgen (general IT controls) bevat om een betrouwbare verwerking te garanderen, zal het aantal salarisslips dat wordt nagerekend, kunnen afnemen.

Onafhankelijk van het gekozen stelsel van controlemaatregelen zal bij een beheersbaar informatiesysteem de mogelijkheid tot repressieve gebruikerscontroles aanwezig moeten zijn. Strikt theoretisch is dit niet noodzakelijk, maar als er problemen optreden is het praktisch als voldoende 'kijkgaten' in het systeem zijn ingebouwd om hierop te kunnen terugvallen.




*Figuur 1. Gebruikte SDM-fasering.*

De gemaakte keuze wordt vastgelegd in een 'Raamwerk van IC-eisen' dat onderdeel moet gaan uitmaken van de projectdocumentatie. Afhankelijk van onder meer de bedrijfstypologie van de organisatie en de aard van het informatiesysteem worden de controledoelstellingen beschreven en vervolgens de IC-eisen op hoofdlijnen uitgewerkt. Hierbij wordt een onderscheid gemaakt tussen de belangrijkste componenten van het IC-stelsel:
- de invoer van mutaties;
- de verwerking door de automatiseringsorganisatie;
- de uitvoer van gegevens.

Een belangrijk onderdeel van de uitwerking is een beschrijving van de verschillende functies die bij het informatiesysteem zijn betrokken, de taken conform het gekozen beheersingsconcept en de aan de uitvoering van die taken verbonden IC-eisen. Bij de keuze voor het steunen op de general IT controls zal in de administratieve organisatie de inrichting van de applicatie- en gegevensbeheerfunctie bijvoorbeeld een belangrijk onderwerp vormen. Deze functie draagt zorg voor de coördinatie tussen gebruikers bij gemeenschappelijk gebruik van applicaties en gegevens.
De praktijk leert dat het opstellen van een Raamwerk IC-eisen in een vroegtijdig stadium van het project sterk is aan te bevelen. Indien niet vanaf de

start van een project aandacht aan interne controle wordt geschonken, wordt het zoals vermeld zeer moeilijk om een consistent geheel van maatregelen te realiseren. Tevens is het belangrijk de projectdeelnemers te motiveren om aandacht te besteden aan interne controle. Het opgestelde Raamwerk IC-eisen, dat wordt geaccepteerd en ondersteund door het management en de projectleiding, kan hierbij een cruciale rol vervullen.

*De praktijk leert dat het opstellen van een Raamwerk IC-eisen in een vroegtijdig stadium van het project sterk is aan te bevelen.*

**Fase Basisontwerp:**
**Opstellen IC-eisen**

De in het Raamwerk IC-eisen opgenomen hoofdlijnen moeten in de fase Basisontwerp worden geconcretiseerd naar betrouwbaarheidseisen per kritische functie van het informatiesysteem. Hiertoe zal met betrekking tot het informatiesysteem een vorm van risico-analyse [Jans91] worden uitgevoerd. Het uitgangspunt voor het concretiseren van de IC-eisen aan de hand van de risico-analyse vormen, conform de CASA-methode, de beschrijvingen van de gegevensverzamelingen. In de terminologie van de SO worden de gegevensverzamelingen ook wel aangeduid als het datamodel of entiteitenmodel. De volgende activiteiten worden onderscheiden:

– Opstellen of verkrijgen van een entiteiten/processen-matrix. Het informatiesysteem wordt in deze matrix beschreven als een verzameling gegevens waarop met behulp van functies manipulaties worden uitgevoerd. De aard van de manipulatie is hierbij eveneens van belang, bijvoorbeeld muteren of raadplegen. Een dergelijke entiteiten/processen-matrix is in veel gevallen aanwezig in de projectdocumentatie of kan eenvoudig worden samengesteld.

– Uitvoeren risico-analyse. In eerste instantie worden hiervoor de schadebepalende factoren en kansbepalende factoren vastgelegd. Binnen de CASA-methodiek wordt onderscheid gemaakt tussen vaste en variabele gegevens om de IC-eisen te kunnen afleiden. Door het gebruik van de schadefactoren en kansfactoren kan het onderscheid tussen vaste en variabele gegevens verder worden genuanceerd. De schadefactoren zijn van belang voor het bepalen van de potentiële schade-omvang ingeval de bedreiging van onbetrouwbare informatie manifest wordt. Schadebepalende factoren zijn onder meer:
  - de hoogte van de financiële gevolgen van een fout;
  - het aantal periodes dat een fout doorwerkt;
  - het aantal objecten dat gevolgen ondervindt van een fout;
  - de soort van mutaties.

De kansbepalende factoren zijn van belang om de kans in te schatten dat de onderkende bedreiging optreedt. Kansbepalende factoren zijn onder meer:
  - de mogelijkheid tot beïnvloeding door de functionaris die de mutaties invoert;
  - het belang van de functionaris die de mutaties invoert bij beïnvloeding;
  - de ervaringscijfers over opleiding en het gedrag van de functionaris die de mutaties invoert;
  - de complexiteit van de onderliggende voorschriften;
  - de mutatiegraad van programmatuur en tabellen;
  - de verhouding van IC-maatregelen in de programmatuur ten opzichte van handmatige IC-maatregelen.

Deze factoren worden gebruikt voor het uitvoeren van een kwalitatieve risico-analyse ten aanzien van de entiteiten en processen. Aan de hand van het inschatten van genoemde factoren kan een indeling van de entiteiten plaatsvinden al naargelang de combinatie van kans en schade-omvang als hoog, gemiddeld of laag wordt geclassificeerd. Het kwantificeren van kansen en schades blijkt in de praktijk bij een dergelijke risico-analyse weinig toegevoegde waarde te hebben. Tijdens de indeling is het van belang dat een goede afstemming plaatsvindt met materiedeskundige gebruikers. In de praktijk zijn het vaak de gebruikers die het beste kunnen aangeven wat de kritische gegevens uit het systeem zijn. In plaats van een complete analyse van de beschreven factoren is het bij eenvoudiger systemen ook mogelijk de indeling aan de hand van gesprekken met gebruikers te laten plaatsvinden.

– Opstellen van IC-eisen. Aan de hand van de indeling van entiteiten, de aard van de processen (bijvoorbeeld invoeren, wijzigen, verwijderen, raadplegen) wordt bepaald of er sprake is van zware, normale of lichte eisen. Indien gewenst kan hierbij nog een onderscheid worden gemaakt tussen bijvoorbeeld volledigheid en juistheid als betrouwbaarheidsaspect. Het resultaat zijn de IC-eisen per systeemfunctie en entiteit (eventueel te detailleren per gegevenselement). Deze IC-eisen moeten worden opgenomen in de projectdocumentatie.

**Fase Detailontwerp:**
**Ontwerpen van IC-maatregelen**

In de fase Detailontwerp moeten de geformuleerde IC-eisen worden omgezet in concrete maatregelen. Tot en met de vorige fase is het niet onoverkomelijk als de IC-aspecten nog in een algemene notitie in de projectdocumentatie zijn opgenomen. In de fase van het detailontwerp moeten per functie de IC-maatregelen worden beschreven, anders zullen deze niet worden gebouwd. Hierbij is de systeemontwikkelaar verantwoordelijk voor het opnemen van de gekozen maatregelen in het ontwerp. De

keuze van de maatregelen is afhankelijk van de gestelde IC-eisen. Voorbeelden van maatregelen zijn:
- dubbele invoer van gegevens;
- fiattering door een tweede functionaris;
- hash totals;
- bestaanbaarheidscontroles;
- waarschijnlijkheidscontroles;
- audit trail.

Het is voor de beoordeling van de IC-aspecten achteraf efficiënt dat in het ontwerp de gekozen IC-maatregelen apart zichtbaar worden gemaakt.

In deze fase zijn vaak verschillende systeemontwerpers met ieder hun eigen gedeelte van het ontwerp aan de slag. Een goede communicatie met de systeemontwikkelaars is dan ook van groot belang. Het is aan te bevelen een standaardset van de belangrijkste IC-maatregelen te definiëren die in de projectdocumentatie wordt opgenomen. Het NIVRA-geschrift 43, waarin een opsomming wordt gegeven van IC-maatregelen, zou hiervoor als bron kunnen dienen. Het doel van de standaardset is het bevorderen van een eenduidige interpretatie en uitwerking in het ontwerp. Per IC-maatregel moet een korte omschrijving aanwezig zijn waarin duidelijk wordt omschreven wat onder de maatregel wordt verstaan. In het ontwerp kan dan bijvoorbeeld worden volstaan met het noemen van de IC-maatregel.

Bij grotere SO-projecten zal de behoefte aan coördinatie van de IC-activiteiten binnen de SO zich nog sterker laten voelen. Gezien het ontbreken bij de meeste systeemontwikkelaars van voldoende inzicht is een mogelijke oplossing het benoemen van een zogenaamde IC-coördinator binnen de SO. Dit is meestal een systeemontwikkelaar met kennis van of affiniteit met interne controle. Deze IC-coördinator wordt verantwoordelijk voor de implementatie van interne controle in de SO-produkten. Hij kan als aanspreekpunt voor de SO, de gebruikers en de accountant of EDP-auditor fungeren. Het is van belang dat de IC-coördinator, ook als het geen fulltime-taak betreft, voortdurend aanwezig is om het doorgaans hoge tempo van de SO bij te houden. In dit verband is het tevens verstandig de toetsing op IC-aspecten een vast onderdeel te laten uitmaken van de procedures binnen de SO waarin de kwaliteit van de produkten wordt beoordeeld.

**Fase Realisatie:**
**Bewaken realisatie IC-aspecten**

Tijdens de fase Realisatie worden de functioneel ontworpen IC-maatregelen door de SO geïmplementeerd. De activiteiten in deze fase richten zich op het bewaken van het Raamwerk IC-eisen. Voortdurend moet erop worden toegezien dat afwijkingen, bijvoorbeeld doordat voorgestelde maatregelen technisch niet haalbaar zijn, binnen de grenzen van het Raamwerk blijven. De activiteiten zijn:
- het beoordelen van de tijdens de fase Realisatie naar voren gekomen wijzigingsvoorstellen ten aanzien van de functionaliteit van het informatiesysteem en het doen van oplossingsgerichte aanbevelingen ten aanzien van IC-aspecten;
- het beoordelen van de testresultaten.

In de praktijk ligt aan het eind van deze fase veel nadruk op het operationeel worden van het systeem. Ondanks alle goede voornemens krijgen sommige voorgestelde IC-maatregelen onder tijdsdruk alsnog een lage prioriteit. Vaak lukt het helaas niet in de eerste versie van het systeem alle benodigde IC-maatregelen ingebouwd te krijgen. Als het niet anders mogelijk is zal in deze situatie in overleg met het management en de ontwikkelaars ernaar moeten worden gestreefd in ieder geval een minimale set van maatregelen te realiseren. In het vervolg van de implementatie moet vervolgens worden bewaakt dat, zo snel mogelijk nadat de eerste versie van het informatiesysteem operationeel is geworden, alsnog de noodzakelijke IC-maatregelen worden ingebouwd. De gebruikers moeten van deze situatie op de hoogte worden gesteld zodat in de tussentijd aanvullende gebruikerscontroles kunnen worden uitgevoerd.

*Ondanks alle goede voornemens krijgen sommige voorgestelde IC-maatregelen onder tijdsdruk alsnog een lage prioriteit.*

**Fase Invoering:**
**Opzetten controlebeleid**

Tijdens de ontwikkeling van het informatiesysteem is conform de aanpak een risico-analyse uitgevoerd om te bepalen welk stelsel van IC-maatregelen moest worden geïmplementeerd. Voortdurend zal door of namens het management van de organisatie moeten worden geëvalueerd of nog steeds terecht op de automatisering wordt gesteund. Het opgestelde Raamwerk IC-eisen moet daartoe voor het operationele systeem worden vertaald in een controlebeleid met bijbehorende controle-activiteiten. Dit systeem van toezicht op de effectiviteit van de maatregelen is onderdeel van het management control system (het beheersingssysteem).

## TOT SLOT

In dit artikel is ingegaan op de gevolgen van de voortschrijdende automatisering voor de wijze waarop de betrouwbaarheid van de informatievoorziening wordt gewaarborgd. In de praktijk kan worden geconstateerd dat het management in toenemende mate op computer controls gaat steunen maar zich niet altijd bewust is van de consequenties. Interne controle kan in deze situatie

*Drs. J.J. van Beek RE RA*
*Is sedert 1986 in dienst bij KPMG Klynveld, gedurende de eerste vier jaar in de algemene controlepraktijk, daarna als EDP-auditor. Hij heeft ruime opdrachtervaring opgedaan bij het participeren in grootschalige systeemontwikkelingsprojecten, onder meer bij het beoordelen van de controleerbaarheid.*

slechts effectief zijn, indien de getroffen maatregelen een samenhangend geheel vormen. Om hoge kosten ten gevolge van aanpassingen te voorkomen moet dit al tijdens de systeemontwikkeling worden onderkend. Door het verschuiven van gebruikerscontroles naar computercontroles wordt ook het belang van de accountant groter om tijdig aandacht te besteden aan de benodigde beheersingsmaatregelen van het systeem dat door de systeemontwikkelorganisatie wordt ontwikkeld. Als gevolg van onder meer het ontbreken van een gestructureerde aanpak, gebrek aan kennis en tijdsdruk krijgt het realiseren van IC-maatregelen tijdens systeemontwikkeling nog niet de gewenste aandacht.

De in dit artikel beschreven aanpak geeft de accountant of EDP-auditor een handvat om zijn participatie binnen een SO-project, gericht op het realiseren van een effectief stelsel van IC-maatregelen, te structureren en daardoor effectiever en efficiënter te laten verlopen. Op langere termijn zou een dergelijke aanpak onderdeel kunnen gaan uitmaken van de gevolgde systeemontwikkelmethodiek, zodat het bouwen van betrouwbare informatiesystemen in de toekomst minder problemen hoeft op te leveren.

## LITERATUUR

[Beek92] M.J. van Beek, *Realisatie van interne controle binnen informatiesystemen; een procesmatige benadering*, afstudeerreferaat EDP-auditing opleiding Erasmus Universiteit Rotterdam, december 1992.

[Bril83] A.E. Brill, *Building controls into structured systems*, Yourdan Press, New York 1983.

[Hart88] Prof. W. Hartman, *Bevordering betrouwbaarheid informatiesystemen*, Kluwer Bedrijfswetenschappen, Deventer 1988.

[Jans91] Mw. D. Jansen Heijtmajer, *Beveiligingsbeleid geautomatiseerde informatievoorziening*, Compact 1991/3.

[Kock91] Prof. H.C. Kocks, *Inzicht in samenhang*, collegedictaat EDP-auditing opleiding Erasmus Universiteit Rotterdam, 1991.

[Koed86] A.H.C. Koedijk, *Beoordeling betrouwbaarheid van een (geautomatiseerd) informatiesysteem: de CASA-methode*, in: 24 over EDP auditing, KPMG Klynveld EDP Audit/Samsom BedrijfsInformatie, Alphen aan den Rijn 1986.

# Audit automation

Drs. L.H. Dam RA en drs. P. Veltman RE RA

**Het cijfermateriaal waarop de jaarrekening is gebaseerd, komt heden ten dage overwegend tot stand via geautomatiseerde processen van gegevensverwerking.**
**Alle reden voor de accountant om ook de controle zoveel mogelijk geautomatiseerd uit te voeren. Talloze hulpmiddelen zijn er beschikbaar, zowel voor onderzoek van de gegevens, als voor onderzoek van de gegevensverwerkende processen en de geautomatiseerde beheersingsprocessen.**
**De gebruiksmogelijkheden van dit scala van hulpmiddelen worden in dit artikel behandeld en aan de hand van een praktisch voorbeeld toegelicht.**

## INLEIDING

Door de technologische ontwikkelingen van de afgelopen tien jaar zijn de gebruiksmogelijkheden van automatisering binnen de accountantscontrole toegenomen. Er zijn meer hulpmiddelen beschikbaar, die bovendien op een simpele wijze zijn te bedienen. Voornaamste gebruiksmotieven zijn het verhogen van de kwaliteit van het controleprodukt (controle met daaraan gerelateerde adviezen) en het verhogen van de efficiëntie van het controleproces. In dit artikel worden moderne technieken besproken die de accountant bij zijn werkzaamheden kunnen ondersteunen.

Het gebruik van audit automation ten behoeve van de jaarrekeningcontrole staat in dit artikel centraal. Wel moet worden bedacht dat veel van de te bespreken technieken niet alleen ten dienste staan aan de interne of externe accountant, maar tevens aan de ondernemingsleiding.

Onder audit automation wordt in dit artikel verstaan *'het geheel van geautomatiseerde hulpmiddelen die de accountant kan aanwenden voor het verrichten van zijn werkzaamheden in brede en enge zin'.*

De werkzaamheden van de accountant in brede zin betreffen alle werkzaamheden. Ook het uitoefenen van het ondernemerschap kan hieronder worden verstaan. In enge zin worden de eigenlijke controlewerkzaamheden bedoeld. Met betrekking tot deze laatste werkzaamheden worden de geautomatiseerde hulpmiddelen ook wel aangeduid als CAAT's, Computer Assisted Audit Techniques. In dit artikel zal deze term worden gehanteerd.

Dit artikel geeft een overzicht van de huidige mogelijkheden tot het gebruik van audit automation. Zowel algemene toepassingen te gebruiken binnen een accountantskantoor worden behandeld, als toepassingen voor de feitelijke accountantscontrole. Tot slot wordt ingegaan op organisatorische en vaktechnische aspecten die in acht moeten worden genomen bij het toepassen van geautomatiseerde hulpmiddelen en op enkele toekomstverwachtingen.

# AUDIT AUTOMATION VAN DE ACCOUNTANTSCONTROLE

Veel werkzaamheden die in het kader van de accountantscontrole moeten worden verricht, kunnen worden ondersteund met geautomatiseerde hulpmiddelen. Het gebruik van deze toepassingen beperkt zich niet tot de accountant. Als onderdeel van de besturing van de organisatie kunnen (geautomatiseerde) audit-technieken intern worden aangewend, bijvoorbeeld ter ondersteuning bij het maken van cijferbeoordelingen, waaronder trendanalyses en exceptierapportages. Deze hulpmiddelen ter controle van de bedrijfsprocessen en de ondersteunende processen kunnen worden aangeduid met de term management-software en passen binnen de management control-benadering zoals geschetst in het artikel van Fijneman elders in deze Compact. De accountant kan genoemd intern gebruik stimuleren waardoor onder andere geen eigen investeringen nodig zijn, alsmede eigen werkzaamheden worden beperkt.

Daarnaast is onderscheid te maken tussen het gebruik van geautomatiseerde hulpmiddelen door de externe versus de interne accountant. De laatste groep zal bepaalde hulpmiddelen eerder inzetten, met name indien deze moeten worden geactiveerd tijdens het operationeel zijn - vanwege technische redenen - van het systeem van de gecontroleerde huishouding. Een voorbeeld hiervan is de controle van bestaan en werking van functiescheidingen binnen de geautomatiseerde omgeving. Deze geschiedt veelal met hulpmiddelen die een onderdeel zijn van het besturingssysteem in de produktieomgeving.

*Toepassingen om openbare databanken te benaderen kunnen worden gebruikt ter verkrijging van informatie over nieuwe of potentieel nieuwe cliënten.*

De te gebruiken geautomatiseerde hulpmiddelen zullen zijn aangepast aan de typische behoeften per activiteit. Veelgebruikte toepassingen zijn:
- tekstverwerkings- en spreadsheet-pakketten;
- pakketten ter ondersteuning van de planning;
- formulieren en vragenlijsten voor structurering van de werkzaamheden, die na invulling automatisch worden vastgelegd en opgeslagen;
- standaard audit-pakketten voor cijferbeoordeling, steekproeven en leadschedules (de indeling van de te controleren verantwoording naar rubrieken van de jaarrekening waarop het controledossier aansluit);
- AO-tekenpakketten voor het vastleggen van de administratieve organisatie.

**Fases in het controleproces**

Het controleproces bestaat uit een aantal fases, waarin per fase gebruik kan worden gemaakt van geautomatiseerde toepassingen. De volgende fases worden onderscheiden en worden, met uitzondering van de uitvoerende fase, navolgend kort toegelicht:
- werkzaamheden voor aanvaarding van de opdracht;
- planning;
- opstelling controleprogramma;
- uitvoering;
- rapportage.

De uitvoerende fase wordt in afzonderlijke paragrafen meer uitvoerig behandeld.

*Werkzaamheden voor aanvaarding van de opdracht*
Deze fase bestaat uit activiteiten voor acceptatie van de opdracht en bestendiging van de relatie, alsmede voor het vaststellen van de opdrachtvoorwaarden. In deze fase bestaan overeenkomsten en verschillen tussen interne-accountantsdiensten en externe accountants. De interne accountant heeft eveneens een goede opdrachtformulering nodig, maar zal minder zorg besteden aan relatiebeheer.

Er wordt met name gebruik gemaakt van tekstverwerkingspakketten en desktop publishing-toepassingen. Toepassingen om openbare databanken te benaderen kunnen worden gebruikt ter verkrijging van informatie over nieuwe of potentieel nieuwe cliënten. Voorts zullen toepassingen voor het relatiebeheer worden ingezet.

*Planning*
De planningsactiviteiten zijn met name gericht op het verkrijgen van inzicht in het bedrijfsgebeuren en het scheppen van een kader voor de vervulling van de opdracht. Te noemen activiteiten zijn initiële cijferbeoordeling, vaststelling van de controletolerantie en de kritische controledoelstellingen, alsmede evaluatie van de controle-omgeving inclusief de maatregelen van interne controle.

De activiteiten in deze fase vereisen diverse beslissingen. Een voorbeeld hiervan is de keuze tussen een systeemgerichte of een gegevensgerichte controle-aanpak. De te gebruiken geautomatiseerde hulpmiddelen moeten in staat zijn tot het vastleggen van de gegevens en het geven van de overzichten die nodig zijn om keuzen te maken en/of beslissingen te nemen. Mogelijke toepassingen zijn decision support-systemen en expertsystemen. Deze systemen worden als volgt gedefinieerd:

- Een Decision Support-Systeem (DSS) is een informatiesysteem dat helpt bij het oplossen van problemen in redelijk gestructureerde situaties. Het systeem neemt geen beslissingen. Door middel van het analyseren van oplossingen, of via 'trial and error' wordt het beslissingsproces ondersteund. In feite is een spreadsheet-pakket een voorbeeld van een eenvoudig DSS.

- Een expertsysteem is een computertoepassing

die op basis van vastgelegde kennis en redeneerregels helpt bij het uitvoeren van slecht-gestructureerde taken. Dergelijke situaties vereisen normaal gesproken ervaring en specifieke deskundigheid (expertise). Door het gebruik van expertsystemen kunnen ook niet-deskundigen de bedoelde taken uitvoeren.

Tegenwoordig wordt veel gebruik gemaakt van het risico-analysemodel, waarmee het inherente risico en het interne-controlerisico worden ingeschat. Er zijn toepassingen beschikbaar die helpen bij het vastleggen van de risico's, alsmede het analyseren van de gevolgen. Voor het verrichten van cijferbeoordelingen zijn diverse pakketten geschikt. De meest gebruikte toepassing voor cijferbeoordeling is het spreadsheet-pakket.

Een belangrijk onderdeel van de planning is het toewijzen van de 'human resources' waarmee de werkzaamheden worden verricht. De medewerkers worden verdeeld over alle opdrachten die moeten worden vervuld. Voor de urenverantwoording kan dan tevens gebruik worden gemaakt van (gekoppelde) geautomatiseerde hulpmiddelen. Daarnaast moeten andere 'resources', zoals computers, printers en dergelijke, worden toegewezen.

