

Drs. H. M. I. van der Putten RA

Accountantscontrole bij kleinschalige automatisering

1. Inleiding

Op automatiseringstechnisch gebied is er een welhaast revolutionaire ontwikkeling geweest door de komst van relatief goedkope maar krachtige en bovendien vaak gebruikersvriendelijke computers (mini- en microcomputers). Hierdoor zijn veel kleinere organisaties in staat een computer in te schakelen bij delen van of het gehele gegevensverwerkingsproces. Bij grotere organisaties is het mogelijk om met een relatief lage investering op niveau van afdelingen of concern-onderdelen extra computercapaciteit toe te voegen, met als grote voordeel dat de gebruiker zelf het beheer daarover kan voeren.

Deze ontwikkeling in een tijd van toenemende decentralisatie en schaalverkleining met bovendien nog voor kleinere organisaties verruimde accountantscontroleplicht heeft het onderhavige vraagstuk zeer direct gebracht bij elke algemene accountant in de praktijk. Hij bemerkt dat hij zonder een bepaalde automatiseringskennis een deel van zijn specifieke arbeidsterrein (in het bijzonder op het gebied van de administratieve organisatie) verliest. Een ruime inschakeling van een op automatiseringscontrolegebied gespecialiseerde EDP-auditor biedt op grond van kostenverhoudingen in de kleinere organisatie ook geen uitweg meer.

2. Wat is kleinschalige automatisering?

Voor dit artikel wordt onder kleinschalige automatisering verstaan de geautomatiseerde informatieverzorging - uitmondend in een jaarrekening - in kleinschalige organisaties. Het begrip wordt dus niet direct gekoppeld aan de omvang van de computercapaciteit. Door de snelle technologische ontwikkelingen zijn begrippen als mini- en microcomputer niet meer onderscheidend genoeg.

Doelmatiger is om de onderscheiding te koppelen aan de omvang van de organisatie waarbij *in dit verband* onder kleinschaligheid zal worden verstaan een omvang waarbij een afzonderlijk volwaardig 'rekencentrum' (in brede zin met full-time-functies systeemontwikkeling, programmering, productie/operating en bestandsbewaring) ontbreekt. Bij de huidige kleinere computers ontbreken technische redenen voor de inrichting van zo een afzonderlijk rekencentrum (afgezonderde airconditioned ruimte, gespecialiseerd bedienend personeel en dergelijke). De computer kan op de gebrui-

kersafdeling worden geplaatst.

Bij deze kleinschaligheid kan het gaan om zowel juridisch en bedrijfseconomisch geheel zelfstandige organisaties als om uit administratief-organisatorisch oogpunt zelfstandige onderdelen van concerns. In het laatste geval dient er dan geen koppeling te zijn met een centrale computer op concerniveau, noch dienen deze onderdelen direct beïnvloed te worden door centrale interne controlemaatregelen anders dan van globaal toezichhoudend/beoordelend karakter.

Kleinschalige automatisering kenmerkt zich meestal door:

- een gering aantal medewerkers waardoor weinig mogelijkheden voor een adequate functiescheiding, en wat betreft automatische gegevensverwerking in het bijzonder:
 - geen functiescheiding tussen elektronische gegevensverwerking en gebruikers (gebruikers creëren basisdocumenten, voeren de gegevens in de computer in, bedienen de computer voor de verwerking en gebruiken de uitvoer);
 - geen functiescheiding tussen systeemontwikkeling, programmering, feitelijke gegevensverwerking (productie) en het bewaren van programma's en gegevensbestanden;
- de (stand-alone) computer bevindt zich op de (of een) gebruikersafdeling. Soms ook wel op een kleine afdeling, als zodanig wel EDP-afdeling geheten, doch niet vergelijkbaar met wat daar normaliter onder dient te worden verstaan. Technische specialisatie wordt bij externe instanties gehaald (leveranciers, adviseurs);
- relatief beperkte automatiseringskennis bij de gebruikers/bedieners van de computer en bij de verantwoordelijke hogere functionarissen. Veelal concentratie van automatiseringsknow-how bij één persoon of een zeer gering aantal personen;
- gebruik van kleinere goedkopere computers met primair op gebruiksgemak en snelheid gerichte besturingssystemen, welke (mede daardoor) minder controlemogelijkheden bieden dan grotere computers; hetzelfde geldt voor de (meestal gekochte standaard-)toepassingsprogrammatuur. Een bijverschijnsel van de lage prijs is doorgaans ook de lage servicegraad van de leveranciers;
- veel standaardprogrammatuur; in principe minder doeltreffend dan maatprogramma's;
- zelf ontwikkelde toepassingsprogrammatuur veelal geschreven in een ook voor 'computerleken' relatief gemakkelijk te leren programmeertaal (vaak Basic) en toepassing van 'interpreters'. Bij interpreters vindt omzetting in machinetaal plaats per opdracht bij de verwerking, waardoor nog op elk moment bij de verwerking wijzigingen eenvoudig, eventueel alleen tijdelijk en achteraf niet meer zichtbaar, kunnen worden aangebracht. Dit in tegenstelling tot het hanteren van 'compilers', waarbij het programma in broncode separaat wordt bewaard en voor de productie alleen een 'objectversie' ter beschikking wordt gesteld;
- beperkte of ontbrekende documentatie omtrent het systeem;
- uitgebreid gebruik van zogenaamde utility-programma's, waarmee naast

andere functies onder andere eenvoudig gegevens rechtstreeks in bestanden kunnen worden ingebracht of gewijzigd, zonder een spoor daarvan achter te laten;