*Opstelling controleprogramma*
Als basis voor het bepalen van de te verrichten detailwerkzaamheden wordt gebruik gemaakt van het risico-analysemodel. Voor het samenstellen en vastleggen van controleprogramma's zijn diverse toepassingen beschikbaar. Hierbij kan worden gedacht aan expertsystemen, waarmee op basis van diverse criteria (zoals ervaring van de medewerkers) werkprogramma's kunnen worden samengesteld. De toepassingen die daadwerkelijk in de praktijk worden gebruikt, zijn veelal gebaseerd op tekstverwerkingspakketten, waarbij de indeling is voorgeschreven. Door branchegerichte werkprogramma's te ontwikkelen kunnen de individuele programma's sneller tot stand worden gebracht.

*Rapportage*
Een belangrijk resultaat van de accountantscontrole is de af te geven verklaring bij de jaarrekening. Het is ook mogelijk dat de jaarrekening door de accountant wordt opgesteld. Overige rapportage betreft adviesbrieven, rapporten bij bijzondere onderzoeken en correspondentie.

Uiteraard moeten hierbij de bepalingen van de GBR in acht worden genomen. Er moeten duidelijke richtlijnen worden opgesteld en nageleefd bij het voeren van correspondentie. Hierbij zal gebruik worden gemaakt van voorgeschreven tekstlay-out, ondersteund door tekstverwerkingspakketten. Ook het gebruik van geautomatiseerde 'checklists' zal de kwaliteit van de rapportage ten goede komen. Ter voorkoming van ongeautoriseerd gebruik kan een toegangsbeveiligingssysteem zijn geïnstalleerd. Dit systeem dient mede de toegang tot (vertrouwelijke) gegevens van en over cliënten te beveiligen.

Voor het samenstellen van de jaarrekening zullen veelal consolidatietoepassingen worden gebruikt. Voorts wordt gebruik gemaakt van pakketten voor grafische vormgeving (desktop publishing), scanners, plaatjes, etc. Tevens kan worden gedacht aan toepassingen voor de opslag van dossiers en rapporten. Dit laatste wordt behandeld als onderdeel van kantoorautomatisering.

*Uiteraard moeten bij de rapportage de bepalingen van de GBR in acht worden genomen.*

**Kantoorautomatisering**

In deze paragraaf zullen enkele toepassingen worden besproken die weliswaar een verband hebben met accountantswerkzaamheden, maar toch een meer algemeen karakter dragen. De toepassingen en/of technieken kunnen ook in andere organisaties worden gebruikt. De koppeling met de specifieke bedrijfsprocessen moet wel worden gerealiseerd. Te denken valt aan een verantwoordingssysteem voor uren en kosten gekoppeld aan een factureringssysteem. Een ander voorbeeld betreft het gebruik van laserprinters en scanners, waardoor de grafische kwaliteiten van rapporten zijn verbeterd. Dit komt mede ten goede aan de presentatie van de communicatie (correspondentie en rapportering) met de cliënt.

*Elektronisch dossier*
Dossiervorming is een belangrijk onderdeel binnen de accountantscontrole. Dit geldt ook voor veel andere beroepen, zoals advocaten, notarissen en belastingadviseurs. Met name de opslag van dossiers is een algemeen probleem. Veel organisaties zoeken oplossingen voor de opslag van de administratie. Vandaar dat dit onderwerp als kantoorautomatisering wordt behandeld.
Het toepassen van een geheel elektronisch dossier is tot op heden nog niet gerealiseerd. Dossiers zullen voor een deel met behulp van computers worden vervaardigd. Er zijn diverse redenen waarom elektronische dossiervorming tot op heden niet succesvol is geweest. De volgende zijn te noemen:

- Papier is overzichtelijk, in tegenstelling tot (standaard) beeldschermen. Daarnaast is de snelheid van bladeren in papieren dossiers veel groter dan in elektronische documenten.

- Een controleploeg bestaat uit meerdere mensen, die allen gezamenlijk aan dezelfde dossiers moeten werken. Voor een geautomatiseerd dossier is het derhalve noodzakelijk op een netwerk te werken. Technisch is dit geen bezwaar, maar het leidt wel tot hoge investeringen in apparatuur en programmatuur.

– Verscheidene toepassingen worden gebruikt bij de uitvoering van de controle. Om een geautomatiseerd dossier volledig te benutten, betekent dit een integratie van alle pakketten tot een nieuwe, allesomvattende toepassing. Hiermee zouden vele voordelen worden behaald op het gebied van documentatie. Bijvoorbeeld de wijze waarop de steekproefomvang wordt vastgesteld, wordt dan automatisch in het dossier vastgelegd.
Vanwege de brede functionaliteit en het beslag op het intern geheugen van microcomputers lijkt een dergelijk pakket voorlopig niet haalbaar.

Hoewel elektronische dossiervorming tijdens de uitvoering van de controle niet praktisch blijkt, is het goed mogelijk afgeronde dossiers in elektronische vorm te archiveren. Technieken die hiervoor kunnen worden gebruikt, zijn opslag op microfiches en CD-rom. Hierbij kan ruimtebesparing worden gerealiseerd. Daarnaast kan een mechanisme worden toegepast waarmee snel en eenvoudig zoekacties worden uitgevoerd. In dit kader past de term multimedia.

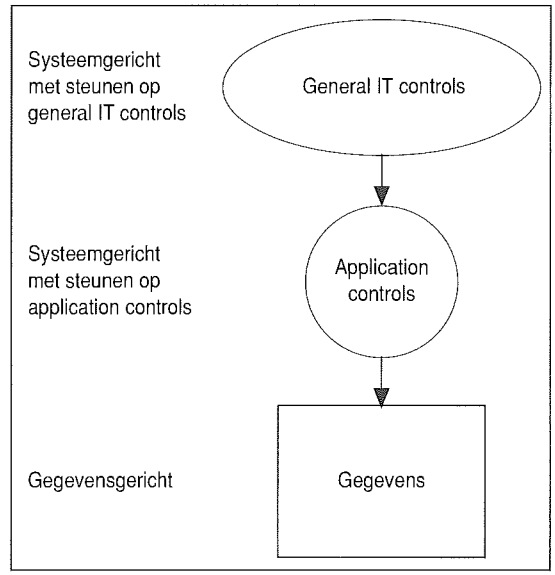
*Multimedia*
Multimedia is een onderwerp waaraan momenteel veel aandacht wordt besteed. Toch is het principe dat hieraan ten grondslag ligt al jaren bekend. Door voortschrijdende technische vernieuwingen worden diverse toepassingen realiseerbaar. Multimediasystemen kunnen worden gedefinieerd als systemen die verschillende informatievormen geïntegreerd kunnen representeren en verwerken. De koppeling van CD-rom aan microsystemen is hier een voorbeeld van. Een ander voorbeeld is videoconferencing (beeld en geluid als informatievorm).

De elektronische dossieropslag en dossiervorming zijn mogelijke toepassingen binnen accountantskantoren. Andere voorbeelden zijn simulatie van bedrijfsprocessen, gebruik van gekoppelde bibliotheken en koppeling met andere gegevensbronnen, zoals koersinformatie, registraties bij de Kamer van Koophandel, registraties bij het kadaster, etc.

*Netwerken*
Netwerken kunnen worden gebruikt voor het zenden en ontvangen van documenten en berichten. Hierbij kan onderscheid worden gemaakt in locatiegebonden netwerken (LAN's, Local Area Networks) en netwerken waarvoor in feite geen (internationale) grenzen bestaan (WAN's, Wide Area Networks). Met name lokale netwerken worden veel gebruikt. De medewerkers zijn dan met hun eigen microcomputer aangesloten op het netwerk. Hiermee kunnen diverse zaken worden gerealiseerd zoals tijdregistratie, doorgeven van de planning, melding van binnengekomen telefoontjes, verzenden van boodschappen, maken van backups, etc.

## UITVOERING VAN DE CONTROLE

De accountant heeft de keuze uit meerdere strategieën om een jaarrekeningcontrole uit te voeren. Onderscheid kan worden gemaakt tussen een gegevensgerichte controle-aanpak, een systeemgerichte aanpak met steunen op application controls en een systeemgerichte aanpak met steunen op general IT controls. Dit is schematisch weergegeven in figuur 1. Voor een verdere uitleg wordt verwezen naar het artikel van Fijneman in deze Compact.




*Figuur 1. Onderscheid tussen systeemgerichte en gegevensgerichte controle-aanpak.*

CAAT's bestaan er ter ondersteuning van elk van de drie genoemde controlebenaderingen. Hierbij is sprake van een 'multi-purpose'-karakter. Als bijvoorbeeld met behulp van een gegevensgericht controlemiddel een oordeel is verkregen over de betrouwbaarheid van de gegevens, kan hiervan een uitspraak worden afgeleid over de betrouwbaarheid van de application controls (het proces ter verwerking van de gegevens). Tevens kan een uitspraak worden afgeleid over de betrouwbaarheid van de general IT controls (het proces ter waarborging van de betrouwbaarheid van het gegevensverwerkingsproces). Met name bij de laatste gevolgtrekking moet voorzichtigheid in acht worden genomen; in feite kan slechts de uitspraak worden gedaan dat eventuele leemten in de general IT controls niet hebben geleid tot (materiële) fouten in de gegevens.

Op overeenkomstige wijze kan - met de nodige voorzichtigheid - uit een oordeel over de goede werking van de application controls een uitspraak worden afgeleid over de betrouwbaarheid van de gegevens en de general IT controls. Uit een oordeel over de goede werking van de general IT controls kan een uitspraak worden afgeleid over de betrouwbaarheid van application controls en gegevens.

Voor een toelichting op het begrip betrouwbaarheid wordt verwezen naar het artikel van Fijneman.

Met betrekking tot gegevensgerichte CAAT's kan nader onderscheid worden gemaakt tussen CAAT's die binnen de gegevensverwerkende processen een relatie leggen tussen verschillende gegevens of gegevensverzamelingen enerzijds, en CAAT's die ondersteuning bieden bij het controleren van gegevens met bewijsstukken en andere elementen buiten de gegevensverwerkende processen anderzijds. In NIVRA-geschrift 13 worden eerstgenoemde activiteiten, voor het uitvoeren van verbandscontroles en overige cijferanalyses, controlemiddelen met een toetsingskarakter genoemd. Laatstge-noemde activiteiten, voor detailcontroles met bewijsstukken en overige afstemmingen met de werkelijkheid, worden controlemiddelen met een verificatiekarakter genoemd.

CAAT's voor de controle van application controls kunnen zijn gericht op de handmatige component hierbinnen of op de geautomatiseerde component. Controle van de gebruikershandelingen kan bijvoorbeeld plaatsvinden door selectie van posten die een handmatig vervolgtraject dienen te krijgen. Controle van de geautomatiseerde processen kan worden uitgevoerd door middel van (partiële) simulatie, of door gebruik te maken van hulpmiddelen die ook worden gehanteerd bij systeemontwikkeling voor het opsporen van fouten in de programmatuur ('debuggers').

CAAT's voor de controle van de general IT controls maken veelal onderdeel hiervan uit; het gaat dan bijvoorbeeld om toepassingen waarmee de werking van de logische toegangsbeveiliging (een belangrijke maatregel van general IT control) kan worden gecontroleerd.

Het gebruik van CAAT's voor bestandsonderzoek, beoordeling van application controls en beoordeling van general IT controls wordt in afzonderlijke paragrafen meer uitvoerig behandeld.

### Techniek

De accountant kan CAAT's op diverse locaties toepassen. Hulpmiddelen die worden gebruikt voor het onderzoeken van de toepassingsprogrammatuur en de general IT controls lenen zich voor gebruik op de apparatuur van de te onderzoeken organisatie. Voor andere hulpmiddelen, spreadheetpakketten bijvoorbeeld, ligt het gebruik van eigen microcomputers voor de hand. Daarnaast kan een computer van het eigen kantoor worden gebruikt voor het lezen van grote bestanden en het maken van selecties, eventueel voor verder gebruik op de microcomputer. Voor deze laatste mogelijkheid kunnen ook faciliteiten van derden worden gebruikt, zoals een servicebureau, met name indien het eigen kantoor over onvoldoende capaciteit beschikt.

Daarnaast kan de accountant kiezen tussen op verschillende wijzen tot stand gekomen CAAT's. De volgende mogelijkheden zijn te noemen: standaard-software, zelf ontwikkelde applicaties of applicaties van de te onderzoeken organisatie (al dan niet door haar zelf ontwikkeld). In een latere paragraaf zal nader worden ingegaan op de voor- en nadelen van de verschillende technieken.

*Met de nodige voorzichtigheid kan uit een oordeel over de goede werking van de application controls een uitspraak worden afgeleid over de betrouwbaarheid van de gegevens en de general IT controls.*

### Onderzoek naar AO/IC

Een onderdeel van de uitvoerende fase is het beoordelen van de administratieve organisatie. Voor het vastleggen van de interne organisatie kan gebruik worden gemaakt van tekenpakketten, toepassingen om interviews te registreren, geautomatiseerde standaardformulieren, vragenlijsten, etc. Dit onderzoek richt zich met name op de opzet van getroffen interne-controlemaatregelen. Omdat de te bespreken toepassingen en technieken met name betrekking hebben op toetsing van bestaan en/of werking, wordt het AO/IC-onderzoek verondersteld te zijn uitgevoerd, doch niet nader behandeld.

### Voorraad als voorbeeld

Met behulp van een vereenvoudigd voorbeeld wordt het gebruik van CAAT's in de navolgende paragrafen toegelicht. Het voorbeeld betreft de controle van de handelsvoorraad en de daaraan gerelateerde onderdelen van de inkopen/crediteuren- en verkopen/debiteuren-cycli bij een handelsonderneming. De onderneming maakt gebruik van een minicomputer met UNIX als besturingssysteem. De transactieverwerking vindt plaats met behulp van een standaardpakket met de modules: inkoop, verkoop, debiteuren, crediteuren en grootboek. De modules zijn gekoppeld; de bestanden kunnen met een opvraagtaal worden benaderd.

Ter wille van de eenvoud worden slechts de volgende controledoelstellingen onderkend:
- juistheid: alle verantwoorde voorraad is accuraat geregistreerd, aanwezig en in bezit van de gecontroleerde;
- volledigheid: de gehele voorraad is in de verantwoording opgenomen;
- waardering: de voorraad wordt op een consistente wijze gewaardeerd in overeenstemming met geaccepteerde waarderingsgrondslagen, waarbij alle incourante en onbruikbare eenheden op een consistente wijze worden gewaardeerd tegen een reële opbrengstwaarde.

# CAAT'S VOOR GEGEVENSGERICHT ONDERZOEK

CAAT's worden sedert jaren toegepast voor het onderzoeken van gegevensverzamelingen. De toepassingen werden in de begintijd gebruikt op mainframes. Naarmate de technische ontwikkelingen zorgden voor kleine en efficiënte computers werden deze micro's meer en meer ingezet. Bij het uitvoeren van bestandsonderzoek heeft de accountant steeds minder behoefte aan hulp van deskundigen op het gebied van bestandsorganisatie en programmering.

*Bij het uitvoeren van bestandsonderzoek heeft de accountant steeds minder behoefte aan hulp van deskundigen op het gebied van bestandsorganisatie en programmering.*

Met hulpmiddelen voor gegevensonderzoek kunnen diverse bewerkingen worden verricht, nadat de gegevens zijn verwerkt. Relevante bewerkingen zijn: selecteren, sorteren, rekenen/tellen, vergelijken, rubriceren/classificeren, en samenvoegen/salderen. Vertaling van deze elementaire bewerkingen geeft onder meer de volgende controle-activiteiten:

- berekenen van steekproeven en het maken van selecties uit de onderliggende populatie;
- aanmaken van saldobiljetten;
- natellen van de totalen van (financiële) overzichten;
- controleren van het rekeningschema;
- controleren van doorlopende nummering;
- vervaardigen van overzichten, zoals voor ouderdomsanalyse;
- uitvoeren van cijferbeoordelingen.

**Techniek**

Bovengenoemde activiteiten kunnen met diverse soorten toepassingsprogrammatuur worden uitgevoerd. Enkele veel voorkomende worden kort besproken.

*Standaardprogrammatuur*
Met standaardpakketten worden CAAT's bedoeld die op de 'markt' te koop zijn en geschikt voor de eerder genoemde controle-activiteiten. De pakketten zijn veelal eenvoudig te bedienen, waardoor bewerkingen zelfstandig kunnen worden verricht, zonder hulp van automatiseringsdeskundigen. Een belangrijke reden om standaardpakketten te gebruiken is de betrouwbaarheid, waarvoor de verspreiding van het pakket een belangrijke aanwijzing is. Over het algemeen zijn de pakketten geschikt voor computers van verschillend fabrikaat. Sommige pakketten bieden de mogelijkheid routines toe te voegen, waarmee de uit te voeren bewerkingen kunnen worden aangepast aan de specifiek te controleren omstandigheden. Deze uitbreidingen bestaan uit toevoeging van procedures geschreven in een programmeertaal, veelal in te brengen door automatiseringsdeskundigen.

*Eigen programmatuur*
Er zijn accountants die gebruik maken van zelf ontwikkelde programmatuur. De motieven om dergelijke toepassingen te gebruiken zijn divers. Zo ondersteunt bijvoorbeeld het standaardpakket niet alle computermerken. Of, bij lage performance van een standaardpakket, kan de transactieverwerking van het te onderzoeken systeem worden belemmerd.

Een moderne toepassing van applicatie-ontwikkeling betreft het gebruik van CASE-tools (Computer Aided Software Engineering). Vanuit een hogere abstractie, bijvoorbeeld een AO-beschrijving met behulp van flow charts, verzorgt een programmagenerator de verlangde toepassing. Er is veel minder automatiseringskennis nodig om de programmatuur te ontwikkelen, waardoor (dure) automatiseringsspecialisten minder noodzakelijk zijn geworden.

*Programmatuur van de te onderzoeken organisatie*
Het is mogelijk gebruik te maken van geautomatiseerde hulpmiddelen (en kennis) van de organisatie die wordt gecontroleerd. Zo kan in een debiteurenpakket een routine zijn opgenomen om saldobevestigingen te vervaardigen. De uitkomsten van de routine moet de accountant beoordelen, waartoe hij de keuze heeft tussen enerzijds toetsing van de wijze waarop de routines tot stand zijn gekomen en anderzijds toetsing van de uitkomst aan de hand van reeds gecontroleerde gegevens.

*Retrieval languages*
Door de ontwikkeling en verspreiding van opvraagtalen, waarmee databases flexibel kunnen worden benaderd, zullen bovengenoemde routines nog zelden voorkomen in toepassingsprogrammatuur. Met behulp van deze gebruikersvriendelijke hulpmiddelen (menugestuurd met online-helpfuncties) kunnen onder meer selecties van gegevens worden gemaakt en rapporten opgesteld. De accountant kan gebruik maken van de kennis en ervaring die binnen de te controleren organisatie aanwezig is omtrent het gebruik van deze talen, mits de betrouwbaarheid van de uitkomsten is gegarandeerd.

*Spreadsheets*
Spreadsheets zijn standaardpakketten met een grote verspreiding. De spreadsheet wordt niet gebruikt om bestanden te lezen en te converteren, maar om reeds geconverteerde bestanden te gebruiken voor verdere bewerking. Met name door de grote flexibiliteit in het manipuleren van gegevens naar eigen inzicht is dit hulpmiddel populair.

De accountant zal de cijferopstellingen veelal zelf maken, waarbij gebruik kan worden gemaakt van macro's (programmeerroutines). Deze macro's zullen niet altijd onderhevig zijn aan kwaliteitsprocedures, waaronder testroutines. Vóór wordt overgegaan tot interpretatie van de uitkomsten zal hij de macro's allereerst kritisch moeten toetsen.

**Het voorbeeld**

Bij de gegevensgerichte controle van de handelsvoorraad uit het voorbeeld dat in de voorgaande paragraaf werd geïntroduceerd, kunnen CAAT's op de volgende manieren ondersteuning bieden:

Gericht op de juistheid en volledigheid:
- het controleren van de verschillende aansluitingen in de goederenbeweging per artikel in aantallen en/of (kostprijs)waarde.

Gericht op de juistheid:
- het berekenen en genereren van steekproeven voor de voorraadopname (inclusief locatiecodes en dergelijke);
- het narekenen van totaaltellingen en de waarde per artikel, bestaande uit prijs maal aantal;
- het genereren van een overzicht gesorteerd op artikelwaarde voor een test op de juistheid en aanvaardbaarheid van de gehanteerde prijzen. Ter vereenvoudiging van verdere werkzaamheden kan dit overzicht per artikel worden aangevuld met de laatste inkoopfactuurnummers en de betaalde inkoopprijs.

Gericht op de volledigheid:
- het gedurende een periode na afloop van het boekjaar selecteren van betalingen voor leveringen die behoren tot het oude boekjaar;
- het controleren van de doorlopende nummering van transacties.

Waardering:
- het genereren van ouderdomsoverzichten en de omloopsnelheid per artikel, met rapportage van oude artikelen en/of artikelen met een lage omloopsnelheid;
- afloopcontrole op de artikelen per balansdatum door automatische vergelijking van de verkochte artikelen in het verkoopboek, in het nieuwe boekjaar.

## CAAT'S VOOR TOETSING VAN APPLICATION CONTROLS

CAAT's voor de toetsing van application controls zijn niet direct gericht op de vaststelling van de betrouwbaarheid van gegevens, maar op de vaststelling van de betrouwbare werking van de interne controle. Hierbij gaat het om zowel handmatige interne controle als geprogrammeerde interne controle in toepassingsprogrammatuur.

**Techniek**

Er zijn diverse technieken voorhanden die kunnen worden gebruikt voor het onderzoeken van application controls. Onderstaand wordt ingegaan op enkele van de meest gebruikte technieken.

*Testgevallen*
De wijze waarop de te onderzoeken applicatie de transacties verwerkt, wordt getoetst door proeftransacties te vervaardigen. De uitkomsten moeten vooraf worden bepaald en worden vergeleken met de resultaten na verwerking door de applicatie. Het toepassen van testgevallen is erg arbeidsintensief (met name indien integraal wordt getest). Daarnaast wordt slechts een momentopname verkregen.

*Simulatie/Parallelverwerking*
Met behulp van de techniek parallelverwerking wordt de actuele verwerking gesimuleerd met andere programmatuur, teneinde te verifiëren of de uitkomsten gelijk zijn. Hierbij is onderscheid te maken tussen twee situaties:
- er dient een uitspraak te worden gedaan over de gegevens;
- er dient een uitspraak te worden gedaan over de applicatie.

In de eerste situatie volstaan uitkomsten die bij benadering overeenkomen met de te controleren gegevens. Een voorbeeld hiervan is het met een eigen toepassing narekenen van de verantwoorde interest op banktegoeden. De uitkomsten van deze simulatie mogen niet materieel afwijken van de verantwoording. Een dergelijke toepassing hoort in feite in de vorige paragraaf thuis.

*Een voorbeeld van simulatie is het met een eigen toepassing narekenen van de verantwoorde interest op banktegoeden.*

In de tweede situatie dienen de resultaten exact overeen te komen met de uitkomsten van de applicatie. Ieder verschil betekent dat de geteste applicatie niet deugt (tenzij de simulator onbetrouwbaar is).

Een nadeel van deze techniek is weer dat slechts een momentopname wordt verkregen. Voorts moet de simulator worden onderhouden en aangepast aan alle modificaties die worden aangebracht op de te testen programmatuur.

*Tagging*
Met tagging wordt een selectie van te verwerken actuele transacties gemaakt, waaraan een merkteken wordt toegevoegd, om het verwerkingsproces

van de applicatie te beoordelen. Als gevolg van dit merkteken wordt een bepaalde actie in gang gezet door de te onderzoeken programmatuur. Er wordt bijvoorbeeld een bepaald rapport afgedrukt met informatie over vooraf gespecificeerde tussenstadia van het verwerkingsproces.

*Tracing*
Met tracing wordt het detail van alle genomen stappen (de 'trail') tijdens de geautomatiseerde transactieverwerking zichtbaar gemaakt. De toepassing die tracing uitvoert schrijft van geselecteerde transacties informatie over de trail in een separaat bestand. Tracers zijn verkrijgbaar als standaardpakket.

*Flow charting*
Met flow charting worden logische schema's gegenereerd uit de broncode van programmatuur, om te beoordelen of de programmatuur voldoet aan gestelde functionele eisen, alsmede een logische structuur heeft. De broncode zal veelal van een lager abstractieniveau zijn. Indien de broncode slecht is gestructureerd, zullen de gegenereerde logische schema's minder bruikbaar zijn voor het analyseren van de programmatuur, wat overigens niet impliceert dat deze dan ook slecht functioneert. Flow charting geeft wederom slechts een momentopname, terwijl deze techniek zeer arbeidsintensief is.
Een techniek die hierop lijkt is het toepassen van software analysers of pre-compilers. Deze programma's controleren broncodes van toepassingen op het voorkomen van ongewenste programmaconstructies of commando's.

*Als de gegevens worden weggeschreven in een speciaal bestand moeten extra maatregelen worden getroffen om dit bestand te beschermen tegen ongeautoriseerde verwijdering en modificatie.*

*Beoordeling van source codes*
Het beoordelen van source codes wordt in de praktijk zelden uitgevoerd. Er zijn evenwel pakketten op de markt die de werkzaamheden kunnen vergemakkelijken. Door toenemend gebruik van standaardpakketten is de noodzaak tot source code-beoordeling afgenomen. Bij gebruik van CASE-TOOLS voor het ontwikkelen van applicaties wordt niet de broncode beoordeeld, maar de gemaakte stroomschema's om de applicatie te bouwen.

*SCARF/EAM*
SCARF staat voor System Control Audit Review File en EAM staat voor Embedded Audit Modules.
De te controleren applicatie moet geschikt worden gemaakt om SCARF toe te passen. Op grond van aangegeven selectiecriteria kunnen transacties worden uitgekozen die een bijzonder vervolg dienen te krijgen. De transacties kunnen uitzonderingen betreffen en mogelijk duiden op foutieve of ongeautoriseerde transacties. Een voorbeeld hiervan is het selecteren van betaalopdrachten die zich boven een gestelde limiet bevinden. Binnen banken kan SCARF worden toegepast om transacties te selecteren op inactieve rekeningen.

SCARF kan tevens worden toegepast als onderdeel van het stelsel van interne-controlemaatregelen. Door het dagelijks selecteren en rapporteren van kritische mutaties kan de techniek worden gebruikt om de transactieverwerking voortdurend te bewaken.

SCARF/EAM is een kostbare techniek, temeer daar de toepassingsprogrammatuur moet worden aangepast. Omdat de gegevens worden weggeschreven in een speciaal bestand moeten extra maatregelen worden getroffen om dit bestand te beschermen tegen ongeautoriseerde verwijdering en modificatie. Dit is overigens van toepassing op alle audit tools die gegevens wegschrijven in een bestand voor latere raadpleging.

*Snapshots*
Met behulp van een snapshot wordt een beeld vastgelegd voor en na de verwerking van geselecteerde transacties. Het geeft alle gegevens die noodzakelijk waren bij het uitvoeren van een berekening of een beslissing, zoals een gebruikt rentepercentage. Zo kan een snapshot van een transactie het volgende wegschrijven: transactiedatum, de transactiegegevens, de tijd die benodigd was om de transactie te verwerken, de identificatie van de gebruiker die de transactie heeft ingevoerd en de naam van de applicatie waarmee is gewerkt.

De snapshot-techniek lijkt zowel op de techniek SCARF/EAM als op tagging. Zij geeft de gebruiker veel detailinformatie over het verwerkingsproces, waardoor de werking van (complexe) applicaties begrijpelijk wordt gemaakt. Wel kleven dezelfde bezwaren aan deze techniek als aan SCARF, namelijk dat zij vrij kostbaar is en dat de toepassingsprogrammatuur geschikt moet worden gemaakt om snapshots toe te passen. De te beoordelen transacties moeten voor verwerking worden geselecteerd. Derhalve kan de techniek niet worden gebruikt ter toetsing van de gegevensverwerking nadat deze heeft plaatsgehad.

*Audit hooks*
Audit hooks worden eveneens in de applicatie gebouwd; hiermee worden signalen afgegeven op het moment dat bepaalde toestanden of gebeurtenissen optreden. Het signaleren van mutaties op inactieve rekeningen werd als voorbeeld gegeven voor het toepassen van SCARF. Dit kan ook met audit hooks worden gerealiseerd. Bij mutaties volgt een signaal waardoor bijvoorbeeld een verslag wordt afgedrukt. Deze techniek is eenvoudiger en goedkoper dan SCARF of snapshot.

*ITF*
ITF staat voor Integrated Test Facility. De testgegevens worden vermengd met produktiegegevens, waardoor het geautomatiseerde systeem continu in de produktiesituatie kan worden getest. De resultaten worden vergeleken met de verwachtingen. Omdat het testen wordt uitgevoerd binnen de produktie-omgeving dienen de handelingen met grote zorgvuldigheid te worden toegepast. De testmutaties moeten worden gecorrigeerd, of worden geleid naar een eenheid die afgescheiden is van de normale bedrijfsadministratie. Deze techniek is arbeidsintensief van aard.

**Het voorbeeld**

Aan de hand van de voorraadcontrole wordt het gebruik van CAAT's voor het testen van de application controls toegelicht. Voorraadregistraties komen tot stand in het inkoop- en verkoopproces, derhalve met de modules inkoop, verkoop, voorraad en grootboek. De modules kunnen worden onderzocht met behulp van source code-onderzoek, flow charting en andere genoemde technieken. Dit wordt niet verder uitgewerkt. De voorbeelden die worden gegeven, richten zich op kritische elementen binnen de processen. Deze elementen of controlevariabelen kunnen met bijvoorbeeld audit hooks of SCARF worden gevolgd, waarvan de resultaten worden weggeschreven in een bestand, dat de accountant later raadpleegt.
De volgende voorbeelden worden genoemd:

- Doorlopende controle op een sluitende goederenbeweging in aantallen, waarbij signalen worden gegeven indien deze niet sluitend is.

- Het rapporteren van negatieve voorraden (indien de applicatie dit toestaat). Indien deze voorkomen kan het duiden op onvolkomenheden in de aansluiting tussen de kantoorvoorraadadministratie (KVA) en de werkelijke voorraad. Een en ander kan leiden tot verschillen bij inventarisatie.

- Het signaleren van alle voorraadcrediteringen die niet worden gedebiteerd op de kostprijs verkopen, bijvoorbeeld vanwege verschrotting, of afboeking van een geconstateerd voorraadverschil. Bij rapportage van dergelijke transacties kunnen de intern getroffen controle-activiteiten worden beoordeeld.

- Het beoordelen van tussenrekeningen door aan de hand van transactiekenmerken automatisch over een periode de op- en afboeking te vergelijken met het inkoopboek, het verkoopboek, etc. Per tussenrekening moet een overzicht worden gemaakt met alle gevonden overeenkomsten in totalen, gesorteerd op tegenrekening. Niet-getraceerde transacties worden gerapporteerd voor nader onderzoek.

- Transacties waarbij marges veel afwijken van gestelde marges. Een deel van de marge kan worden weggegeven in de vorm van kortingen die op een andere wijze worden geboekt. Om een en ander te kunnen controleren is kennis nodig van de procedures en het boekingsschema.

- Het signaleren van transacties met grote inkoopprijsverschillen.

- Onderzoek van geaccepteerde orders van debiteuren die tot de categorie dubieus behoren.

## CAAT'S VOOR TOETSING VAN DE GENERAL IT CONTROLS

CAAT's voor de toetsing van de general IT controls zijn evenmin als CAAT's voor de toetsing van de application controls direct gericht op de vaststelling van de betrouwbaarheid van gegevens. Een verschil is dat de relatie met de uiteindelijk te certificeren gegevens nog losser is; hebben application controls tot doel de betrouwbaarheid van gegevens te waarborgen, general IT controls dienen ter waarborging van de betrouwbaarheid van (geautomatiseerde) gegevensverwerkende processen.

General IT controls hebben betrekking op:
- aanschaf of ontwikkeling, onderhoud en in gebruik neming van apparatuur, besturingsprogrammatuur en toepassingsprogrammatuur;
- toegangsbeveiliging;
- rekencentrumprocedures.

Vooral de werking van toegangsbeveiliging, rekencentrumprocedures en procedures voor het in gebruik nemen van apparatuur en programmatuur leent zich voor toetsing door middel van CAAT's. Procedures voor aanschaf, ontwikkeling en onderhoud van apparatuur en programmatuur zijn niet eenvoudig met behulp van CAAT's te controleren.

**Techniek**

Voor het toetsen van de general IT controls kan gebruik worden gemaakt van standaardfuncties van de besturingsprogrammatuur en/of van speciale audit software, zoals log analysers. Deze CAAT's kunnen verder in twee groepen worden ingedeeld:
- gericht op het registreren en toetsen van toestanden (statisch georiënteerd);
- gericht op het registreren en toetsen van gebeurtenissen (dynamisch georiënteerd).

Navolgend zullen van beide groepen enkele voorbeelden worden gegeven.

*Statisch georiënteerde CAAT's*
Statisch georiënteerde CAAT's kunnen worden gebruikt om installatieparameters, beveiligingsdefinities en andere systeeminstellingen geautomatiseerd te toetsen aan vooraf gedefinieerde waarden. Afwijkingen worden gerapporteerd ten behoeve van handmatig vervolg. Ook kunnen zij worden toegepast voor het uitlijsten van bijvoorbeeld beveiligingsdefinities, die dan verder handmatig moeten worden beoordeeld.
Voorbeelden van instellingen die kunnen worden getoetst, zijn de volgende:

- parameters waarmee de beveiligingsprogrammatuur 'aan' en 'uit' wordt gezet;
- parameters die het mogelijk maken dat programma's buiten de toegangsbeveiliging omgaan;
- parameters waarmee de aanlogprocedure wordt bestuurd (bijvoorbeeld het maximaal toegestane aantal aanlogpogingen);
- syntaxregels voor passwords (aantal tekens, geldigheidsduur en dergelijke). Daarnaast kan worden getoetst op eenvoudig te raden passwords;
- parameters die de logging van gebeurtenissen (operator-handelingen, geweigerde en geslaagde toegangspogingen, etc.) besturen;
- netwerkdefinities, bijvoorbeeld dial in-verbindingen (met dial back-verplichting);
- versie-aanduidingen van programmatuur.

Voorts kunnen de beveiligingsdefinities van bepaalde programma's en gegevensbestanden worden uitgelijst voor handmatige toetsing (aan de voorgeschreven maatregelen van functiescheiding). Ook kan een lijst worden vervaardigd van gebruikers die beschikken over vergaande bevoegdheden, bijvoorbeeld de bevoegdheid om de beveiligingsprogrammatuur uit te schakelen.

De statisch georiënteerde CAAT's hebben niet alleen betrekking op het bestaan van getroffen maatregelen, maar verschaffen ook informatie over de werking van voorgeschreven procedures. Zo zijn te ruime bevoegdheden een aanwijzing dat maatregelen van functiescheiding niet goed werken; de toegekende schrijfrechten op de produktiebibliotheek geven een indicatie over de werking van de procedures voor het in gebruik nemen van programmatuur.

*Dynamisch georiënteerde CAAT's*
Gebeurtenissen die binnen het computersysteem plaatsvinden worden door de besturingsprogrammatuur (soms ook door de toepassingsprogrammatuur) vastgelegd in log-bestanden. Hoewel de omvang van de activiteiten die worden gelogd - afhankelijk van het computersysteem - is in te stellen door de gebruiker, is deze in de regel zodanig omvangrijk dat het handmatig beoordelen van een uitlijsting hiervan ondoenlijk is. Met behulp van CAAT's kunnen de gebeurtenissen worden geselecteerd die relevant zijn voor het vormen van een oordeel over de goede werking van de general IT controls. Voorbeelden van dergelijke gebeurtenissen zijn:

- wijzigingen in installatie- en beveiligingsparameters zoals hiervoor genoemd;
- niet-geslaagde toegangspogingen vanaf bepaalde terminals of door bepaalde gebruikers;
- het uitvoeren van bepaalde programma's, bijvoorbeeld 'utilities';
- geslaagde toegangspogingen door bepaalde gebruikers en/of tot bepaalde programma's en gegevensbestanden.

*Met behulp van CAAT's kunnen de gebeurtenissen worden geselecteerd die relevant zijn voor het vormen van een oordeel over de goede werking van de general IT controls.*

**Het voorbeeld**

Toegespitst op het voorbeeld kan de accountant met behulp van CAAT's de volgende controles uitvoeren op de general IT controls:

Statisch:

- Toetsing van de actuele programmaversies van de inkoop-, verkoop- en voorraadmodules aan de geautoriseerde programmaversies volgens de test- en overdrachtsdocumentatie.

- Toetsing van de toegekende bevoegdheden tot de relevante programmamodules en gegevensbestanden aan de voorgeschreven functiescheiding. Bijvoorbeeld: de inkoopfunctie heeft (via de desbetreffende modules) uitsluitend schrijfrechten op het bestand met inkooporders en leesrechten op de bestanden met voorraadgegevens en inkoopfactuurgegevens.

Dynamisch:

- Selectie van programmawijzigingen (schrijfacties op de produktiebibliotheek) en toetsing aan de test- en overdrachtsdocumentatie.

- Toetsing van de uitgevoerde programma's aan de hand van het verwerkingsrooster.

- Toetsing van de bij de geregistreerde transacties vastgelegde gebruikers aan de voorgeschreven functiescheiding. Bijvoorbeeld: bij alle inkooporders moet de gebruikerscode van de inkoopfunctie zijn vastgelegd; bij geen enkele inkoopfactuur mag de gebruikerscode van de inkoopfunctie zijn vastgelegd.

## VOORWAARDEN VOOR HET TOEPASSEN VAN CAAT'S

Voor het toepassen van CAAT's zal moeten zijn voldaan aan een aantal voorwaarden, zowel aan de zijde van de gecontroleerde als aan de zijde van de controlerend accountant. In deze paragraaf zal hierop nader worden ingegaan. De volgende onderwerpen worden behandeld:

- juistheid en volledigheid van de bestanden;
- integriteit en vertrouwelijkheid van de gegevens;
- betrouwbaarheid van de applicatie;

- voortdurende werking van de application controls en general IT controls;
- beheerst gebruik van CAAT's;
- bewaring, documentatie en beveiliging van bestanden en programmatuur.

*Juistheid en volledigheid van de bestanden*
Indien bestanden van de cliënt worden gebruikt voor nader onderzoek, zal moeten worden vastgesteld dat de bestanden die worden onderzocht de juiste en volledige gegevens bevatten. Dit geldt zowel indien wordt gewerkt op het systeem van de cliënt, als bij gebruik van de eigen micro. Met name indien het oorspronkelijke bestand is ontleed tot een kleiner en handzamer bestand, moet de wijze waarop deze ontleding heeft plaatsgevonden, worden beoordeeld en gedocumenteerd.

*Integriteit en vertrouwelijkheid van de gegevens*
De cliënt zal niet altijd positief staan tegenover het beschikbaar stellen van alle gegevensbestanden. De accountant zal grondige maatregelen moeten treffen om de vertrouwelijkheid van de gegevens te waarborgen. Daarnaast mogen gegevens van de gecontroleerde niet worden veranderd. Hoewel een aantal verificatiewerkzaamheden in de produktie-omgeving moet worden uitgevoerd zal, daar waar mogelijk, moeten worden gewerkt in een van produktie afgescheiden omgeving.

*Betrouwbaarheid van de applicatie*
Er moet worden vastgesteld dat de controletoepassing betrouwbaar functioneert. Dit is niet alleen voor de accountant van belang, maar ook voor de gecontroleerde:
- het verwerkingsproces van de gecontroleerde kan worden beïnvloed door (onevenwichtige) routines die in opdracht van de accountant worden uitgevoerd;
- de routines die de accountant laat uitvoeren, kunnen (bewust) door de gecontroleerde worden beïnvloed.

Dit laatste risico is groter wanneer gebruik wordt gemaakt van toepassingen van de gecontroleerde. De accountant moet de betrouwbaarheid van de uitkomsten zelfstandig vaststellen aan de hand van reeds gecontroleerde gegevens. Indien de general IT controls zijn beoordeeld en afdoende functioneren, zijn deze risico's minimaal en behoeven minder eigen werkzaamheden te worden uitgevoerd. Ook toepassingen van te goeder naam en faam bekend staande leveranciers, waarop geen modificaties zijn aangebracht, hebben een positieve invloed op de risico-afweging.

Het feit dat de accountant het verwerkingsproces van de organisatie stoort, kan worden voorkomen door te werken op rustige momenten van de dag, op een eigen computer of op een testsysteem. Indien 'bugs' voorkomen in de toepassingen kan het verwerkingsproces stagneren. Er bestaan bijvoorbeeld programma's waarvoor accountantskantoren een zogenaamde 'travel license' hebben. Dit houdt in dat één licentie ter beschikking staat aan het over de gehele wereld verspreide accountantskantoor. De applicatie zal over de gehele wereld reizen, her en der worden geïnstalleerd (en weer verwijderd) waardoor de kans op virussen wordt vergroot.

*Voortdurende werking van de application controls en general IT controls*
Het onderzoek naar de application controls en general IT controls zal doorgaans tijdens de interimwerkzaamheden worden uitgevoerd, waarbij tijdens de balanscontrole de blijvende werking van de application controls en/of de general IT controls moet worden vastgesteld. Bij het ontbreken van goed werkende general IT controls zal onder meer moeten worden vastgesteld dat de geprogrammeerde procedures, een onderdeel van de application controls, periodiek worden getoetst door de gebruikers. Anders gesteld: er moet worden vastgesteld dat de gebruikers gebruik maken van de in de automatisering opgenomen controlemaatregelen, maar hier niet onvoorwaardelijk op steunen en zelfstandig controles uitvoeren om de blijvende werking van de automatisering te testen.

*Beheerst gebruik van CAAT's*
Voor het toepassen van CAAT's moet een proces worden gevolgd dat vergelijkbaar is met de ontwikkeling van een (geautomatiseerd) systeem in het algemeen. Een veel gevolgde fasering hierbij is: probleemanalyse, vooronderzoek, ontwerp, programmering, testen en invoering.

In de fase van het vooronderzoek en de probleemanalyse dient, gegeven de controle-omgeving van de te onderzoeken organisatie, beoordeeld te worden of gebruik kan worden gemaakt van geautomatiseerde toepassingen. De accountant kan hiervoor advies inwinnen bij onder meer EDP-auditspecialisten, programmeerdeskundigen en het hoofd Automatisering. Hierbij moet worden afgewogen of de te realiseren besparingen opwegen tegen de inspanningen. De besparingen zullen veelal in toekomstige periodes worden terugverdiend. Daarnaast kunnen de inspanningen eventueel worden gebruikt bij andere controles. Dit geldt vooral voor branchegerichte toepassingen.

De te verrichten werkzaamheden voor gebruik van CAAT's dienen goed te worden gepland. Op het moment dat de balanscontrole begint, moet de testfase zijn gepasseerd en de toepassing klaar staan voor gebruik. Het uitvoeren van de balanscontrole is over het algemeen een vrij hectische periode waarin weinig tijd is om veranderingen door te voeren en/of nieuwe toepassingen uit te proberen.

*Bewaring, documentatie en beveiliging van bestanden en programmatuur*
De controlewerkzaamheden dienen in het algemeen goed en helder te worden gedocumenteerd. Indien gebruik wordt gemaakt van CAAT's, met name voor dit doel speciaal ontwikkelde programma's, queries, spreadsheets en dergelijke, dienen deze te worden gedocumenteerd en bewaard. Dit is noodzakelijk om verantwoording te kunnen afleggen. Daarnaast moeten deze hulpmiddelen bij

*Drs. L.H. Dam RA*
*Was van 1989 tot 1992 werkzaam als assistent-accountant. Vanaf 1992 is hij werkzaam als EDP-auditor. Hij heeft ervaring met de begeleiding en uitvoering van onderzoeken naar de betrouwbaarheid, continuïteit en doeltreffendheid van kleine tot middelgrote geautomatiseerde informatiesystemen. Deze beoordelings- en adviseringsactiviteiten hebben betrekking op organisatorische en technische aspecten bij cliënten uit het bankwezen, de handelsbranche en de dienstverlening.*

*Drs. P. Veltman RE RA*
*Is sedert 1983 werkzaam bij KPMG Klynveld, gedurende een aantal jaren in de controlepraktijk, thans in de functie van senior EDP-auditor. Zijn audit-ervaring ligt op het terrein van besturingssystemen en beveiligingspakketten, informatiesystemen en automatiseringsorganisaties. Hij heeft een aantal artikelen over deze onderwerpen gepubliceerd.*

de volgende controle opnieuw worden ingezet. Gegevens en bestanden die afkomstig zijn van cliënten dienen uiteraard met de grootste zorgvuldigheid te worden bewaard, zonder dat toegang aan ongeautoriseerden wordt verleend.

## DE TOEKOMST VAN AUDIT AUTOMATION

De informatietechnologie heeft de afgelopen tien jaar, net als het decennium ervoor, een grote ontwikkeling gekend. Geconstateerd moet worden dat het toepassen van CAAT's hierbij geen aansluiting heeft kunnen vinden. De verwachting is dat het belang van informatietechnologie in die mate zal toenemen dat de accountant wordt gedwongen ervan gebruik te maken. Een voorbeeld dat altijd wordt aangehaald, is EDI (Electronic Data Interchange). Bij gebruikmaking van EDI behoeven geen (bron)documenten meer te worden uitgewisseld, waardoor detailcontrole met brondocumenten niet meer kan worden uitgevoerd. Het onderzoek naar general IT controls en application controls zal dan een belangrijke plaats innemen binnen het geheel van controlewerkzaamheden.

Voorts bestaan er verwachtingen dat de accountant efficiënter te werk kan gaan door gebruik te maken van computers, waardoor de accountantskosten lager worden. Dat de toepassingen in het 'bedrijfsleven' ook niet altijd hebben geleid tot noemenswaardige efficiëntiewinsten wordt wel eens vergeten.

Hardware heeft ook een sterke ontwikkeling ondergaan. Integratie tussen platforms van diverse merken heeft al jaren de aandacht. Hoewel leveranciers, vanuit concurrentie-overwegingen, fel gekant waren tegen integratie met andere computers, is nu een duidelijke trend begonnen op het gebied van integratie met andere platforms en standaardisatie van database management-systemen.

Het end-user computing is de laatste jaren verder uitgebreid. Meer en meer wordt de gebruiker in staat gesteld eigen applicaties te ontwikkelen, doordat de toepassingen waarmee dit mogelijk is eenvoudiger zijn te bedienen. Derhalve neemt de noodzaak van (dure) specialisten af.

Met behulp van de huidige datacommunicatietechnieken is het al mogelijk te controleren vanaf één werkplek. De controle-activiteiten kunnen hierdoor meer worden verspreid over het jaar, met vermindering van de tijdsdruk waaronder veelal in de eerste maanden van het jaar wordt gewerkt. Door de verspreiding van de werkzaamheden wordt de 'leegloop' gedurende de zomermaanden opgevuld, waardoor accountantskantoren minder medewerkers in dienst behoeven te hebben.

Er is in de jaren tachtig een ontwikkeling geweest op het gebied van decision support-systemen, expertsystemen en artificial intelligence. Deze ontwikkelingen hebben minder gebracht dan op voorhand was verwacht. Misschien dat in de komende jaren een doorbraak wordt gerealiseerd, waardoor dergelijke systemen een bredere toepassing kunnen krijgen. Hier past evenwel een kanttekening met betrekking tot het onafhankelijk oordeel dat de accountant uitspreekt. Dit is mede gebaseerd op 'professional judgement', iets wat moeilijk tastbaar is, maar wordt gevormd gedurende het contact met de cliënt, het aanwezig zijn, het proeven van de organisatie. De verwachting is dat accountants, net als de meeste professionals, weerstand moeten overwinnen om bedoelde toepassingen te gebruiken.

## CONCLUSIES

De technische vooruitgang is in het laatste decennium wederom enorm geweest. Zij heeft echter niet geleid tot revolutionair gebruik van audit software. De ontwikkelingen op het gebied van hardware en toepassingsprogrammatuur zullen zich meer en meer richten op de eindgebruiker. Door het gebruik van krachtige pakketten die eenvoudig te bedienen zijn zal de behoefte aan programmeurs verder afnemen. Ook accountants zullen in staat worden gesteld dergelijke flexibele toepassingen te gebruiken.

In het kader van de adviserende taak van de accountant verdient het gebruik van audit software de aandacht. Hoewel de accountant toepassingen kan gebruiken om de controle efficiënter uit te voeren, zal met name de organisatie erbij gebaat zijn een goede informatievoorziening te hebben. De toepassingen kunnen veel waarde hebben ter beoordeling van de eigen, interne activiteiten. De inzet van CAAT's zou derhalve moeten worden overlegd met de gecontroleerde voor eventueel intern gebruik. Met name de toepassingen die (om technische redenen) operationeel moeten zijn in de produktie-omgeving, zijn niet zonder overleg en medewerking van de gecontroleerde te gebruiken. De accountant zal vooral het intern gebruik moeten toetsen, in plaats van deze toepassingen zelfstandig te gebruiken.

Als doelstelling voor het gebruik van audit automation werd gegeven dat zij moest bijdragen aan een efficiënte vervulling van de accountantscontrole. Hierbij gaat het inderdaad om het gebruik maken van audit software en niet zozeer om het zelf toepassen. In dit artikel is daarom ook de term management-software geïntroduceerd.

# Operational auditing en EDP-auditing; is hier sprake van een begripsverwarring?

J.C. Boer RE RA

**Is het terecht om EDP-auditing te beschouwen als een onderdeel van het momenteel sterk opkomende operational auditing? Wat zijn de overeenkomsten en verschillen tussen deze disciplines? De auteur toont aan dat er plaats is voor een zelfstandige positie van EDP-auditing, naast operational en ook financial auditing. Wel is er sprake van overlap. Boer bepleit om voor het overlappende gebied tusen EDP- en operational auditing, het begrip operational EDP-auditing te introduceren.**

## INLEIDING

Operational auditing is een begrip dat thans een prominente plaats inneemt in de management-literatuur en in publikaties binnen accountantskringen. Het is een auditing-begrip naast begrippen als financial auditing (de jaarrekeningcontrole), EDP-auditing en milieu-auditing.
Publikaties over operational auditing wijden over het algemeen enige paragrafen aan de positie van operational auditing ten opzichte van de andere auditing-begrippen. Dit artikel belicht de raakvlakken en de verschillen tussen operational en EDP-auditing vanuit laatstgenoemde discipline. De bedoeling is vanuit deze positie een bijdrage te leveren in de discussie over de toegevoegde waarde van operational auditing, in het bijzonder met betrekking tot de beheersing van de geautomatiseerde informatieverwerking.

Het artikel start met een beschouwing van operational auditing, waarbij aspecten worden belicht die van belang zijn in relatie tot EDP-auditing. Vanuit dit standpunt kunnen echter niet alle relevante aspecten worden beschouwd. De tweede paragraaf gaat in op de resterende punten indien vanuit het vakgebied EDP-auditing wordt geredeneerd. Tot slot zal nog enige aandacht worden besteed aan de bijdrage van auditing voor de beheersing van de geautomatiseerde gegevensverwerking.

## OPERATIONAL AUDITING

Er zijn verschillende definities van operational auditing in omloop. Ook zijn er publikaties waarin operational auditing wordt omschreven zonder een definitie op tafel te leggen. Om dit artikel niet in misverstanden te laten verzanden moet het begrip duidelijk zijn. Het artikel gaat uit van de volgende brede definitie:
Operational auditing is een periodieke, onafhankelijke doorlichting van een organisatie-eenheid of een proces waarbij aan de hand van een aantal relevante indicatoren systematisch een oordeel kan worden gegeven over een breed scala van aspecten van de bedrijfsvoering. Hierdoor kunnen op discontinue wijze met behulp van normen de opzet, het bestaan en de werking van de interne organisatie aan de geformuleerde doelstellingen worden getoetst. [Drie92]

### Management tool

Operational auditing wordt over het algemeen gepresenteerd als een management tool voor het besturen van organisaties. Als sterk punt van het tool wordt de bruikbaarheid voor het beheersen van sterk gedecentraliseerde organisaties gezien. Door de uitvoering van een operational audit krijgt het topmanagement een beeld van de wijze waarop deze decentrale units met hun verantwoordelijkheden omgaan. Dit is een uitbreiding van de beheersing die uitsluitend steunt op de (financiële) prestaties van de units. De opkomst van operational auditing mag niet los gezien worden van de delegatie van bevoegdheden naar plaatsen in de organisatie waarop het management geen direct zicht meer heeft.

*De inzet van EDP-auditors moet voorkomen dat 'blind' op de goede uitvoering van de gedelegeerde taken moet worden vertrouwd.*

In de voorgaande alinea zien we een overeenkomst met het ontstaan van EDP-auditing als tool voor het management. EDP-auditing geeft de manager grip op een onderdeel van het bedrijfsproces dat door zijn technische karakter buiten de directe controlemogelijkheden van het verantwoordelijke management is komen te liggen. De inzet van EDP-auditors moet voorkomen dat 'blind' op de goede uitvoering van de gedelegeerde taken moet worden vertrouwd.

### Relatie met financial auditing

Naast de positionering als zelfstandig management tool is er mijns inziens een overlap tussen het terrein van de operational auditing en de financial auditing. Operational auditing kan tot conclusies leiden die een antwoord geven op vragen die in het kader van een systeemgerichte accountantscontrole van belang zijn. Dit komt overeen met de resultaten van sommige EDP-audits. Het betreft conclusies die iets zeggen over de betrouwbaarheid van de procedures met betrekking tot de registratieve en administratieve processen. In de praktijk bestaan situaties waarbij de interne accountantsdienst een operational auditing-opdracht heeft waarbij de invulling in de praktijk zich richt op de terreinen van de administratieve organisatie en interne controle. De externe accountant steunt bij het uitvoeren van zijn financial audit voor wat betreft de toetsing van de administratieve organisatie en interne controle volledig op de intern verrichte operational audit-werkzaamheden.

### Terreinafbakening

Operational auditing kan gericht zijn op een veelheid van objecten (de 'operations'). De afbakening van deze objecten wordt bepaald door de kaders en de regelgeving zoals deze door het topmanagement zijn aangegeven. Ook de kwaliteitsaspecten waarop de operational auditing zich richt kunnen van velerlei aard zijn. De invulling wordt bepaald door de behoefte van de opdrachtgever. Het object kan betrekking hebben op bijvoorbeeld logistiek, personeelszaken, systeemontwikkeling. De gekozen kwaliteitsaspecten liggen over het algemeen op het terrein van de efficiëntie, effectiviteit en betrouwbaarheid.

### Deskundigheid

Het ligt voor de hand de audit te laten uitvoeren door deskundigen op het terrein van auditing. In het algemeen gesproken ligt de materiedeskundigheid voor de audit van administratieve bedrijfsprocessen bij accountants. De onderzoeken van de accountants zijn over het algemeen sterk gericht op de aspecten betrouwbaarheid en controleerbaarheid van processen, met betrekking tot een terrein dat afgebakend wordt door de deskundigheid die nodig is voor de wettelijk verplichte verklaring bij de jaarrekening.

Voor de uitvoering van operational audits is, naast de algemene kennis en ervaring over de aanpak van een audit, deskundigheid vereist over de efficiënte en effectieve inrichting van het in beschouwing genomen proces. Bij accountants is deze deskundigheid beperkt tot de financiële en administratieve processen. Voor de uitvoering van operational audits is deskundigheid op het specifieke onderzoeksterrein (logistiek, personeelszorg, systeemontwikkeling) onontbeerlijk. Dit betekent, indien ervoor wordt gekozen de operational auditing vanuit de accountantsdiscipline in te vullen, een bijscholing en/of het aantrekken van specialisten op het terrein van de te beschouwen objecten. Hetzelfde is te zien geweest ten aanzien van EDP-auditing. Door bijscholing en het aantrekken van specialisten waren accountants in staat op een verantwoorde wijze invulling te geven aan EDP-auditing.

De reden dat EDP-auditing door de accountants is opgepakt, ligt in de noodzaak tot onderzoeken in de EDP-organisatie uit hoofde van de accountantscontrole. De onderzoeken zijn nodig om een oordeel te kunnen krijgen over de betrouwbaarheid van het totale administratieve systeem in omgevingen waar ook de gebruikers van de computers (onbewust) in meerdere of mindere mate steunen op de betrouwbaarheid van de computerverwerking. Doordat de accountant deze onderzoeken niet zonder meer kan uitvoeren, is een specialisme ontstaan.

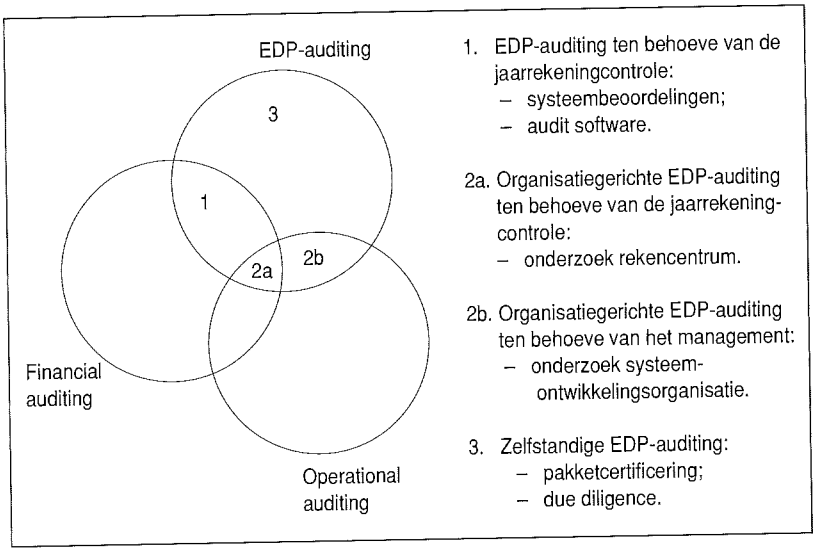
Onderzoeken naar de betrouwbaarheid van processen (operations) binnen de organisatie-eenheden belast met de registratie van het bedrijfsproces en de administratieve verwerking, zijn door accountants altijd als een natuurlijk onderdeel van hun werkzaamheden gezien en zijn als zodanig niet apart benoemd. Hierbij moet worden aangetekend dat dikwijls deze onderzoeken, vooral bij interne accountants, niet tot de interne controle beperkt blijven, doch dat ook aan de efficiëntie van de genoemde processen aandacht wordt besteed; dit laatste binnen de kaders van de gevraagde en ongevraagde adviesfunctie die in de controle-opdracht zijn begrepen. Nu echter voor onderzoeken van de 'operations' nieuwe terminologie beschikbaar komt kan de accountant hier dankbaar gebruik van maken.

### Normen

De accountancy kent een normenstelsel dat op basis van ervaring en studie op het terrein van de beheersing van het administratieve proces tot stand is gekomen. Ook binnen de EDP-auditing heeft dit proces zich voltrokken, al is de ontwikkeling door haar relatief jonge leeftijd ten opzichte van de financial auditing minder ver.
Operational auditing is breder dan het gebied dat van oudsher door de accountants wordt afgedekt. Met de uitvoering van operational audits worden vanuit auditing gezien nieuwe terreinen betreden, waarvoor de ontwikkeling van normen nog moet geschieden. Het hebben van normen is een voorwaarde voor de professionalisering van het vakgebied. Zonder het expliciet kunnen maken van een normenstelsel zal herhaalde uitvoering van een zelfde audit tot andere en niet tot de andere audit herleidbare resultaten leiden. Het ontwikkelen van uitgangspunten om tot het formuleren van normen te kunnen komen is een krachtsinspanning waarvoor het vakgebied operational auditing zich thans geplaatst ziet.

## EDP-AUDITING

Het handboek EDP-auditing hanteert de volgende definitie:
*'EDP-auditing is het vakgebied dat zich bezighoudt met het beoordelen van één of meer kwaliteitsaspecten van (onderdelen van) de informatievoorziening in een omgeving waar gebruik wordt gemaakt van informatietechnologie' [Hand93].*




*Figuur 1. Samenhang auditing-begrippen.*

In figuur 1 is de verhouding tussen financial en operational auditing gevisualiseerd. Bepalend voor de plaats in de cirkels is de doelstelling waarmee EDP-auditing wordt uitgevoerd (hetgeen verduidelijkt is met enkele voorbeelden). Zij kan onderdeel uitmaken van de controle van de jaarrekening (1) of van operational auditing (2). Hierbij kan een begripsverwarring optreden omdat bij een systeemgerichte aanpak van de accountantscontrole ook controlewerkzaamheden worden uitgevoerd die onder het begrip operational auditing en EDP-auditing zijn te rangschikken (2a). Daarnaast zijn er EDP-audits (2b) die, omdat ze sterk op de organisatie gericht zijn (de operations van de systeemontwikkeling, computerverwerking of de netwerken), tevens als een operational audit gericht op de geautomatiseerde informatieverwerking kunnen worden aangeduid. Hiervoor zou het nieuwe begrip 'operational EDP-auditing' kunnen worden geïntroduceerd.

### Scope

Operational auditing is gericht op een oordeelsvorming naar de mate waarin een organisatie voldoet aan de door het management aangegeven doelstellingen en regels. Het onderzoek heeft betrekking op de structuur van het desbetreffende organisatieonderdeel en/of de daarbinnen operationeel zijnde processen. Toetsing van de kwaliteit van het produkt van de organisatie is geen doel op zich. De kwaliteit van het produkt kan hooguit worden gebruikt als middel om iets over het te beoordelen proces of de te beoordelen organisatie vast te stellen (bijvoorbeeld het aantal door een proces voortgebrachte produkten om een indruk van de produktiviteit te krijgen).
De jaarrekeningcontrole is primair gericht op een door de organisatie voortgebracht produkt: de jaarrekening. Beoordeling van de processen en structuren heeft hier slechts een ondersteunende functie. Door een deels systeemgerichte aanpak is het niet nodig alle aan de jaarrekening ten grondslag liggende gegevens te toetsen. Het oordeel steunt deels op de kwaliteit van de controle- en

*J.C. Boer RE RA*
*Is lid van de maatschap KPMG Klynveld EDP Auditors. Hij is verantwoordelijk voor een regionaal opererend EDP-auditing-team. Op grond van zijn in 1978 gestarte EDP-auditing-loopbaan bezit hij een lange en ruime ervaring op alle terreinen van de EDP-auditing.*

herstelmaatregelen die onderdeel uitmaken van de organisatiestructuur en de inrichting van het administratieve proces (de procedures).
EDP-auditing kent onderzoeken die gericht zijn op de organisatie (structuur en werkproces) van systeemontwikkeling, gegevensverwerking en -transport (bijvoorbeeld onderzoeken gericht op de rekencentrumorganisatie, de beveiliging van een netwerk). Anders dan operational auditing kent EDP-auditing echter ook opdrachten die gericht zijn op de produkten uit de automatiseringsorganisatie; voorbeelden hiervan zijn systeemonderzoek en pakketcertificering.
De stemmen die EDP-auditing als een vorm van operational auditing betitelen, gaan voorbij aan een belangrijk aspect van de EDP-auditing: de toetsing van de produkten van de automatiseringsorganisatie. De oordeelsvorming over het produkt vraagt over het algemeen andere vaardigheden dan het beoordelen van organisaties. Het laatste heeft meer het karakter van adviseren; het eerste ligt dichter tegen de problematiek omtrent verklaringen/mededelingen aan zoals wij die ook zien bij de financial audit.

In tegenstelling tot operational auditing is bij EDP-auditing op voorhand aan te geven op welke bedrijfsprocessen de audit betrekking heeft: de geautomatiseerde informatievoorziening. Dit maakt het ook duidelijker door wie een dergelijke audit moet worden uitgevoerd. Alhoewel binnen EDP-auditing ook weer specialisatie te onderkennen is, is duidelijk dat de auditor deskundig moet zijn met betrekking tot de geautomatiseerde informatieverwerking. Dit in tegenstelling tot de operational auditor; de hiervoor benodigde deskundigheid kan op vele gebieden liggen. Op basis van deze constatering is het voor de operational auditor moeilijker dan voor de EDP-auditor om zelf, op algemeen niveau, het vakgebied in zijn geheel te beheersen. Een goede operational auditing-staf zal moeten bestaan uit auditors met verschillende achtergronden.

## BEHEERSING VAN DE ELEKTRONISCHE GEGEVENSVERWERKING

Het is een misverstand te veronderstellen dat operational EDP-auditing een directe bijdrage levert tot een betrouwbaar en/of efficiënt proces. Het zijn oordelen op basis waarvan te constateren is in hoeverre de voorwaarden hiertoe aanwezig zijn. De uitkomsten van een audit kunnen worden gebruikt om de kwaliteit van de gegevensverwerking op onderzochte aspecten te vergroten.
Alvorens tot de inrichting van audit-staven te komen respectievelijk externen opdracht voor audits te verstrekken is het een betere investering om direct te werken aan de beoogde kwaliteitsverbetering. De organisatie moet in staat zijn de bevindingen van de audit te absorberen. Het periodiek beoordelen van een organisatie met een zwak stelsel van interne controle en beveiligingsmaatregelen leidt niet tot een beter produkt van deze organisatie. De constatering dat de automatiseringsorganisatie mogelijk onbetrouwbare produkten voortbrengt, selecteert en repareert deze 'mislukte' produkten nog niet. Onder al het auditing-geweld dreigt dit nog wel eens te worden vergeten. In dit stadium heeft een organisatie meer behoefte aan een veranderingsmanagement en een advies ten aanzien van de inrichting van de systeemontwikkelings- en verwerkingsorganisatie.
Op het terrein van de EDP-auditing begint het besef door te dringen dat met het rapport van de EDP-auditor de organisatie nog niet beter is geworden. Na de audit moet de bereidheid aanwezig zijn lacunes weg te nemen. De frustratie van een EDP-auditor kan wellicht verminderd worden indien de audit onder de vlag van operational auditing in opdracht van het voor de gegevensverwerking verantwoordelijke management wordt uitgevoerd. Dit is voor het initiëren van een verandering een betere positie dan een audit in opdracht van een gebruiker van de produkten van de automatiseringsorganisatie (de accountant).

## CONCLUSIE

Recapitulerend is er een aantal verschillen en overeenkomsten tussen EDP-auditing en operational auditing. De overeenkomsten maken het mogelijk operational auditing als verzamelnaam voor operations-gerichte onderzoeken te gebruiken, waar termen als EDP en administratieve organisatie verwijzen naar het proces waarop zij betrekking heeft. Daarnaast omvat EDP-auditing echter een aantal activiteiten die niet zonder meer onder de vlag operational auditing kunnen worden gebracht. Het begrip operational auditing mag op deze terreinen niet in de plaats van het begrip EDP-auditing worden gebruikt.
In de verhouding EDP-auditing en operational auditing is sprake van twee verzamelingen die voor een deel overlappend zijn. Het geheel overziend kan de conclusie worden getrokken dat het begrip operational auditing geen afgebakend terrein bestrijkt. Bij een concrete audit zal duidelijk moeten worden aangegeven op welke operations de audit betrekking heeft en welke kwaliteitsaspecten in de scope worden betrokken. De aard van de operations bepaalt immers het kennis- en ervaringsgebied dat voor de uitvoering van de audit noodzakelijk is. Voor het deelterrein van de geautomatiseerde gegevensverwerking valt de term operational EDP-auditing te overwegen.

## LITERATUUR

[Drie92] Drs. A.J.G. Driessen en A. Molenkamp, *Operational auditing: managementtechniek of interne-controlemethodiek?* MAB, juni 1992.

[Drie93] Drs. A.J.G. Driessen, J.W. van der Kerk en A. Molenkamp, *Operational auditing*, Kluwer Bedrijfswetenschappen, 1993.

Hand93] *Handboek EDP-auditing;* Kluwer Bedrijfswetenschappen, 1993.

# Accountant, EDP-auditor en jurist: een multidisciplinaire samenwerking

Mw.mr.drs. A.W. Duthler

**Welke consequenties heeft de Wet computercriminaliteit voor organisaties die gebruik maken van informatietechnologie, en wat wordt hierbij van de accountant en de EDP-auditor verwacht? Wat moet er allemaal worden geregeld in een Service Level Agreement en hoe kunnen accountant en EDP-auditor de cliënt hierbij ondersteuning bieden?**
**De auteur beargumenteert vanuit een bestuurskundige en juridische achtergrond dat voor de beantwoording van deze en dergelijke vragen multidisciplinaire samenwerking tussen accountant, EDP-auditor en jurist noodzakelijk is.**

## INLEIDING

Gedurende drie jaar was een topambtenaar van de financiële afdeling van de gemeente Rotterdam in staat de geautomatiseerde gegevensverwerking te manipuleren, waardoor hij 8,2 miljoen gulden kon oversluizen naar persoonlijke rekeningen. De fraude werd bij toeval ontdekt door een bankemployé. De ambtenaar was aangesteld om door het opzetten van een geautomatiseerd systeem een einde te maken aan de administratieve chaos die op de financiële afdeling heerste. Het gevolg was dat hij als enige wist welke mogelijkheden het computersysteem bood. Controles werden nooit uitgevoerd, er werd van uitgegaan dat het computersysteem zichzelf controleerde. De voorschriften die waren bedoeld om fraude te voorkomen, werden slecht nageleefd. Niet alleen bleven zelfs de eenvoudigste controlehandelingen achterwege, ook werd verzuimd het werk van de ambtenaar te laten toetsen door het gemeentelijk rekencentrum. Waarschuwingen van de gemeentelijke accountantsdienst werden genegeerd. Deze miljoenenfraude was te voorkomen geweest door een betere interne controle.

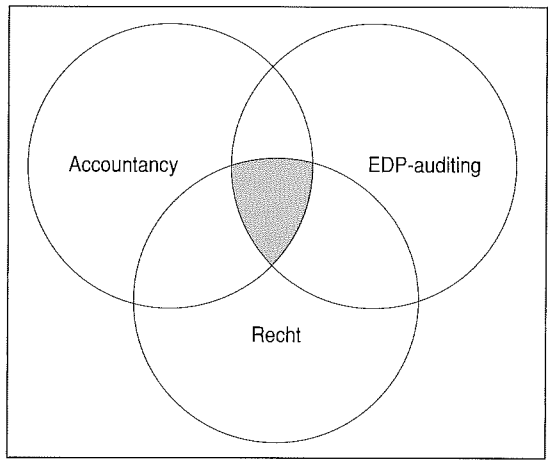
Beheersing van informatietechnologie vergt steeds meer een multidisciplinaire aanpak van zowel juridisch, technisch, administratief als organisatorisch gespecialiseerde professionals. Meestal is juridische, technische, administratieve en organisatorische kennis niet in één persoon verenigd. Accountants, EDP-auditors en juristen blijken elkaar steeds vaker nodig te hebben bij vraagstukken die betrekking hebben op beheersing van informatietechnologie.

In dit artikel zal een overzicht worden gegeven van de raakvlakken tussen de verschillende disciplines accountancy, EDP-auditing en recht.
Eerst zullen mogelijke onderwerpen worden geïnventariseerd waarbij zich raakvlakken tussen verschillende disciplines voordoen. Vervolgens zullen enkele onderwerpen worden geselecteerd, waarbij per onderwerp de rol van de verschillende disciplines zal worden beschreven.

In het kader van dit artikel wordt met 'de accountant' zowel de interne als de externe accountant bedoeld, tenzij anders wordt aangegeven of uit de context blijkt dat anders wordt bedoeld. Geredeneerd vanuit de natuurlijke adviesfunctie kan de accountant in aanraking komen met onderstaande onderwerpen. Hij komt dan op een terrein waarop raakvlakken bestaan met andere disciplines. De belangrijkste rol van de accountant is dan het onderkennen van die raakvlakken en het signaleren van mogelijke knelpunten, zodat hij - indien nodig - de andere disciplines kan inschakelen. De accountant wordt in dit artikel dan beschouwd als een generalist die specialisten zoals juristen en EDP-auditors kan inschakelen. Daarnaast treedt de accountant op als specialist wanneer het administratief-organisatorische aspecten betreft. Behalve door de accountant kunnen EDP-auditors en juristen ook rechtstreeks door het management worden ingeschakeld.

## INVENTARISATIE

In figuur 1 is het gebied van mogelijke raakvlakken tussen de verschillende disciplines (gearceerd) weergegeven.




*Figuur 1. Het raakvlak tussen accountancy, EDP-auditing en recht, waarop multidisciplinaire samenwerking gewenst is (gearceerd).*

Een eerste inventarisatie van onderwerpen waarop deze raakvlakken betrekking hebben levert het volgende beeld op:

*Privacy-bescherming*
Er zijn veel wettelijke regelingen die betrekking hebben op de bescherming van de persoonlijke levenssfeer. Eén daarvan is de Wet persoonsregistraties (WPR). Deze wet stelt onder andere beveiliging van persoonsregistraties waarin gevoelige gegevens zijn opgenomen verplicht. Voor het opstellen of beoordelen van beveiligingsmaatregelen is inbreng van EDP-auditors en accountants gewenst. Advisering over andere vereisten uit de WPR is een taak voor een jurist.

*Computercriminaliteit*
Computercriminaliteit kan worden omschreven als door de wet strafbaar gestelde gedragingen waarbij van computers gebruik wordt gemaakt. Maatregelen ter voorkoming en beperking van de schade als gevolg van computercriminaliteit moeten worden gezocht in de techniek, in de (administratieve) organisatie en in contracten. Maatregelen waarbij zowel accountants, EDP-auditors als juristen betrokken zijn.

*Service Level Agreements (SLA's)*
Een SLA regelt de afspraken tussen een automatiseringsorganisatie en haar afnemers van informaticadiensten. Het opstellen van dergelijke contracten vergt een gedegen kennis van automatisering, administratieve organisatie en contractvormen. Deze kennis zal moeten worden geleverd door EDP-auditors, accountants en juristen gezamenlijk.

*Bewijs- en bewaarplicht in een geautomatiseerde omgeving*
Elektronische berichten kunnen worden gebruikt als bewijsmiddel in civiele procedures. (Bewijs kan worden geleverd met alle mogelijke middelen.) De rechter staat echter argwanend tegenover elektronische bewijsmiddelen omdat deze kunnen worden gewijzigd zonder dat dat achteraf is vast te stellen. EDI-gebruikers kunnen de bewijskracht van hun elektronische registraties vergroten door maatregelen te nemen die de kans op onjuiste registratie van het bericht of een manipulatie van de inhoud van het bericht na registratie minimaliseren. Deze maatregelen kunnen worden opgesteld door accountants en EDP-auditors.

Met bewijs hangt bewaring samen. Op een aantal plaatsen in de wet is een bewaarplicht van bepaalde documenten vastgesteld. De vraag of en hoe aan de wettelijke bewaarplichten in een EDI-omgeving kan worden voldaan, zal moeten worden beantwoord door juristen, accountants en EDP-auditors gezamenlijk.

*Escrow*
Escrow houdt in dat de broncode van programmatuur bij een derde in bewaring wordt gegeven, die deze broncode aan de gebruiker zal uitleveren als een bepaalde, van tevoren contractueel omschreven voorwaarde in vervulling is gegaan.
Behalve de juridische regeling is de technische en praktische uitwerking van een escrow van groot belang. Een technische test zal moeten worden uitgevoerd om te controleren dat datgene wat de leverancier deponeert en hetgeen de gebruiker ontvangt bij uitlevering, exact die broncode is die hoort bij de door de gebruiker gebruikte versie van de programmatuur. Deze test zal kunnen worden uitgevoerd door - onder andere vanwege zijn onafhankelijkheid - een EDP-auditor. Voorts kan de depotnemer verplicht worden op eigen kosten en op eerste verzoek van gebruiker of leverancier een verklaring te overleggen van een accountant omtrent de betrouwbaarheid, vertrouwelijkheid en/of de continuïteit van de organisatie van de depotnemer.

*Geschillenregeling*
Veel geschillen in de automatiseringsbranche dragen een gemengd karakter. De geschillen betreffen vaak zowel technische, organisatorische als juridische vraagstukken. Bij de oplossing of regulering van deze geschillen zullen accountants, EDP-auditors en juristen zijn betrokken. Juristen zijn opgeleid om geschillen op te lossen of te reguleren. Het gaat erom de gevolgen van een gerezen conflict in te perken en de partijen weer op het spoor te brengen om - zo mogelijk - samen verder te gaan. Lukt dat niet, dan moet het conflict in goede banen worden geleid en moet de schade zoveel mogelijk worden beperkt. Juristen zijn voor deze functie het best toegerust, maar indien technische vragen of specifieke programmeervaardigheden een belangrijke rol spelen, zullen zij het niet zonder deskundigen op het gebied van automatisering en organisatie kunnen stellen.

*Software-bescherming*
Computerprogrammatuur wordt in Nederland en in de Europese Gemeenschappen door middel van het auteursrecht beschermd. Voor het gebruik van programmatuur door iemand anders dan de auteursrechthebbende is toestemming vereist van de rechthebbende. Die ander verkrijgt dan gebruiksrechten, ook wel licentierechten genoemd. Heeft hij die toestemming niet, dan gebruikt hij op een illegale manier de software. De praktijk leert dat veel bedrijven vaak, al dan niet bewust, illegale software gebruiken. Onnadenkendheid en onbekendheid met verkregen auteursrechten van de auteursrechthebbende liggen hier vaak aan ten grondslag. De risico's die bedrijven als gevolg van het gebruik van illegale software lopen variëren van schadeclaims door auteursrechthebbende tot aantasting van de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Accountants en EDP-auditors zouden bedrijven hierop moeten attenderen. Ook kunnen zij technische en organisatorische maatregelen voorstellen die gericht zijn op het voorkómen van het gebruik van illegale software [Hors93]. Juristen zouden 'goede' contracten moeten opstellen of contracten goed moeten lezen om te voorkómen dat op een illegale wijze gebruik wordt gemaakt van software.

Omdat het in het kader van dit artikel te ver voert alle hierboven genoemde onderwerpen uitgebreid te bespreken, zullen alleen die onderwerpen aan de orde komen die het meest in de praktijk van zowel een accountant als een EDP-auditor en een jurist zullen voorkomen en/of waarbij de behoefte aan een multidisciplinaire samenwerking het meest noodzakelijk is.
De onderwerpen die hieronder zullen worden besproken, zijn privacy-bescherming, computercriminaliteit, bewijs- en bewaarplicht en geschillenbeslechting. Steeds zal per onderwerp eerst een algemene inleiding worden gegeven. Vervolgens zal de rol van de accountant, respectievelijk EDP-auditor en jurist ten aanzien van dat onderwerp worden besproken, waarna een beschrijving zal worden gegeven van de mate waarin multidisciplinaire samenwerking ten aanzien van dat onderwerp noodzakelijk is. Begonnen wordt met privacy-bescherming.

## PRIVACY-BESCHERMING

Er zijn en er komen steeds meer wettelijke regelingen die betrekking hebben op privacy-bescherming. Denk aan de Wet Gemeentelijke Basisadministraties (GBA), de Wet persoonsregistraties, de Wet Politieregisters en de privacy-richtlijnen van de EG. De Wet Geneeskundige Behandelingsovereenkomst ligt in de Kamer. De belangrijkste (in de zin van meest toepasselijke) of misschien wel meest besprokene is de WPR.
De WPR richt zich op de bescherming van de persoonlijke levenssfeer van diegenen van wie persoonsregistraties in een geschrift zijn opgenomen [NIVR91].
De bescherming heeft betrekking op persoonsgegevens, dat wil zeggen gegevens die tot individuele personen herleidbaar zijn. Zowel geautomatiseerde als sommige handmatig gevoerde persoonsregistraties vallen onder de wet. Behalve eisen ten aanzien van het verstrekken van gegevens - aan wie, op welke wijze - en het aanmelden van registraties bij de Registratiekamer, bevat de wet ook een beveiligingseis.[1] De beveiligingseis is verwoord in artikel 8 van de WPR en stelt dat de houder van een registratie 'zorg moet dragen voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van een persoonsregistratie tegen verlies of verminking van gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan.' Voor de bewerker geldt een zelfde plicht voor het gedeelte van de apparatuur dat hij onder zich heeft, waarmee de registratie wordt gevoerd.
Voor de nadere invulling van deze beveiligingseis zal inbreng van zowel een accountant en een EDP-auditor als een jurist vereist zijn. In de volgende subparagrafen zal nader worden ingegaan op de rol van de drie verschillende functionarissen.

*De praktijk leert dat veel bedrijven vaak, al dan niet bewust, illegale software gebruiken.*

### De rol van de accountant

Redenen waarom een accountant kan worden ingeschakeld, zijn ten eerste dat een accountant onafhankelijk en onpartijdig is; de Gedrags- en Beroepsregels voor accountants hebben een wettelijke basis en bevatten bepalingen ten aanzien van onpartijdigheid, onafhankelijkheid, geheimhouding en tuchtrechtspraak. Ten tweede omdat de privacy-bescherming ook een administratief-organisatorisch vraagstuk is. De administratieve organisatie is een terrein waarop de accountant deskundig is.

De rol van de accountant kan zowel een adviserende als een controlerende zijn [NIVR91]. In zijn adviserende rol kan de accountant behulpzaam zijn bij de ontwikkeling van nieuwe organisatorische procedures, zoals het tot stand brengen van functiescheidingen, om aan de eisen van de WPR te voldoen.

In zijn controlerende rol kan de accountant een onafhankelijk en onpartijdig onderzoek doen met als doel een oordeel te verkrijgen over de wijze waarop persoonsregistraties worden gevoerd en de wijze waarop deze worden beveiligd. Houders, geregistreerden en de Registratiekamer kunnen ieder voor zich behoefte hebben aan een dergelijk onafhankelijk en onpartijdig oordeel door een accountant. Een dergelijk onderzoek is tot op zekere hoogte mogelijk. Aanvullende specialistische deskundigheid op het gebied van automatisering en controle (EDP-audit) zal vaak nodig blijken te zijn.

1. *Overigens stelt de wet ook andere eisen, zoals de eis dat de houder een ieder die daarom verzoekt inzage geeft in diens persoonsgegevens, behoudens enkele uitzonderingen, en de eis dat de houder de geregistreerde op diens verzoek meedeelt aan welke derden het jaar voorafgaand aan het verzoek gegevens zijn verstrekt.*

### De rol van de EDP-auditor

De EDP-auditor zal kunnen adviseren over de te nemen (logische, hardware-matige en fysieke) beveiligingsmaatregelen. Behalve adviseren kan de EDP-auditor ook een oordeel geven over de reeds getroffen beveiligingsvoorzieningen.
Verder kan de EDP-auditor een oordeel geven over hoe de wet wordt nageleefd en kan hierover een uitspraak doen bij de Registratiekamer. Aandachtspunten daarbij zijn de wijze waarop de beheerorganisatie is ingericht en de manier waarop de organisatie omgaat met persoonsgegevens. Ook kan de EDP-auditor een oordeel geven over de gegevens die door het bedrijf worden verstrekt aan derden.

*De eerste verantwoordelijkheid voor de bestrijding van computercriminaliteit ligt bij de bestuurders van de onderneming.*

### De rol van de jurist

Kijken de EDP-auditor en de accountant vooral naar de technische en organisatorische implicaties van de WPR voor organisaties, de jurist zal kunnen adviseren omtrent de interpretatie van wettelijke bepalingen. Zo zal de jurist uitspraken kunnen doen over de gevolgen van het (niet) treffen van adequate beveiligingsmaatregelen.
Tevens zal een jurist organisaties kunnen adviseren over de nadere invulling van wettelijke vereisten. Zo zal hij kunnen aangeven of een organisatie haar registraties dient te beschrijven en te melden bij de Registratiekamer, en zal hij kunnen ondersteunen bij het opstellen van reglementen.

## COMPUTERCRIMINALITEIT

Allereerst de vraag: wat is computercriminaliteit? Computercriminaliteit wordt meestal in verband gebruikt met het begrip computermisbruik. Computermisbruik kan worden omschreven als:
*'gedrag met een voor anderen (potentieel) schadelijk karakter waarbij geautomatiseerde apparatuur en/of programmatuur ter opslag, verwerking of uitwisseling van gegevens is betrokken'* [Jaco93].
Indien een dergelijke gedraging in de wet strafbaar wordt gesteld, spreekt men van computercriminaliteit. Een wet die dergelijke gedragingen strafbaar stelt is de op 1 maart 1993 in werking getreden Wet computercriminaliteit.[2]
Deze wet heeft tot doel computercriminaliteit te bestrijden, door middel van uitbreiding van strafbaar gestelde gedragingen, verruiming van bevoegdheden en opsporingsmogelijkheden en vergroting van het beveiligingsbewustzijn.

2. *Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit).*

Het bestrijden van computercriminaliteit kan op verschillende niveaus plaatsvinden. In de eerste plaats kunnen burgers zelf maatregelen nemen om schade te voorkomen. Gedacht kan worden aan fysieke bescherming door plaatsing van apparatuur in afsluitbare ruimten. Daarnaast vragen waarborgen in de organisatie van de onderneming, zoals scheiding van functies, procesbewaking en kwaliteitscontrole, de aandacht. De Rotterdamse ambtenaar die ruim acht miljoen gulden naar zijn vriendin in een ver land heeft gesluisd, kon dat doen omdat hij zowel ontwerper, programmeur, uitvoerder en controleur was. Het principe van functiescheiding was niet toegepast, noch in de administratieve organisatie noch in de apparatuur en programmatuur. Het is dus noodzakelijk een beveiliging aan te brengen in de te gebruiken programmatuur (encryptie, toegangscode).
Ten slotte komen juridische maatregelen aan de orde [Fran93].

### De rol van de accountant

Zoals hierboven al gesteld heeft de Wet computercriminaliteit tot doel onder andere door vergroting van het beveiligingsbewustzijn computercriminaliteit te bestrijden. De accountant kan hierin een rol spelen door het adviseren ten aanzien van de administratieve organisatie en daarin opgenomen maatregelen van interne controle.
Ook de wetgever heeft voor de accountant een taak weggelegd gezien. De accountant moet op grond van het Burgerlijk Wetboek verslag uitbrengen aan de raad van commissarissen en aan het bestuur. De nieuwe Wet computercriminaliteit heeft daaraan in artikel 2:393 lid 4 de verplichting toegevoegd daarbij ten minste melding te maken van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Het gaat om bevindingen van de accountant die zijn opgedaan in het kader van zijn jaarrekeningcontrole [Pasm93]. Pasmooy is van mening dat hiermee wordt aangegeven dat de eerste verantwoordelijkheid voor de bestrijding van computercriminaliteit bij de bestuurders van de onderneming ligt. Zoals het NIVRA-geschrift stelt begint de strafrechtelijke bescherming door de overheid daar waar de preventieve redelijke bescherming door individuen en organisaties zelf ophoudt [NIVR93]. De accountant kan hier vanuit zijn deskundigheid op het gebied van de administratieve organisatie en de interne controle nuttige diensten verrichten.

### De rol van de EDP-auditor

Ter voorkoming van computercriminaliteit dienen beveiligingsmaatregelen te worden getroffen (zie daarvoor de beschrijving van de rol van de EDP-auditor ten aanzien van privacy-bescherming).

### De rol van de jurist

De jurist kan in zijn functie als adviseur en onderhandelingspartner preventieve juridische maatregelen voorstellen. Hierbij kan worden gedacht aan

het deponeren van de broncode bij een onafhankelijk persoon of notaris (in het geval bijvoorbeeld virussen worden verspreid waardoor programma's worden gewist) of het uitdrukkelijk regelen van licenties (om iemand die inbreuk maakt op het intellectuele eigendomsrecht van een beschermd computerprogramma met de opzet dat programma commercieel te exploiteren, te kunnen aanpakken). Ook kan de jurist repressieve maatregelen voorstellen, zoals regelingen met betrekking tot garanties, exoneratiebepalingen in automatiseringscontracten en het sluiten van verzekeringsovereenkomsten.

## BEWIJS- EN BEWAARPLICHT

In toenemende mate wordt door het Nederlandse bedrijfsleven gebruik gemaakt van de elektronische uitwisseling van gegevens tussen computers, kortweg EDI. Welke gevolgen heeft deze elektronische uitwisseling voor het leveren van bewijs door middel van elektronische berichten en voor de wettelijke bewaarplicht van bedrijven?

Bewijs en bewaring hangen ten nauwste met elkaar samen. In een procedure zal het bewijs van een feit kunnen worden gehaald uit de boekhouding van één van de partijen. Om deze reden kan het van belang zijn dat bedrijven hun boekhouding een aantal jaren bewaren. Ook een aantal wetten stelt het bewaren van bepaalde bescheiden verplicht.
Zo legt artikel 6 van het Wetboek van Koophandel een ieder die een bedrijf uitoefent de verplichting op om 'naar de eischen van zijn bedrijf aanteekening te houden'. Lid 3 bepaalt vervolgens 'Hij is gehouden de boeken en bescheiden, waarin hij overeenkomstig het eerste lid aanteekening heeft gehouden, alsmede de balansen, de ontvangen brieven en telegrammen en afschriften van de uitgaande brieven en telegrammen tien jaar lang te bewaren'.
In artikel 2:10 lid 3 en 2:24 lid 1 BW is ten aanzien van rechtspersonen eveneens een bewaarplicht van tien jaar geformuleerd. Ook art. 54 Algemene Wet inzake Rijksbelastingen kent een bewaarplicht van tien jaar ten dienste van de belastingheffing.
Het niet voldoen aan de wettelijke bewaarplicht kan als gevolg hebben dat de bestuurder van een rechtspersoon in geval van faillissement aansprakelijk wordt gesteld. De wet stelt dat het bestuur dan zijn taak onbehoorlijk heeft vervuld en vermoed wordt dat onbehoorlijke taakvervulling een belangrijke oorzaak is geweest van het faillissement (zie art. 2:248 BW).
De vraag kan worden gesteld of de bewaarplicht ook geldt ten aanzien van moderne informatiedragers. Opgemerkt moet worden dat op dit moment een wetswijziging in voorbereiding is, die met name de oude regeling van het Wetboek van Koophandel moet moderniseren.[3] Ontvangen gegevens mogen eventueel op een ander medium worden vastgelegd. Voorwaarde is echter wel dat dit geschiedt met juiste en volledige weergave van de gegevens en dat de gegevens gedurende de hele bewaartijd binnen redelijke tijd leesbaar kunnen worden gemaakt.

Behalve de vraag of de bewaarplicht ook geldt ten aanzien van een moderne informatiedrager, kan de vraag worden gesteld of een elektronisch bericht als bewijs kan worden gebruikt.
Artikel 179 lid 1 van het Wetboek van Burgerlijke Rechtsvordering stelt dat in beginsel bewijs kan worden geleverd door alle middelen. Het tweede lid stelt dat de rechter vrij is in zijn waardering van dit bewijs (zogenaamde vrije bewijskracht).[4]
Partijen mogen deze wettelijke vrijheid (van de rechter) echter opzij zetten met een bewijsovereenkomst: bepaalde bewijsmiddelen kunnen zo worden uitgesloten of juist tot enig bewijs worden verheven. Ook kan de kracht van het bewijsmiddel in zo'n overeenkomst worden bepaald.

*Indien partijen geen bewijsovereenkomst hebben afgesloten, heeft computermateriaal vrije bewijskracht.*

Indien partijen geen bewijsovereenkomst hebben afgesloten, heeft computermateriaal dus vrije bewijskracht. De rechter zal aan de hand van de omstandigheden van het geval beslissen welke bewijskracht het computermateriaal toekomt. Hij zal rekening houden met de technische betrouwbaarheid van het middel en met name ook de mogelijkheid tot vervalsing. In veel gevallen zal de rechter zich (moeten) laten bijstaan door deskundigen.

### De rol van de accountant

De rechter kan voor een deskundig oordeel over de waardering van het computermateriaal als bewijsmiddel een accountant inschakelen. Zo kan een accountant aangeven of voldoende maatregelen in de administratieve organisatie zijn getroffen ter vergroting van de betrouwbaarheid van elektronische berichten [Graa91-2].
Behalve voor de rechter kan de accountant ten aanzien van deze maatregelen ook adviserend voor bedrijven optreden.
Tevens kan in verband met de wettelijke bewaarplicht ten aanzien van moderne informatiedragers de accountant voorstellen doen voor maatregelen die een juiste en volledige weergave van gegevens kunnen garanderen.

### De rol van de EDP-auditor

Behalve een accountant kan ook een EDP-auditor als deskundige voor de waardering van computermateriaal als bewijsmateriaal en in verband met de wettelijke bewaarplicht optreden.
Van belang voor de toe te kennen bewijskracht aan computermateriaal is onder andere in hoeverre in de geregistreerde gegevens mutaties kunnen worden aangebracht. Een EDP-auditor zou uitspraken kunnen doen over de betrouwbaarheid van het voor computergebruik bestemde informatiebe-

3. *Wetsontwerp 23024, nrs. 1-2: Wijziging van het Burgerlijk Wetboek, het Wetboek van Koophandel en enige andere wetten terzake van het voeren van een administratie, d.d. 13 februari 1993.*

4. *Slechts bij uitzondering wordt de rechter in de waardering van het bewijs gebonden. Zo levert een akte - behoudens tegenbewijs - verplicht volledig (dwingend) bewijs op tussen partijen van de inhoud van die akte (art. 184 lid 2 Rv): de rechter mag geen aanvullend bewijs verlangen.*

stand: zijn deze gegevens gecontroleerd door een gekwalificeerd persoon; welke maatregelen zijn genomen om vergissingen te voorkomen?; welke maatregelen zijn getroffen ten aanzien van fraude-preventie en fraude-ontdekking; is een logboek bijgehouden van gebruikers?; hoe zijn programma's beveiligd? etc. [Hidm93].
In verband met de wettelijke bewaarplicht kan de EDP-auditor maatregelen voorstellen die een juiste en volledige weergave van de gegevens en het leesbaar blijven van die gegevens kan garanderen.

**De rol van de jurist**

De jurist zal bij de beoordeling van geschillen of bij het opstellen van contracten steeds vaker te maken krijgen met elektronische berichtenuitwisseling.
Bij de beoordeling van geschillen zal de jurist in zijn rol als rechter elektronische berichten op hun bewijskracht moeten waarderen. De jurist in zijn rol als adviseur kan een bewijsovereenkomst opstellen, waarin wordt afgesproken dat de bewijsmiddelen van (één van) de deelnemers aan een EDI-systeem dwingend bewijs opleveren tot het tegenbewijs is geleverd [Schu92]. Voor een antwoord op de vraag welke bewijsmiddelen dwingend bewijs zullen opleveren, zal de jurist een EDP-auditor kunnen inschakelen die hem adviseert over de betrouwbaarheid van het bewijsmiddel.

## GESCHILLENBESLECHTING

Bij het oplossen van automatiseringsgeschillen krijgt men te maken met vaak gemengde (zowel juridische als technische) problemen. Voor het oplossen van de juridische problemen zijn juristen - uiteraard - de aangewezen personen. Voor het oplossen van de technische of organisatorische aspecten van de problemen zullen deskundigen, zoals een EDP-auditor of accountant, moeten worden ingeschakeld.

Een voorbeeld: Een software-leverancier ontwikkelt, in opdracht en in samenwerking met de klant, een bepaald systeem. Na verloop van tijd, het systeem is in gebruik bij de klant, wil de leverancier met het systeem de markt op. De klant echter is van mening dat dat niet mogelijk is, omdat het systeem 'van hem' is. Hij heeft immers meegewerkt aan de ontwikkeling van het systeem en er veel kosten voor gemaakt. Ook heeft hij de leverancier toch betaald! Over de eigendomsrechten (de auteursrechten in dit geval) is niets geregeld. Er wordt een jurist ingeschakeld. Omdat in de contracten niets is geregeld omtrent de auteursrechten, geldt de wet. De wet zegt dat de auteursrechten toekomen aan de maker van het systeem. Daarvoor gelden de criteria: oorspronkelijkheid en een eigen zelfstandige creatieve inbreng. Of sprake is geweest van een zelfstandige creatieve inbreng in het ontwikkelingsproces moet worden aangegeven door een EDP-auditor. Daarvoor ontbreekt meestal de technische of automatiseringskennis bij een jurist. De jurist heeft dus bij de oplossing van dit conflict een EDP-auditor nodig.

Er zijn verschillende vormen van conflictoplossing te onderscheiden [Muts93]. Naast de mogelijkheid het geschil voor te leggen aan de overheidsrechter, bestaan er alternatieve methoden om geschillen te beslechten, zoals problem solving-onderhandelen, mini-trial, bindend advies en arbitrage.
In geval van problem solving-onderhandelen spoort een derde de knelpunten op en confronteert de betrokken partijen met hun gedrag en helpt aan te geven hoe de problemen kunnen worden opgelost, zodat partijen onderling tot een vergelijk kunnen komen.
In een mini-trial tracht een derde partijen tot elkaar te brengen door oplossingsvoorstellen te evalueren of zelf voorstellen te doen. Indien partijen een aanbeveling tot minnelijke schikking niet wensen te accepteren, betekent dit het einde van de mini-trial. De derde blijft een adviseur en kan dus wel drang maar geen dwang uitoefenen.
Van een bindend advies is sprake wanneer partijen zijn overeengekomen, hetzij naar aanleiding van een gerezen geschil, hetzij met het oog op geschillen die in de toekomst zouden kunnen ontstaan, hun onenigheid te laten beslissen door een derde die daartoe advies uitbrengt. De partijen verklaren dan bij voorbaat zich jegens elkaar gebonden te achten aan dat advies. Een dergelijk advies heeft geen rechtskracht. Indien een partij zich er niet aan wenst te houden, kan men derhalve alsnog naar de rechter stappen.
Grondslag voor arbitrage is een daartoe strekkende overeenkomst van partijen. In die overeenkomst hebben partijen bepaald dat geschillen aan particuliere scheidslieden (arbiters) worden voorgelegd. De uitspraak die de arbiters voor een geschil geven, heeft de status van een vonnis dat rechtskracht heeft en met behulp van overheidssteun kan worden verwezenlijkt.
Wanneer partijen niet anders zijn overeengekomen, worden geschillen door de overheidsrechter beslecht. Beroep op de rechter is niet altijd adequaat. Gebrek aan deskundigheid van de overheidsrechter en de vaak lange procedures kunnen op onoverkomelijke bezwaren stuiten in de automatiseringsbranche. Automatiseringsconflicten lenen zich meer voor de alternatieve manieren om geschillen te reguleren.

**De rol van de accountant en de EDP-auditor**

Zowel de accountant als de EDP-auditor kan optreden als deskundige bij bemiddeling van conflicten. Zo kan de accountant aangeven of er in de administratieve organisatie voldoende maatregelen zijn getroffen ter voorkoming van bijvoorbeeld manipulatie van gegevens, en kan de EDP-auditor een oordeel geven over de bewijskracht van een elektronisch bericht.

**De rol van de jurist**

Enerzijds zal de jurist de leiding dragen van de procedure, voor welke methode van geschillenbeslechting ook is gekozen. Hij zal moeten waken voor een zorgvuldige procesgang en zal de rechtswaarborgen moeten bewaken, zoals de beginselen van hoor en wederhoor. Anderzijds is hij er voor

de juridische kwesties, zoals algemene voorwaarden, exoneratie (vrijtekening), financiering, leveringscondities (eigendomsvoorbehoud), termijnen, distributie-afspraken, vertegenwoordiging en dienstverlening.

## SAMENVATTING

In dit artikel is een overzicht gegeven van de verschillende raakvlakken tussen de disciplines accountancy, EDP-auditing en recht. Op verschillende terreinen liggen deze raakvlakken, zoals privacy-bescherming, computercriminaliteit, escrow, Service Level Agreements, bewijs- en bewaarplicht, software-bescherming en geschillenbeslechting. Enkele onderwerpen zijn er uitgelicht en daarvan is de verwevenheid tussen de drie vakgebieden nader beschreven.
Het is van belang dat de aandachtspunten door de accountant dan wel de EDP-auditor of jurist in ieder geval onderkend worden, zodat deze kunnen doorverwijzen naar specialisten wanneer hun kennis tekort schiet. Gezien de grote verwevenheid tussen de drie vakgebieden is een multidisciplinaire samenwerking onontkoombaar.

## LITERATUUR

[Esch92] R.E. van Esch, *Electronic Data Interchange, Het elektronisch identificatiemiddel en volmacht*, 33 NJB 1992.

[Fran93] H. Franken, *Wet computercriminaliteit sinds 1 maart 1993 in werking*, Dossier Account, Onderneming & Automatisering, 1993.

[Graa91-1] F. de Graaf, *Hoofdstukken informaticarecht*, Alphen aan den Rijn 1991, p. 237.

[Graa91-2] I.M.A de Graaf-Hinfelaar, A.M.Ch.Kemna, *De bewijskracht van computermateriaal in de civiele procedure*, Compact 1991/1, p. 9.

[Hidm93] T.R. Hidma, *Bewaren en bewijzen met moderne informatietechnieken*, Dossier Account, nr. 12, 1993.

[Hors93] H.F. van der Horst RE, *Illegale software: voorkomen is beter dan genezen*, in: Twintig over informatietechnologie en recht, redactie A.M.Ch. Kemna en A.W. Neisingh, Samsom BedrijfsInformatie, Alphen aan den Rijn/Zaventem 1993.

[Jaco93] R.A. s'Jacob, *Strafbaarstelling van computermisbruik, Een analyse van de Wet computercriminaliteit*, in: Twintig over informatietechnologie en recht, redactie A.M.Ch. Kemna en A.W. Neisingh, Samsom BedrijfsInformatie, Alphen aan den Rijn/Zaventem 1993.

[Knaa93] P.A.J. van der Knaap, *Een invulling van de beveiligingseis uit de Wet Persoonsregistraties*, in: Twintig over informatietechnologie en recht, redactie A.M.Ch. Kemna en A.W. Neisingh, Samsom BedrijfsInformatie Alphen aan den Rijn/Zaventem 1993.

[Muts93] F.V.B.M. Mutsaerts, *Geschillenbeslechting in de automatiseringsbranche*, in: Twintig over informatietechnologie en recht, redactie A.M.Ch. Kemna en A.W. Neisingh, Samsom BedrijfsInformatie, Alphen aan den Rijn/Zaventem 1993.

[NIVR91] NIVRA-geschrift nr. 58, *Automatisering en controle, deel VIII. Privacy-bescherming; de gevolgen voor organisaties en de rol van de accountant.*

[NIVR93] NIVRA-geschrift nr. 62, *Automatisering en controle, deel IX. Computercriminaliteit: de wetgeving, de gevolgen voor bedrijven en de accountant.*

[Pasm93] J. Pasmooy, *Computercriminaliteit, 'Voorkomen is beter dan genezen'*, De Accountant nr. 11, juli/augustus 1993, p. 781.

[Rood92] J. Roodnat, *Wet computercriminaliteit, Extra beveiligingsmaatregelen en een verandering in de rol van de accountant?*, De Accountant nr. 3, november 1992.

[Schu92] G.J. Schuringa en R.E. van Esch, *Beveiligingsaspecten en juridische aspecten als communicerende vaten*, Compact 1992/4.

*Mw.mr.drs. A.W. Duthler Is sinds februari 1993 werkzaam bij KPMG Klynveld EDP Auditors als adviseur informaticarecht. In deze functie houdt zij zich bezig met de juridische aspecten van automatisering en de connecties daarvan met EDP-auditing. Tot haar werkzaamheden behoren onder andere het beoordelen van automatiseringscontracten, het adviseren inzake privacy-wetgevingen, de Wet computercriminaliteit en EDI. Zij studeerde Bestuurskunde aan de Technische Universiteit Twente en Rechten aan de Rijksuniversiteit Leiden.*

# Automatiseringsrisico's, verzekeringen en de rol van de accountant

Drs. G.J.W.C. Vankan

**Verzekeringen vormen het sluitstuk van het stelsel van maatregelen om schade als gevolg van verstoringen in de geautomatiseerde gegevensverwerking te beperken. In Nederland is het aanbod van computerverzekeringen echter nog betrekkelijk beperkt, en is de diversiteit aan polisvoorwaarden groot. Voor de accountant of EDP-auditor die de cliënt wil adviseren over de toereikendheid van de af te sluiten of afgesloten computerverzekeringen, biedt dit artikel een heldere uiteenzetting over praktische mogelijkheden, beperkingen en bijzondere polisvoorwaarden.**

## INLEIDING

Dat het gebruik van automatisering ter ondersteuning van bedrijfsprocessen niet zonder risico's is, mag als bekend worden verondersteld. In toenemende mate verschijnen publikaties waarin melding wordt gemaakt van bedrijven die schade hebben geleden als gevolg van het (tijdelijk) niet of incorrect functioneren van geautomatiseerde informatiesystemen [Kear79], [Vrij86].

Het behoort tot de toegevoegde waarde van de accountant om zijn/haar cliënten te informeren omtrent de bedreigingen waaraan een organisatie blootstaat alsmede aan te geven op welke wijze een organisatie met deze bedreigingen kan omgaan. Ook van een interne accountantsdienst wordt veelal verwacht dat hij hierover aan de bedrijfsleiding rapporteert.
Vanuit dit oogpunt treft men het onderwerp verzekeringen dan ook vaak aan op de werkprogramma's van de accountant (intern dan wel extern). De bedoeling hiervan is dat de accountant inzicht krijgt in de risico's die een organisatie loopt en in de mate waarin een organisatie tegen deze risico's is gedekt. Hiertoe dient de accountant antwoord te geven op de volgende drie vragen:

- Zijn de mogelijke risico's voldoende gedekt?
- Is de organisatie in staat schade als gevolg van risico's die niet bij derden zijn verzekerd, zelf te dragen (voorziening, liquiditeit)?
- Wordt aandacht besteed aan de naleving van door verzekeraars gestelde voorwaarden?

Met betrekking tot een groot aantal risico's (brandschade, inbraak, kredietrisico, valutarisico, wettelijke aansprakelijkheid, enz.) zal de accountant op basis van zijn algemene kennis en de kennis van de organisatie een adequaat antwoord op bovenstaande vragen kunnen geven.

Het gebruik van geautomatiseerde gegevensverwerking brengt additionele risico's met zich mee. Zowel de cliënt als de Nederlandse wetgever (Wet computercriminaliteit) verwacht dat de accountant ook over deze risico's een uitspraak doet. De accountant zal daarom bekend moeten zijn met de mogelijke bedreigingen die gepaard gaan met het gebruik van automatisering en met de door de markt geboden mogelijkheden ter dekking van deze risico's.
In dit artikel wordt inzicht gegeven in de met de automatisering samenhangende risico's en de op de markt verkrijgbare verzekeringsprodukten. Daarnaast wordt aangegeven op welke wijze de accountant, al dan niet in samenwerking met de EDP-auditor, nadere invulling kan geven aan het onderwerp verzekeringen in relatie tot automatisering.

## AUTOMATISERING EN RISICO'S

Het gebruik van geautomatiseerde gegevensverwerking betekent voor een organisatie veelal dat er wijzigingen plaatsvinden in de inrichting/structurering van de bedrijfsprocessen en dat er gebruik wordt gemaakt van nieuwe of additionele mensen en middelen. Praktisch vertaald betekent dit dat een organisatie zal overgaan tot de aanschaf van:
- hardware (computer, opslagmedia, terminals, printers);
- software (besturings- en toepassingsprogrammatuur);
- infrastructuur (computerruimte, netwerk).

Daarnaast zal een herstructurering en/of uitbreiding plaatsvinden van de interne organisatie (en de daarmee samenhangende AO/IC). Al naargelang de grootte van de organisatie kunnen de volgende nieuwe (functionele) organisaties ontstaan:
- gegevensverwerkende organisatie (rekencentrum);
- systeemontwikkelingsorganisatie (ontwikkelen en onderhouden van programmatuur);
- gewijzigde gebruikersorganisatie.

Deze nieuwe elementen brengen naast een (verwachte) hogere efficiëntie en effectiviteit echter ook nieuwe of andere bedreigingen met zich mee. Deze bedreigingen kunnen als volgt kort worden samengevat:
- materiële (lees: fysieke) schade aan apparatuur en opslagmedia;
- bedreiging van de continuïteit van de bedrijfsprocessen bij uitval van de geautomatiseerde gegevensverwerking;
- verlies van programmatuur en data als gevolg van materiële[1] en niet-materiële beschadiging van de apparatuur of de gegevensdragers.

## RISICO'S EN MAATREGELEN

Ter voorkoming of beperking van de schade als gevolg van het manifest worden van de in de voorgaande paragraaf genoemde bedreigingen, kan een organisatie maatregelen treffen. Deze maatregelen kunnen worden onderverdeeld in preventieve, detectieve, repressieve en correctieve maatregelen [Velt91]. Deze categorieën maatregelen kunnen vervolgens weer worden onderscheiden in:
- organisatorische;
- fysieke;
- hardware-matige; en
- software-matige

maatregelen.

De bedrijfsleiding zal op basis van een kosten/baten-afweging bepalen in hoeverre het treffen van maatregelen bijdraagt aan de realisatie van de ondernemingsdoelstellingen en opweegt tegen mogelijke schade. In deze kosten/baten-analyse zal er een moment komen dat het treffen van verdere maatregelen niet meer kosteneffectief wordt geacht of dat het treffen van verdere maatregelen niet meer mogelijk is door gebrek aan (financiële) middelen. De bedrijfsleiding wordt op dat moment geconfronteerd met een bepaald "restrisico" (zie figuur 1).

Een organisatie kan ten opzichte van deze restrisico's in de volgende posities verkeren:

- De organisatie kiest doelbewust voor het zelf dragen van het risico. Op basis van de inschatting van het risico in combinatie met de financiële draagkracht van de onderneming acht de bedrijfsleiding het acceptabel het risico zelf te dragen. Eventuele schade zal dan in de meeste gevallen uit het operationele budget of uit een reservering worden gedekt.

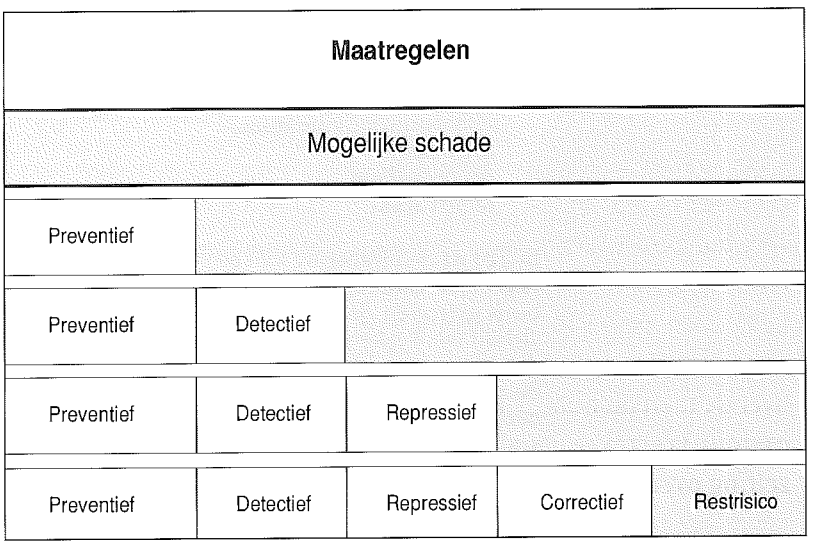
- De kosten van een verzekering (hoogte van de premie) kunnen niet door de organisatie worden gedragen. Verzekeren van het risico is derhalve om financiële redenen niet mogelijk. De organisatie is gedwongen het risico zelf te dragen.

- Het risico is niet verzekerbaar. Deze situatie kan ontstaan wanneer de bedreigingen die ten grondslag liggen aan het risico in geen enkele verzekering zijn opgenomen (bijvoorbeeld aardbevingen, molest) doordat de verzekeraars het risico zo hoog inschatten dat zij niet bereid zijn een polis af te sluiten.

- Het restrisico kan extern worden gefinancierd (gedekt) door het afsluiten van een verzekering.

In de praktijk zullen bovenstaande situaties niet zwart/wit bestaan. In veel gevallen zullen gedeelten van de (rest)risico's door de organisatie (kunnen) worden gedragen, en andere gedeelten extern worden gedekt. Het fenomeen 'eigen risico' in verzekeringen is hier een voorbeeld van. De juiste verhouding van zelf te dragen risico's en extern te dekken risico's (indien mogelijk) zal door de ondernemingsleiding wederom op basis van een kosten/nut-afweging worden bepaald.

*Figuur 1. Maatregelen en risico's.*




1. *Materieel in de zin van fysiek. Het verzekeren van schade als gevolg van niet-materiële schade (bijvoorbeeld virusbesmettingen en dergelijke) is niet bij elke verzekering mogelijk.*

Het bepalen van de aard en de omvang (kwalificeren en kwantificeren) van het restrisico is voor de individuele onderneming en voor de accountant een moeilijke en tijdrovende zaak. Dit is echter ook niet noodzakelijk. Voor het bepalen van het restrisico kan een verzekeraar namelijk uitkomst bieden.

*Het is van belang te onderkennen dat ten behoeve van de bepaling van de restrisico's niet alleen primaire systemen van belang zijn.*

Aan de hand van statistische informatie kunnen verzekeraars namelijk bepalen welk (rest)risico, afhankelijk van de branche en de organisatie, in een bepaalde situatie aanwezig zal zijn. Dit risico kunnen verzekeraars op basis van het principe van risicospreiding [Shar85] tegen relatief lage premies afdekken.

## ACCOUNTANT EN AUTOMATISERINGSRISICO'S

Om als accountant een advies en/of oordeel inzake de mogelijk te verzekeren risico's te kunnen geven is een onderzoek vereist dat alle vlakken raakt waar zich bedreigingen kunnen manifesteren. Gezien de hiervoor vereiste specialistische kennis is het veelal raadzaam hiervoor een deskundige (EDP-auditor) in te schakelen.

Een door een EDP-auditor uitgevoerde continuïteits-audit bevat als standaardaandachtspunt een globale beoordeling van de verzekeringsportefeuille met betrekking tot de automatisering. Daarnaast kan er gekozen worden voor een diepgaande beoordeling van de verzekeringsportefeuille, waarbij aandacht aan de volgende aspecten dient te worden besteed:

- omgeving;
- gegevens;
- apparatuur en gegevensdragers;
- applicaties;
- systeemprogrammatuur;
- organisatie;
- documentatie;
- registraties.

Indien na de uitvoering van een continuïteits-audit blijkt dat een organisatie zodanige maatregelen heeft getroffen dat men binnen de gewenste hersteltijd weer operationeel kan zijn, betekent dit niet dat er geen schade zal zijn. Met de uitvoering van de procedures om binnen de uitvaltijd operationeel te zijn, zijn veelal hoge kosten gemoeid. Deze kosten kunnen met behulp van verzekering tot een minimum worden beperkt.
Bij het uitvoeren van een continuïteits-audit wordt het meest primaire (vitale) systeem als uitgangspunt genomen voor het uitvoeren van de audit. Het is echter van belang te onderkennen dat ten behoeve van de bepaling van de restrisico's niet alleen primaire systemen van belang zijn. Ook systemen met een ondersteunende functie (bijvoorbeeld personeelsadministratie, salarisadministratie, marketingsysteem) kunnen als gevolg van bepaalde gebeurtenissen een belangrijke schadepost betekenen. Bovendien vertonen systemen vaak een onderlinge samenhang/interactie waarbij de uitval (of het disfunctioneren) van het ene (ondersteunende) systeem, de uitval van een ander, wellicht vitaal systeem kan betekenen.

## VERZEKERINGEN ALS SLUITSTUK

Uit het voorgaande blijkt dat het afsluiten van verzekeringen gezien kan worden als het sluitstuk van een stelsel van maatregelen ter voorkoming of beperking van schade. Om vast te stellen welke verzekeringen als "adequaat" sluitstuk in aanmerking komen is enige kennis van de op de markt aangeboden verzekeringen noodzakelijk.

Reeds vele jaren bieden nationale en internationale verzekeringsmaatschappijen de zogenaamde 'computerverzekeringen' aan. De aangeboden produkten vertonen echter wat betreft opzet en inhoud een aantal belangrijke verschillen. Om enig inzicht te geven in deze verscheidenheid aan produkten wordt in deze paragraaf een beeld gegeven van enkele verzekeringsprodukten die op de Nederlandse markt (vanaf december 1992) verkrijgbaar zijn.

### Historie

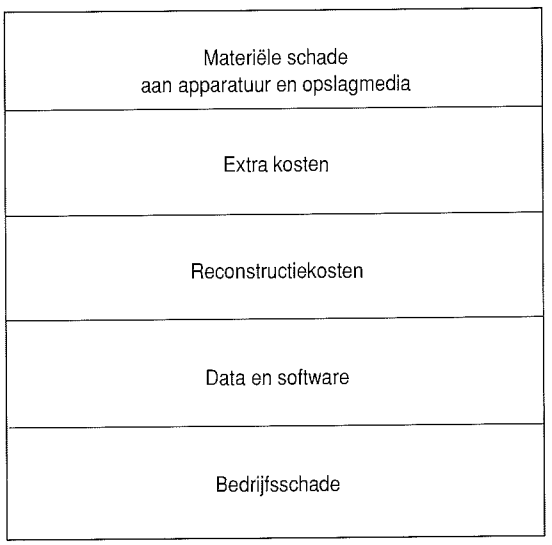
In de eerste jaren na de introductie van de computer betekende de aanschaf van computers en bijbehorende randapparatuur een zeer grote investering. Een dergelijke investering werd evenals de rest van de 'inventaris' verzekerd geacht onder de dekking van een inboedelverzekering, maar in de meeste gevallen werd computerapparatuur niet door de reguliere verzekering gedekt. Derhalve werden al snel verzekeringen aangeboden waarmee deze apparatuur wel kon worden verzekerd.

De verzekering tegen materiële schade werd uitgebreid met de mogelijkheid tot het verzekeren van kosten van extra arbeid en inspanning die nodig zijn om de bedrijfsprocessen tijdelijk handmatig voort te zetten indien er sprake is van computeruitval.
Al vlug besefte men dat niet alleen de materiële schade aan de apparatuur van belang was. Door het goedkoper worden van de hardware-componenten maakt de software (toepassingsprogrammatuur) een steeds belangrijker deel uit van de totale investeringen in automatisering. Het verlies van programmatuur werd spoedig gedekt door een extra rubriek 'reconstructiekosten' in een aantal verzekeringsprodukten. Hiermee worden de kosten gedekt welke gemaakt worden om de programmatuur (hetzij standaard hetzij maatwerk) en

de gegevens weer in oorspronkelijke vorm terug te brengen. Doch ook hier is er veelal alleen maar sprake van een uitkering indien de programmatuur en/of data teniet is gegaan door fysieke oorzaken.
Met name ten aanzien van magnetische opslagmedia (tapes, diskettes, hard disks, disk packs) bestaat een groot aantal bedreigingen dat kan resulteren in verminking/vernietiging van programmatuur en data zonder dat dit fysieke beschadiging met zich meebrengt.

**De computerverzekering**

De verzekering welke schade dekt met betrekking tot geautomatiseerde gegevensverwerking wordt veelal 'computerverzekering' genoemd. De lading die door deze vlag wordt gedekt, kan per aangeboden produkt op essentiële punten verschillen. Zo is de schade aan programmatuur en gegevens door niet-materiële beschadigingen recent in een aantal verzekeringen als dekkingsgebied opgenomen. Onder deze niet-materiële schade wordt verstaan 'verminking en verlies van gebruikersprogrammatuur, zich op informatiedragers bevindende informatie en opslagcapaciteit op informatiedragers welke niet gepaard gaat met beschadiging van de dragers van de informatie of de gebruikersprogrammatuur'.
In de bestaande verzekeringsprodukten geldt in het algemeen een indeling van dekkingsgebieden in een aantal standaardcategorieën. Een computerverzekering omvat veelal verscheidene van de in figuur 2 aangegeven rubrieken. De dekking kan echter per rubriek nog verschillen.




*Figuur 2. Indeling dekkingsgebieden computerverzekeringen.*

In de volgende subparagrafen zal per rubriek worden aangegeven wat men onder het dekkingsgebied verstaat, welke aandachtspunten hierbij van belang zijn en welke belangrijke uitsluitingen er worden gehanteerd. Hierbij wordt uitgegaan van een aantal algemene op de markt verkrijgbare verzekeringsprodukten. Het is derhalve noodzakelijk dat een verzekeringsprodukt op genoemde aspecten afzonderlijk wordt onderzocht alvorens kan worden vastgesteld of dit produkt voor een bepaalde situatie/organisatie geschikt is.

*Apparatuur en opslagmedia*
Als dekkingsgebied gelden veelal alle apparatuur (centrale verwerkingseenheid en randapparatuur) en alle opslagmedia. Schade wordt vergoed tegen vervangingswaarde waarbij een bedrag in mindering wordt gebracht voor afschrijving en restwaarde.
Bepaling van deze vervangingswaarde kan een probleem opleveren indien er sprake is van sterk verouderde apparatuur. Indien de verzekerde apparatuur niet meer wordt geproduceerd, is een vergelijkbare machine wellicht niet moeilijk te vinden. De aanschaf van een dergelijke vergelijkbare machine zal echter veelal met zich meebrengen dat een groot deel van de randapparatuur (beeldschermen, toetsenborden, bekabeling, printers, modems, disk/tape-units) alsmede de besturingsprogrammatuur en mogelijk de applicatieprogrammatuur vervangen dienen te worden zonder dat deze beschadigd zijn. Aan de wijze waarop een dergelijke schade wordt gedekt, dient bij het afsluiten van een polis specifiek aandacht te worden besteed.
Bij deze rubriek geldt veelal als uitsluiting alle schade welke volgens de condities van het onderhoudscontract voor rekening van de leverancier/fabrikant komt of zou zijn gekomen. Uitsluiting van schade als gevolg van brand en/of diefstal is mogelijk.

*Extra kosten*
Onder de dekking van de rubriek 'extra kosten' (ook wel meerkosten genoemd) valt de vergoeding van extra kosten die door de verzekerde worden gemaakt om de normaal met behulp van de onder de rubriek 'apparatuur en opslagmedia' verzekerde objecten uit te voeren werkzaamheden, tijdens de periode van uitval te kunnen blijven uitvoeren. Voorbeelden van deze kosten zijn:
- huur van vervangende apparatuur (uitwijk);
- transport naar uitwijklocatie;
- verblijfkosten op uitwijklocatie;
- salaris van extra personeel.

Alhoewel in geen van de aangeboden verzekeringsprodukten in deze rubriek een specificatie per toepassing/applicatie kan worden gemaakt, lijkt het voor de hand liggend de mogelijkheid te bieden deze rubriek te beperken tot door de bedrijfsleiding aangegeven specifieke toepassingen. Bij deze verzekeringsprodukten wordt geen onderscheid gemaakt tussen integrale uitwijk (alle applicaties inclusief bijbehorende gegevens) of partiële uitwijk (deelsystemen of individuele applicaties, met bijbehorende gegevens). Zoals bekend mag worden verondersteld, zijn er voor een integrale uitwijk andere procedures/acties en beheersingsmaatregelen nodig dan voor een partiële uitwijk.

*Reconstructiekosten*
Onder de dekking van de rubriek 'reconstructiekosten' valt de vergoeding van kosten welke door

de verzekerde worden gemaakt om bij verlies van gegevens en programmatuur deze zodanig te reconstrueren dat de normaal met behulp van de onder de rubriek 'apparatuur en opslagmedia' verzekerde objecten uit te voeren werkzaamheden, na de periode van uitval kunnen worden voortgezet. Voorbeelden van deze kosten zijn:
- huur van vervangende apparatuur ten behoeve van reconstructiewerkzaamheden;
- salaris van extra personeel ten behoeve van de reconstructie;
- programmeerkosten ten behoeve van reconstructieprogrammatuur.

*De eisen die aan de verzekerde worden gesteld, zijn bij de aangeboden verzekeringsprodukten vaak zeer algemeen en globaal van aard.*

Ook hier is van belang dat alleen reconstructiekosten worden vergoed indien er sprake is van gegevensverlies als gevolg van een materiële beschadiging van de gegevensdragers als gevolg van een onder de rubriek 'apparatuur en opslagmedia' genoemde gebeurtenis.
In tegenstelling tot wat vaak wordt gedacht, heeft deze rubriek geen betrekking op de reconstructie van apparatuur en computerruimten. Deze kosten worden veelal gedekt onder één van de eerder behandelde rubrieken.

*Data en software*
Als uitbreiding op de rubriek 'reconstructiekosten' is bij verschillende verzekeringsprodukten de rubriek 'data en software' toegevoegd. Het is mogelijk dat deze rubriek wordt gehanteerd als vervanging van de rubriek 'reconstructiekosten'.
In tegenstelling tot de rubriek 'reconstructiekosten' biedt de rubriek 'data en software' tevens dekking voor reconstructiekosten van data en programmatuur wanneer er geen sprake is van verlies als gevolg van een materiële beschadiging van de gegevensdragers. Onder deze rubriek wordt ook schade gedekt als gevolg van:
- computervirussen[2], Trojan horses en wormen;
- opzettelijke schade als gevolg van sabotage, data- of programmamanipulatie;
- elektrostatische lading, magnetische en elektromagnetische storing;
- stroomuitval;
- fouten van de operator.

Het is mogelijk dat deze rubriek beperkt is tot niet in ontwikkeling zijnde programmatuur. Programma's die in een systeemontwikkelingsafdeling worden ontwikkeld, zijn derhalve niet altijd in deze rubriek gedekt. Indien dit het geval is dient er extra aandacht te worden besteed aan de backup van de in ontwikkeling zijnde programmatuur.
Indien deze rubriek in de verzekering wordt opgenomen, is het regelmatig veilig stellen van programmatuur en data alsmede het gebruik van virusdetectieprogrammatuur veelal een vereiste.

*Bedrijfsschade*
Onder deze rubriek wordt veelal gedekt de bedrijfsschade waaronder wordt verstaan de derving van winst en de vaste kosten indien de bedrijfsvoering geheel of gedeeltelijk tot stilstand is gebracht of storing ondervindt.
Deze rubriek is vooral van belang voor bedrijven die in grote mate afhankelijk zijn van de continuïteit van de geautomatiseerde gegevensverwerking en niet over de middelen beschikken om op adequate wijze de continuïteit van deze gegevensverwerking te waarborgen. Bij het opnemen van deze rubriek in de verzekering dient vooraf te worden bepaald voor welke termijn de uitkering zal gelden. Ter voorkoming van onder- of oververzekering dient per situatie te worden beoordeeld in hoeverre deze rubriek overlap/verschil vertoont met de bestaande standaard-bedrijfsschadeverzekeringen (dit geldt in wezen voor elk dekkingsgebied).

*Polisvoorwaarden*
Zoals in artikel 293 lid 1, Wetboek van Koophandel staat vermeld, is 'de verzekerde verplicht om alle vlijt en naarstigheid in het werk te stellen teneinde schade te voorkomen of te verminderen, met als sanctie schadevergoedingsplicht jegens de verzekeraar'.

Bovenstaand artikel is in de hedendaagse verzekeringswereld vertaald in de polisvoorwaarden. Hierin zijn de voorwaarden vastgelegd waaraan moet worden voldaan alvorens de verzekeraar tot (gehele of gedeeltelijke) schadevergoeding zal overgaan.
Tevens wordt aan de hand van de mate waarin aan deze voorwaarden wordt voldaan, bepaald of de verzekeraar bereid is de verzekering aan te gaan en tegen welke premie dit zal geschieden.
Met betrekking tot de computerverzekeringen waarbij programmatuur, data en bedrijfsschade zijn meeverzekerd, kunnen deze voorwaarden in de volgende categorieën worden ingedeeld:
- fysieke beveiliging van de computerruimte;
- onderhoud van apparatuur;
- opslag en beheer van programmatuur en data;
- logische beveiliging van de toegang tot programmatuur en data;
- backup, restart en recovery.

Na bestudering van enkele van de aangeboden verzekeringsprodukten kan worden opgemerkt dat de eisen welke gesteld worden aan de verzekerde vaak zeer algemeen en globaal van aard zijn. Een nadere invulling door de verzekeraar, de verzekerde of een deskundige is hier gewenst.
Om op een adequate wijze invulling te geven aan deze voorwaarden is enige deskundigheid op het gebied van automatisering, organisatie en verzekeringen gewenst. Om te kunnen vaststellen of de verzekerde aan de gestelde eisen voldoet zal de verzekeraar derhalve gebruik maken van een eigen deskundige of een externe deskundige inschakelen. Indien de verzekerde over deze invulling geen

2. *Volgens Algemene verzekeringsvoorwaarden ME 02, Interlloyd schade, Computer-Softwareverzekering:*
***virus:*** *"een aantal instructies die in staat zijn zich (eventueel in gewijzigde vorm) in een ander programma te kopiëren. Het is geen onafhankelijk proces, maar 'besmet' bestaande programma's. Het kan instructies bevatten die verschillende soorten schade aan het systeem aanrichten."*
***worm:*** *"een programma of een aantal programma-onderdelen dat zich vanzelf via een netwerk van computer tot computer vermenigvuldigt. In tegenstelling tot een virus komt een worm als onafhankelijk proces voor."*
***Trojan horse:*** *"een programma waaraan, naast de opgegeven en beschreven functies, bewust functies zijn toegevoegd met het oogmerk de software te manipuleren."*

overeenstemming met de verzekeraar kan bereiken, kan ook hij gebruik maken van een externe deskundige.

Naast het concreet invullen van de door de verzekeraar gestelde eisen (polisvoorwaarden) is het ook van belang dat deze invulling ondersteund wordt door een stelsel van beheersingsmaatregelen.
Zo zal het verrichten van onderhoud op de hardware pas aangetoond kunnen worden als:
- er contracten aanwezig zijn;
- deze contracten op een veilige (tegen calamiteiten beschermde) plaats zijn opgeborgen;
- alle hardware geregistreerd is;
- nieuw aangeschafte apparatuur in de registraties wordt opgenomen en aan de verzekering wordt doorgegeven.

Zo zal de logische beveiliging van gegevens en programmatuur pas effectief worden geacht als:
- de invoer, het wijzigen en het gebruik van autorisaties geschiedt volgens adequate procedures;
- registraties worden bijgehouden van de (soorten) gegevens en programmatuur.

De verzekeraars formuleren geen eisen ten aanzien van de benodigde beheersingsmaatregelen. Dit betekent dat het in de praktijk invullen van de (vage) eisen van de verzekeraar wellicht onvoldoende is om de hiermee nagestreefde doelen te bereiken. Dit zou kunnen betekenen dat in geval van schade de verzekeraar niet tot uitkering overgaat omdat de invulling van de gestelde polisvoorwaarden als onvoldoende wordt beschouwd. Het ondersteunen van de getroffen maatregelen door aanvullende beheersingsmaatregelen is derhalve noodzakelijk.

Met name in schadegevallen zal de verzekeraar willen vaststellen of door de cliënt aan de gestelde polisvoorwaarden is voldaan. Mogelijk zal hierbij een beroep op de accountant worden gedaan. Bij gebrek aan deskundigheid kan een EDP-auditor de accountant hierbij ondersteunen. De accountant zal in samenwerking met de EDP-auditor in staat zijn de verzekeraar een onafhankelijk oordeel te geven over de wijze waarop de organisatie de gestelde voorwaarden heeft ingevuld.
Het verdient aanbeveling om een dergelijk oordeel te baseren op een periodiek (bijvoorbeeld jaarlijks) onderzoek van de organisatie van de verzekerde. Hierdoor krijgt de verzekeraar een betrouwbaarder beeld van diens organisatie. Daarnaast stuit het uitvoeren van een onderzoek na melding van een schadegeval op enkele bezwaren:
- de organisatie/omgeving kan zodanig ontregeld of beschadigd zijn dat een onderzoek niet meer mogelijk is;
- de organisatie heeft de mogelijkheid om alsnog ervoor te zorgen dat aan de gestelde voorwaarden wordt voldaan alvorens de schade te melden.

*Overige aandachtspunten*
Uit geen van de onderzochte verzekeringsprodukten wordt duidelijk in hoeverre schade als gevolg van uitval/beschadiging van apparatuur en/of programmatuur van derden (bijvoorbeeld huurlijnen van de PTT, Value Added Network Services (VAN's), geleasete apparatuur en programmatuur, gebruik extern rekencentrum) in de dekkingsgebieden is opgenomen.
De praktijk leert dat het gebruik van deze dienstverlening door derden in de automatisering steeds meer in opkomst is. Hierdoor zal de continuïteit van de geautomatiseerde gegevensverwerking in toenemende mate afhankelijk worden van diensten van derden.

*De continuïteit van de geautomatiseerde gegevensverwerking zal in toenemende mate afhankelijk worden van diensten van derden.*

Van belang is dat bepaald wordt wie in gevallen van storingen, calamiteiten en/of beschadiging verantwoordelijk is voor zowel de directe schade als de gevolgschade. Het is niet uitgesloten dat een deel van deze dienstverleners zich met behulp van contractbepalingen aan deze aansprakelijkheid zal onttrekken. De wijze waarop verzekeraars met deze problematiek omgaan is wellicht een onderwerp voor nadere studie.

## RISICOBEWUSTZIJN

Alhoewel het rendement[3] op computerverzekeringen (momenteel circa 45 à 50 procent, doch afnemend) voor verzekeraars als aantrekkelijk mag worden beschouwd, zijn er in Nederland slechts enkele verzekeraars die deze (uitgebreide) computerverzekeringen aanbieden. Volgens mededeling van geïnterviewde verzekeraars wordt dit veroorzaakt door een (te) kleine vraag naar dergelijke produkten in Nederland. Dit in tegenstelling tot landen als Zweden, Duitsland en de Verenigde Staten. De verzekeraars noemen een (niet nader onderbouwd) laag risicobewustzijn bij de Nederlandse ondernemer als één van de voornaamste redenen.

Een toename van dit risicobewustzijn kan in belangrijke mate door de overheid worden gestimuleerd. Zo is men in Zweden in 1981 overgegaan tot de installatie van een speciale raad (BÅRK) die zich bezighoudt met projecten die gericht zijn op het terugdringen van de kwetsbaarheid van computersystemen. Het feit dat ook de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) reeds in 1981 een speciaal seminar belegde waarin deze kwetsbaarheid aan de orde kwam, zou voor de Nederlandse ondernemer genoeg reden moeten zijn de risico's met betrekking tot de automatisering nauwkeurig te analyseren.

In hoeverre het relatief lage risicobewustzijn bij de

3. *Het rendement is gedefinieerd als (100-schadepercentage), waarbij het schadepercentage is berekend als (uitgekeerde schadebedragen/ontvangen premies). Hierbij wordt voor de eenvoud geabstraheerd van de normale bedrijfskosten.*

*Drs. G.J.W.C. Vankan*
*Is sinds 1990 werkzaam bij KPMG Klynveld EDP Auditors. In 1992 studeerde hij af aan de post-doctorale opleiding EDP-auditing aan de Erasmus Universiteit te Rotterdam. Dit artikel is een aangepaste versie van zijn afstudeerreferaat.*

Nederlandse ondernemer daadwerkelijk resulteert in relatief meer financiële schade als gevolg van een kwetsbaarder automatisering is onduidelijk.
In het kader van de adviesfunctie naar het management zal de accountant het management moeten attenderen op mogelijke (bedrijfseconomische) risico's ten gevolge van lacunes in de procedures en maatregelen met betrekking tot de geautomatiseerde gegevensverwerking die invloed hebben op de realisatie van de bedrijfsdoelstellingen.

## SAMENVATTING EN CONCLUSIE

Een toenemend aantal cliënten verwacht dat de accountant bevindingen rapporteert over de mate waarin een organisatie maatregelen heeft getroffen ter voorkoming en/of beperking van schade in een geautomatiseerde omgeving. Ook de Nederlandse wetgever (Wet computercriminaliteit) verwacht dat de (externe) accountant zijn bevindingen omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking rapporteert (voor zover in het kader van de jaarrekeningcontrole van toepassing).
Dit betekent dat de accountant de volgende vragen ten aanzien van de risico's in een geautomatiseerde omgeving moet kunnen beantwoorden:

- Zijn de mogelijke risico's voldoende gedekt?
- Is de organisatie in staat schade als gevolg van risico's die niet bij derden zijn verzekerd zelf te dragen (voorzieningen, reserves, liquiditeit)?
- Wordt aandacht besteed aan de naleving van door verzekeraars gestelde voorwaarden?

Beantwoording van deze vragen vereist een kennisverbreding van de accountant dan wel inschakeling van deskundigen (in casu EDP-auditors).
Als sluitstuk op het stelsel van maatregelen ter voorkoming en/of beperking van schade kunnen verzekeringen worden afgesloten. Op de Nederlandse markt wordt hiervoor door een aantal verzekeraars de zogenaamde 'computerverzekering' aangeboden. Deze computerverzekeringen kunnen qua dekkingsgebieden per verzekeraar verschillen. Kennis van de mogelijkheden van deze verzekeringen is dan vereist om een adequaat advies richting cliënt te kunnen geven.

## LITERATUUR

[Bork87] J.J. Borking, *Enige kanttekeningen bij informaticaverzekeringen*, Informatie, jaargang 29, nr. 1, 1987.

[Kear79] B. Kearns, *Disasters: are you sure you're really covered?*, Data Processing, July/August 1979.

[Kock80] H.C. Kocks en J.H. Urbanus, *Risicoanalyse met betrekking tot de automatisering*, Informatie, jaargang 22, nr. 3, 1980.

[Kock90] H.C. Kocks, *Inzicht in samenhang*, post-doctorale opleiding EDP-auditing, Erasmus Universiteit Rotterdam, 1990-1991.

[Koni80] W.A.M. Koning, *Gegevensbeveiliging, Risicobeheer en verzekeren*, Informatie, jaargang 22, nr. 3, 1980.

[Lent86] A.A. van Lent, *Risk Management, Risicobeheer plus risicobeheersing*, Informatie, jaargang 28, nr. 6, 1986.

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

# Geautomatiseerde betalingen

Drs. R. Oudega en drs. P. Veltman RE RA

**Geautomatiseerd betalingsverkeer noopt meer dan andere toepassingen van informatietechnologie tot het treffen van preventieve beheersingsmaatregelen, om te voorkomen dat een organisatie onherstelbare schade lijdt. Zeker zolang nog geen sprake is van standaardisatie ten aanzien van technische faciliteiten op dit terrein vereist een beoordeling van de betrouwbaarheid van geautomatiseerd betalingsverkeer specifieke kennis van de verschillende technieken en media die hiervoor beschikbaar zijn. Dit artikel geeft hiertoe de nodige achtergrondinformatie.**

## INLEIDING

Het uitgaand betalingsverkeer en de desbetreffende administratieve organisatie vormen belangrijke aandachtspunten bij de controle van de jaarrekening. Niet alleen zijn uitgaande betalingen één van de ankerpunten voor de controle van de volledigheid van de opbrengstverantwoording, ook zijn zij vatbaar voor malversaties. Veelal verwacht de gecontroleerde huishouding dat de accountant leemtes signaleert die het mogelijk maken dat onbedoelde betalingen worden verricht.

In dit artikel komen de verschillende verschijningsvormen van het geautomatiseerd betalingsverkeer aan de orde, zoals deze worden aangetroffen bij zakelijke bank- en Postbank-cliënten. Daarbij worden geen uitgebreide beschrijvingen gegeven maar zal worden ingegaan op de specifieke aandachtspunten vanuit het oogpunt van interne controle.

Allereerst wordt daarvoor een kort overzicht gegeven van de verschillende betalingscircuits in Nederland, de 'omgeving' waarbinnen het geautomatiseerde betalingssysteem zich afspeelt. Op de veranderingen in deze omgeving wordt kort ingegaan.

Het sterk opkomend gebruik van elektronische bankiersystemen kent zijn eigen specifieke beheersingsproblematiek. Deze wordt in een aparte paragraaf meer uitgebreid behandeld, waarbij wordt ingegaan op het gehele stelsel van maatregelen in en rond het elektronisch bankiersysteem. Onderscheid wordt gemaakt tussen de maatregelen in het elektronisch bankiersysteem en de maatregelen die de organisatie zelf dient te treffen. Tevens worden de verschillen tussen de elektronische bankiersystemen onderling aangegeven.

## OVERZICHT BETALINGSCIRCUITS

In Nederland zijn voor het particuliere en zakelijke betalingsverkeer twee betalingscircuits te onderscheiden: het bancaire circuit via de BankGiro-Centrale (BGC) en het circuit van de Postbank. Daarnaast vormen de rekeninghouders bij De Nederlandsche Bank samen het topgirocircuit. In deze paragraaf zullen van de verschillende circuits kort de karakteristieken worden aangegeven. Daarbij zal de ontwikkeling van het Nationaal Betalings-circuit tevens aan de orde komen.

### BGC/banken-circuit

De BankGiroCentrale is het verevenmgsinstituut voor de banken. Zakelijke betalingen (alsmede incasso-opdrachten) via het BGC/banken-circuit worden veelal rechtstreeks bij de BGC aangeleverd. De banken zelf zijn echter verantwoordelijk voor de controle op bestedingsruimte van de cliënt en authenticatie van de aangeleverde opdrachten. Deze authenticatie houdt in dat de banken dienen vast te stellen dat de aangeleverde opdrachten daadwerkelijk door de opdrachtgever zijn aangeleverd. Met de bank kunnen afspraken worden gemaakt over wie tot welk bedrag tekeningsbevoegd is. Na fiat van de bank verzorgt de BGC de betalingstransacties, waarbij een aantal controles wordt uitgevoerd. Deze controles betreffen onder meer de bestaanbaarheid van de rekeningnummers en de integriteit van de aangeleverde betalingsbestanden.

### Postbankcircuit

Het Postbankcircuit kent slechts één bank, waardoor een vereveningsinstituut zoals de BankGiro Centrale niet nodig is. De controles die de Postbank uitvoert zijn vergelijkbaar met de controles die door de banken en de BankGiroCentrale worden uitgevoerd en richten zich derhalve op de bestedingsruimte van de cliënt, de authenticiteit van de opdrachtgever en de integriteit van de aangeleverde bestanden.

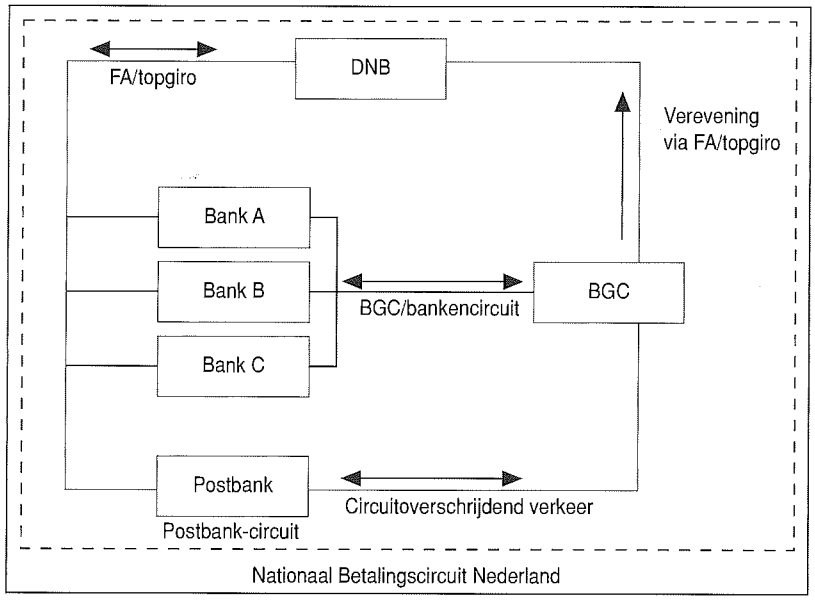
### Topgirocircuit

Rekeninghouders bij De Nederlandsche Bank kunnen via het topgirocircuit betalingen aan elkaar verrichten. Deze rekeninghouders zijn de banken, de BankGiroCentrale, de Postbank, de overheid en andere centrale banken. Om betalingen te kunnen verrichten en informatie te kunnen opvragen zijn de rekeninghouders aangesloten op het FA-systeem.

### Nationaal Betalingscircuit

Het bestaan van de verschillende betalingscircuits naast elkaar wordt reeds langere tijd als storend ervaren. Het circuitoverschrijdend betalingsverkeer (bijvoorbeeld een betaling van een bankcliënt aan een Postbank-rekeninghouder) is trager en duurder. In de jaren zeventig is in opdracht van de minister van Financiën een project gestart om te komen tot één geïntegreerd betalingscircuit. In 1985 is besloten het Nationaal Betalingscircuit geleidelijk te ontwikkelen. Van de toen geformuleerde zeven fases is inmiddels een aantal ingevoerd. Per fase wordt één soort betaling behandeld, waarbij de techniek en de organisatie van de verschillende circuits op elkaar worden afgestemd. Het resultaat van de reeds ingevoerde fases is onder meer een verkorting van de duur van het betaaltraject van circuitoverschrijdende betalingen met één dag voor de desbetreffende soorten betalingen.
Schematisch zijn de verschillende circuits en het Nationaal Betalingscircuit weer te geven als in figuur 1.

*Figuur 1. Betalingscircuits.*




## MEDIA VOOR GEAUTOMATISEERDE BETALINGEN

Het geautomatiseerd aanleveren van betaalopdrachten is bij de zakelijke cliënten van banken en Postbank reeds lange tijd een gebruikelijke zaak. De opdrachten kunnen worden aangeleverd op tape (of cartridge), diskette of via datacommunicatie. De opdracht tot uitvoering van de aangeleverde betaalopdrachten is schriftelijk vastgelegd in een geleidebrief. Enerzijds bevat deze brief één of meer handtekeningen van de procuratiehouders, aan de hand waarvan de bank de authenticiteit van de opdrachtgever kan vaststellen. Anderzijds is op de geleidebrief een aantal controletotalen opgenomen, aan de hand waarvan de integriteit van de betaalopdrachten op het medium kan worden vastgesteld. Deze totalen zijn:
- het totaal aantal betaalopdrachten;
- de som van de rekeningnummers;
- de som van de bedragen.

De ontvanger (BGC of Postbank) telt het medium door en berekent opnieuw de controletotalen. Indien deze overeenkomen met de totalen op de geleidebrief wordt de integriteit van de betaalopdrachten bewezen geacht.

Ondanks de controles die door banken, BGC en/of Postbank worden uitgevoerd, is het niet geheel uitgesloten dat ten onrechte een batch met gemanipuleerde betalingen wordt geaccepteerd en verwerkt. Het gevaar van manipulaties wordt veroorzaakt doordat het in het algemeen voor mensen niet mogelijk is de betalingsinformatie op het machinaal leesbaar medium rechtstreeks waar te nemen. Controle, autorisatie en procuratie van betalingsopdrachten geschieden daarom op basis van een geleidedocument of aan het beeldscherm. Het is echter mogelijk zodanige manipulaties uit te voeren dat de informatie op het geleidedocument en zelfs op het beeldscherm afwijkt van de eigenlijke betalingsinformatie op het machinaal leesbaar medium. Zolang hierbij de controletotalen op het medium rekenkundig juist zijn (dat wil zeggen de som vormen van de afzonderlijke bedragen en rekeningnummers op het medium), én overeenstemmen met de controletotalen op het geleideformulier, zullen de betalingsopdrachten voor verwerking worden geaccepteerd. Dit kan geïllustreerd worden aan de hand van het volgende, geanonimiseerde voorval dat zich onlangs voordeed.

Een middelgroot handelsbedrijf gebruikt voor zijn financiële administratie een bekend PC-pakket. Voor het verrichten van betalingen gebruikt het bedrijf een, door een bank geleverde, standaardtoepassing met behulp waarvan betaalopdrachten automatisch worden aangemaakt en op diskette gezet. Tevens wordt een geleidelijst geproduceerd met de som van de rekeningnummers en het totaalbedrag. Een medewerker van het bedrijf zag kans de programmatuur die deze diskette en geleidelijst aanmaakt te manipuleren. De rekeningnummers van de begunstigden werden hierdoor op de diskette vervangen door het eigen rekeningnummer. Op de geleidelijst werd de som van de rekeningnummers afgedrukt die correspondeerde met de som van de (gemanipuleerde) rekeningnummers op de diskette. De procuratiehouder ontdekte dit niet en de medewerker ging er vandoor met circa twee miljoen gulden.

De beschreven fraude had kunnen worden voorkomen als de procuratiehouder de controletotalen op de geleidelijst had herberekend. Problematischer wordt het als bij de manipulatie de controletotalen niet veranderen. Dit kan door twee of meer bedragen en/of rekeningnummers te wijzigen zodanig dat de som hiervan gelijk blijft (ook wel verschuivingen genoemd). Weliswaar wijkt de inhoud van het geleideformulier nu ook af van de inhoud van het betaalmedium, maar dit kan niet meer door natellen van het geleideformulier worden ontdekt.
Om deze manipulatie te voorkomen zijn technieken ontwikkeld voor het berekenen van controletotalen waarbij elke wijziging in een afzonderlijke betalingsopdracht moet leiden tot een wijziging in het controletotaal. Zo is manipulatie al moeilijker als het controletotaal de som vormt van het produkt van bedrag en rekeningnummer; nog geavanceerder zijn controletotalen gebaseerd op cryptografische technieken. Hieraan zijn echter ook weer nadelen verbonden; controletotalen kunnen niet (eenvoudig) meer worden nageteld zodat andere maatregelen moeten worden getroffen om te waarborgen dat de inhoud van de geleidelijst overeenstemt met de betaalopdrachten op het medium. Deze maatregelen kunnen worden getroffen in de automatiseringsorganisatie. Een andere mogelijkheid is gebruik te maken van een afgescheiden, veilige omgeving, waar ongeautoriseerde manipulatie van programmatuur en/of gegevens vrijwel uitgesloten is. Het is mogelijk met behulp van een elektronisch bankiersysteem een dergelijke, beveiligde omgeving te creëren.

*Ondanks de controles die door banken, BCG en/of Postbank worden uitgevoerd, is het niet geheel uitgesloten dat een batch met gemanipuleerde betalingen wordt geaccepteerd en verwerkt.*

In de volgende drie subparagrafen wordt per medium kort aangegeven wat vanuit het oogpunt van interne controle de karakteristieke voor- en nadelen zijn, en welke maatregelen kunnen worden getroffen om de risico's te beperken.

**Tape**

Gebruik van tape als betaalmedium heeft als nadeel dat visuele controle van de inhoud aan een beeldscherm niet eenvoudig is te realiseren. Het is mogelijk een tapestreamer aan een PC te koppelen, met behulp waarvan de inhoud van de tape kan worden vergeleken met de geleidelijst, maar dit is een weinig toegepaste, dure methode. Het voordeel van een tape is dat voor het aanbrengen van frauduleuze wijzigingen toegang tot dure apparatuur noodzakelijk is, waardoor de fraudemogelijkheid wordt verkleind.
De onzekerheid van de procuratiehouder omtrent de inhoud van de tape kan worden opgelost door het treffen van zodanige maatregelen binnen de automatiseringsorganisatie dat waarborgen worden geboden dat de inhoud van de tape overeenkomt met de geleidelijst. Volstrekte zekerheid kan hierdoor echter niet worden verkregen. Aanvullende maatregelen kunnen zijn:

- Het limiteren van het totaalbedrag dat met één tape wordt betaald. Dit is mogelijk door afspraken met de bank te maken. Een fraude is hierdoor minder aantrekkelijk.

- Al of niet steekproefsgewijs verzenden van de tape met geleidelijst naar een onafhankelijke instantie (bijvoorbeeld een accountant, EDP-auditor of servicebureau) die de overeenstemming tussen

beide kan vaststellen. Deze maatregel, die ook als fake-procedure kan worden gehanteerd, wordt in de praktijk weinig toegepast.

– Afspraken over de terugmelding van de verrichte betalingen zodat ten onrechte verrichte betalingen tijdig worden gesignaleerd en kunnen worden hersteld.

**Diskette**

Betaalopdrachten op diskettes hebben het voordeel dat de procuratiehouder gemakkelijk met behulp van een PC de inhoud van de diskette kan bekijken en vergelijken met de geleidebrief. Het is echter wel raadzaam deze PC fysiek te beveiligen om manipulatie van de programmatuur op de PC te voorkomen.

*Het nadeel van een diskette is dat in principe iedereen met een PC de diskette (na procuratie) kan wijzigen.*

Het nadeel van een diskette is dat in principe iedereen met een PC de diskette (na procuratie) kan wijzigen. De beste oplossing daarvoor is te zorgen dat de diskette zo spoedig mogelijk na de procuratie wordt verzonden.

**Verzending door middel van datacommunicatie**

Verzending van betaalopdrachten door middel van datacommunicatie verschilt niet wezenlijk van het gebruik van tapes of diskettes. In plaats van de verzamelde transacties op een tape of diskette te plaatsen worden ze nu via een datacommunicatielijn verstuurd. Een voordeel is dat de procuratiehouder op zijn beeldscherm het bestand met de geleidelijst kan vergelijken alvorens hij het bestand verstuurt. Een nadeel is dat de procuratiehouder geen zekerheid kan hebben dat het door hem gecontroleerde bestand overeenkomt met het verzonden bestand. Dit kan worden opgelost door maatregelen in de automatiseringsorganisatie te treffen. Andere oplossingen kunnen zijn het beperken van het maximaal in één keer te verzenden bedrag en afspraken omtrent de wijze van terugmelden.

## ELEKTRONISCH BANKIEREN

Steeds vaker wordt gebruik gemaakt van elektronische bankiersystemen. Dit zijn systemen met behulp waarvan betaalopdrachten door middel van datacommunicatie aan de bank worden verzonden. Daarnaast kan met behulp van een elektronisch bankiersysteem informatie worden opgevraagd over de eigen rekeningen. De vanuit het oogpunt van interne controle relevante verschillen ten opzichte van geautomatiseerd betalingsverkeer met behulp van de eerder genoemde media zijn:

– Bij elektronische bankiersystemen wordt ter authenticatie geen separate begeleidingsbrief aan de bank verzonden. De begeleidingsbrief wordt in elektronische vorm meegezonden met de betaalopdrachten. Hierdoor kan geen gebruik meer worden gemaakt van de handtekeningkaarten maar dient op een andere manier te worden vastgesteld dat de betalingsopdrachten afkomstig zijn van de geautoriseerde opdrachtgever. Hierop wordt later in dit artikel nader ingegaan.

– De betaalopdrachten worden naar de bank verzonden in plaats van naar de BGC (bij de Postbank is dit geen verschil).

Elektronische bankiersystemen komen in vele vormen voor. De meeste banken hebben eigen systemen ontwikkeld en aangeboden op de markt. De eisen van interne controle die aan de elektronische bankiersystemen kunnen worden gesteld zijn, gezien de overeenkomende functionaliteit, voor al deze systemen gelijk. De maatregelen die in en rond het elektronisch bankiersysteem zijn getroffen, dienen te waarborgen dat slechts juiste en geautoriseerde betalingen aan de rechthebbenden worden uitgevoerd. Deze maatregelen zijn onder te verdelen in twee groepen. Enerzijds de maatregelen zoals die binnen het elektronisch bankiersysteem zijn getroffen en anderzijds de door de organisatie te treffen maatregelen.

**Maatregelen binnen het elektronisch bankiersysteem**

De maatregelen zoals die binnen de verschillende elektronische bankiersystemen zijn getroffen, zijn veelal gericht op:

1 het aanbrengen en onderhouden van functiescheidingen in het betaaltraject (invoeren, controleren, verzenden en autoriseren van betaalopdrachten);

2 het beheersen van de procuratiefunctie, door het gebruik van aanvullende identificatie/authenticatiehulpmiddelen af te dwingen;

3 het volledig/juist verzenden van betaalopdrachten;

4 het controleren van de betaalopdrachten in verschillende stadia van het betaaltraject, inclusief de reconciliatie.

*Ad. 1*
De functiescheidingen in het betaaltraject hebben tot doel te voorkomen dat één functionaris alle schakels in het betaaltraject kan beïnvloeden. Gebruikelijk is bijvoorbeeld een functiescheiding tussen invoer, controle/autorisatie en procuratie. Dergelijke functiescheidingen worden door elektronische bankiersystemen ondersteund.
Voor het invoeren en onderhouden van de functiescheidingen op het lokale werkstation is bij de

meeste systemen een systeembeheerfunctie gedefinieerd. Een bedreiging die daardoor ontstaat is dat de systeembeheerder zichzelf dusdanige bevoegdheden kan toekennen dat hij alle functies in het betaaltraject kan uitvoeren. Om deze bedreiging tegen te gaan is het bij een aantal systemen noodzakelijk dat gebruikers tevens bekend zijn op de hostcomputer van de bank, of zijn voor belangrijke functies extra hulpmiddelen noodzakelijk voor identificatie/authenticatie.

*Ad. 2 en 3*
Doordat geen separate begeleidingsbrief aan de bank wordt verzonden, dient de bank op een andere wijze de authenticiteit van de opdrachtgever vast te stellen. Dit gebeurt door de procuratiehouder een elektronische handtekening te laten zetten. De wijze waarop dit in de diverse elektronische bankiersystemen is gerealiseerd, verschilt sterk. Zo maakt Girotel van de Postbank ten behoeve van de procuratie gebruik van een lijst met Transactie Acceptatie Nummers, de zogenaamde TAN-lijst. Na verzending van de opdrachten aan de Postbank dienen ter procuratie twee TAN-codes te worden opgegeven. Doordat de opdrachtgever beschikt over een unieke lijst met TAN-codes kan de Postbank de authenticiteit vaststellen.

Andere elektronische bankiersystemen maken gebruik van een calculator waarop een code wordt gegenereerd die aan de batch met betaalopdrachten dient te worden toegevoegd. Nadat de procuratiehouder een specifieke code in de calculator heeft ingevoerd of nadat met behulp van de calculator een code van het scherm is afgelezen, toont deze calculator als respons een code. Doordat de calculator uniek is voor de opdrachtgever stelt de bank aan de hand van die code de authenticiteit vast.

Ter waarborging van de integriteit van de betaalopdrachten worden controletotalen met de betaalbatches meegezonden, zoals het totaalbedrag, de som van de rekeningnummers en de som van de produkten van de bedragen en de rekeningnummers. De ontvangende bank stelt op basis van deze met de batch meegezonden gegevens en de eigen tellingen vast dat de batch juist en volledig is ontvangen.
Een gescheiden toepassing van enerzijds een integriteitskenmerk en anderzijds een authenticiteitskenmerk kan tot gevolg hebben dat na het plaatsen van het authenticiteitskenmerk de gegevens en het integriteitskenmerk worden gemanipuleerd. Het voorstel voor een Nederlandse standaard voor de elektronische handtekening van de Nederlandse Vereniging van Banken (NVB) biedt daarvoor een oplossing [Lith92-1]. Deze standaard kent het zogenaamde twee-lagenprincipe. De eerste laag bestaat uit de NVB-hash en biedt waarborgen voor de integriteit van de data. De NVB-hash is een controlegetal dat met een op cryptografische technieken gebaseerd algoritme is berekend. De tweede laag is de elektronische handtekening, die als authenticiteitskenmerk dienst doet. De elektronische handtekening wordt berekend over de NVB-hash, en beschermt deze daarmee tegen het aanbrengen van wijzigingen.

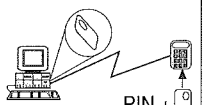
In enkele elektronische bankiersystemen is dit twee-lagenprincipe of een variant hierop geïmplementeerd.

*Ad. 4*
De elektronische bankiersystemen bieden diverse mogelijkheden de betaalopdrachten in de opeenvolgende stadia in het betaaltraject te volgen door deze aan het scherm op te vragen of door een overzicht van de betaalbatches aan te maken. Het belangrijkste controlepunt is gelegen bij het verlenen van procuratie voor de betaalopdrachten. Hierna worden de betalingen geëffectueerd en kunnen, uitgaande van voldoende waarborgen, geen wijzigingen in de betaalbatches worden aangebracht.

Het sluitstuk op het hele betaaltraject is de controle van de juiste verwerking van de betaalopdrachten. Door de informatie die daarvoor van de bank wordt ontvangen in detail te controleren kunnen eventuele onjuiste of ongeautoriseerde betalingen snel worden ontdekt. Deze reconciliatie kan handmatig worden uitgevoerd maar ook geautomatiseerd. Bij automatische reconciliatie wordt de elektronische informatie die van de bank wordt ontvangen omtrent betalingen (en ontvangsten) gematched met de eigen crediteurenadministratie (of in het geval van ontvangsten de debiteurenadministratie). Enkele elektronische bankiersystemen bieden deze mogelijkheden standaard. Voor andere is aanvullende programmatuur noodzakelijk.

De mate waarin de verschillende elektronische bankiersystemen gebruik maken van de bovenge-

*Tabel 1. Configuraties van elektronische bankiersystemen.*

| | | |
|---|---|---|
| Software only  | De beveiligingsmaatregelen zijn uitsluitend software-matig geïmplementeerd. Er is geen fysieke beveiliging. | – lage bedragen<br>– klein aantal transacties |
| Calculator offline   | De elektronische handtekening wordt in de calculator berekend en wordt handmatig naar de telefoon of terminal overgebracht. | – lage tot middelgrote bedragen<br>– klein aantal transacties |
| PC en calculator offline  | De in de PC berekende hash wordt handmatig overgebracht naar de calculator, waar de handtekening wordt berekend. De handtekening wordt vervolgens handmatig naar de PC overgebracht. | – lage tot middelgrote bedragen<br>– klein aantal transacties |
| PC en smartcard online   | De in de PC berekende hash wordt automatisch overgebracht naar de calculator, waar de handtekening wordt berekend. De handtekening wordt vervolgens automatisch teruggetransporteerd. | – middelgrote bedragen<br>– groot aantal transacties |
| PC en security board en smartcard online   | Naast de PC en de smart card-lezer wordt gebruik gemaakt van een security board, die in de PC is geplaatst. De berekening van de hash en die van de elektronische handtekening vinden beide plaats binnen het security board. | – hoge bedragen<br>– groot aantal transacties |

noemde maatregelen maakt ze meer of minder geschikt voor het verrichten van grote betalingen. In [Lith92-2] wordt een mogelijke indeling gegeven van configuraties van elektronische bankiersystemen (zie tabel 1).

**Maatregelen in de organisatie**

Afhankelijk van de faciliteiten die worden geboden door het elektronisch bankiersysteem dient de organisatie maatregelen te treffen om van deze faciliteiten optimaal gebruik te maken. Onderstaand worden de aandachtspunten daarvoor nader uitgewerkt.

*Handhaven van de functiescheidingen in het betaaltraject*
De procedures rond het invoeren en onderhouden van gebruikersbevoegdheden dienen de blijvende juistheid van de aangebrachte functiescheidingen te waarborgen. Aandacht dient daarbij te worden gegeven aan de systeembeheerfunctie en aan de aanwezigheid van standaardgebruikers met vergaande bevoegdheden op de PC. Voorbeelden daarvan zijn de standaardgebruikers zoals die binnen Girotel ZTM zijn gedefinieerd; twee standaardgebruikers ('111' en '333') hebben volledige bevoegdheid tot het verrichten van betalingen. Het is aan te bevelen deze gebruikers bij het in gebruik nemen van het elektronisch bankiersysteem te verwijderen.
In het ideale geval dwingt het elektronisch bankiersysteem af dat het invoeren en onderhouden van gebruikersbevoegdheden door twee systeembeheerders wordt uitgevoerd. Dit is bijvoorbeeld het geval bij systemen voor het interbancaire betalingsverkeer, zoals het FA-systeem en de BGC-PC. Indien het elektronisch bankiersysteem dit niet afdwingt, is het mogelijk als compenserende maatregel de systeembeheerfunctie af te schermen voor ongeautoriseerd gebruik door het systeembeheerpassword slechts ter beschikking te stellen indien noodzakelijk. Een andere mogelijkheid is de PC te voorzien van een toegangsbeveiligingspakket, zodanig dat een tweede persoon noodzakelijk is om de systeembeheerder toegang te verlenen. Noodzakelijk is in ieder geval dat de procuratiehulpmiddelen met name voor de systeembeheerders zijn afgeschermd.

*Beheersing van de hulpmiddelen ter procuratie*
Voor het plaatsen van de elektronische handtekening wordt, zoals eerder vermeld, gebruik gemaakt van diverse hulpmiddelen, zoals codelijsten, calculators of chipcards. Door deze elektronische handtekening kan de authenticiteit van de opdrachtgever worden vastgesteld. Voor het afschermen van de procuratiefunctie dienen deze hulpmiddelen op een adequate wijze te worden beheerd, zodat ongeautoriseerd gebruik wordt voorkomen. Door het gemak waarmee deze hulpmiddelen kunnen worden overgedragen, is echter een mogelijke uitholling van de procuratiefunctie geïntroduceerd. In de praktijk blijkt dat veel procuratiehouders, al of niet vanwege tijdgebrek, niet bereid zijn naar de PC met het elektronisch bankiersysteem te komen, en geneigd zijn het plaatsen van de elektronische handtekening door andere functionarissen te laten uitvoeren. Hierdoor wordt de beschikkende bevoegdheid gelegd bij uitvoerende functionarissen, met alle risico's van dien. Dit kan, afhankelijk van het gebruikte elektronisch bankiersysteem, worden ondervangen door de procuratiehouders een eigen PC met elektronisch bankiersysteem ter beschikking te stellen.

*Uitvoeren van de noodzakelijke controles in het betaaltraject*
De organisatie dient, om een betrouwbaar betalingsverkeer te realiseren, in voldoende mate gebruik te maken van de door het elektronisch bankiersysteem geboden controlefaciliteiten. Vanuit een relatief 'onveilige' omgeving worden betaalopdrachten aangeleverd en in het elektronisch bankiersysteem ingevoerd. In deze relatief 'veilige' omgeving is het zinvol controles uit te voeren. Het meest effectief is daarbij een detailcontrole van de betaalopdrachten door de procuratiehouder. Door tijdgebrek van de druk bezette procuratiehouders is dit echter veelal niet realiseerbaar. Een oplossing hiervoor is het introduceren van een derde functionaris die geen betaalopdrachten kan invoeren of wijzigen maar belast is met de controle daarvan. Een andere mogelijkheid is de detailcontrole te beperken tot betalingen groter dan een bepaald bedrag. Daarnaast dient als sluitstuk op het betaaltraject de reconciliatie van de verrichte betalingen daadwerkelijk te worden uitgevoerd.

*Voorkomen van manipulatie van de programmatuur*
De programmatuur van een elektronisch bankiersysteem wordt geïnstalleerd op een PC. Een dergelijke omgeving is meestal vrij toegankelijk voor onbevoegden. Het is met eenvoudig te verkrijgen hulpprogramma's mogelijk de programmatuur aan te passen. Deze aanpassing kan zodanig zijn dat de gegevens op het scherm verschillen van de werkelijke gegevens, waardoor ten onrechte procuratie kan worden verleend. Hierbij dient wel te worden bedacht dat het uitvoeren van deze aanpassingen de nodige inspanning en kennis vereist, hetgeen de kans op het manifest worden van deze bedreiging kleiner maakt.
Bij de eerder genoemde systemen voor interbancair betalingsverkeer zijn maatregelen genomen om manipulatie van de programmatuur te verhinderen. Mogelijke maatregelen die de organisatie kan nemen, zijn:
- gebruik maken van toegangsbeveiligingspakketten;
- onmogelijk maken van het gebruik van het diskettestation;
- fysiek afschermen van het werkstation.