- uitgebreid gebruik van (kwetsbare) diskettes als opslagmedium;
- voornamelijk interactieve transactiegewijze verwerking van gegevens ook indien sprake is van meerdere gebruikers van het ene computersysteem (multi-usersystemen gebruik makend van terminals). In het laatste geval zijn vaak alle programma's en gegevensbestanden voortdurend on-line op het systeem aanwezig (multi-tasking).

Deze uit controleoogpunt minder gunstige karakertrekken komen boven op de ook bij niet geautomatiseerde kleine organisaties reeds bestaande controleproblemen zoals:

- (uiteraard) gebrek aan controletechnische functiescheidingen;
- concentratie van eigendom en/of dagelijks beheer bij een of slechts enkele personen met kans op dominerende en/of proceduredoorkennende handelingen, die een doorslaggevend effect hebben op delen van of de gehele administratieve vastlegging;
- betrekkelijk geringe kennis van verslaglegging en van administratieve organisatie (in het bijzonder ook van interne controlemaatregelen en het belang daarvan) bij de leiding en de overige medewerkers;
- informele procedures ter zake van registratie, verslaglegging, analyse, planning en controle.¹

3. De interne controle bij kleinschalige automatisering

3.1 Verschillen met de niet-geautomatiseerde situatie

De problematiek voor de controlerend accountant wordt nog duidelijker als wij aan de voorgaande opsomming nog de verschillen toevoegen tussen een situatie van wel en niet geautomatiseerde gegevensverwerking. Op deze meer algemene aspecten van automatisering en controle kan in het kader van dit artikel niet uitgebreid worden ingegaan. Volstaan wordt met wat hoofdlijnen. Met name kunnen genoemd worden:

- toenemende integratie van de gegevensverwerking waardoor traditionele functiescheidingen vervallen zonder dat er een technische reden is om deze op andere wijze weer aan te brengen of door andere controlemaatregelen te compenseren. Vooral bij kleinere organisaties zal dit dan ook uit kostenoverwegingen niet snel plaatsvinden;
- verdwijnen van voor de mens leesbare vastleggingen. Het ontbreken (soms) van basisdocumenten, mutatieoverzichten, uitvoer op papier. Ook het ontbreken van inzicht in het tot stand komen van door de computer gegenereerde gegevens op basis van geprogrammeerde beslissingen;
- toenemende afhankelijkheid van het geautomatiseerde systeem. De dagelijkse activiteiten kunnen na enige tijd van automatisering niet meer met dezelfde kwaliteit en/of snelheid plaatsvinden indien de computer of een bepaald programma zou uitvallen. De continuïteit van de organisatie is direct in het geding (afhankelijk van de bereikte automatiseringsgraad).

3.2 Algemene afwijkingen ten opzichte van de grootschalige automatisering
Bij de geautomatiseerde gegevensverwerking bij grotere organisaties ontstond door de concentratie op een EDP-afdeling een massaliteit die leidde tot verschillende full-time te vervullen specialistische functies, zoals systeemanalist, programmeur, operator, werkvoorbereider en media(tape-, schijf-)beheerder.

Bij kleinschalige automatisering zijn deze specialisten niet meer of niet full-time meer nodig. De gebruiker vraagt en krijgt directe toegangsmogelijkheden tot de informatie die hij nodig heeft zonder daarvoor omslachtige procedures te moeten volgen. Ontwikkeling van op heel specifieke eigen wensen afgestemde programmatuur wordt hem steeds gemakkelijker gemaakt, in toenemende mate zonder tussenkomst van anderen (utilityprogrammatuur, reportgenerators).

Daardoor zijn een groot aantal van de van de grootschalige automatisering bekende interne controlemaatregelen niet of niet geheel toepasbaar. Echter ook in de kleinere organisatie zullen er procedures moeten zijn om te voorkomen dat nieuwe gegevens onjuist worden vastgelegd of bestaande verminkt, zullen er afspraken moeten zijn wie verantwoordelijk is voor bepaalde gegevens, voor de continuïteit van de verwerking enz. en zullen er mede daarom beperkingen moeten worden gesteld aan de bevoegdheden van de andere medewerkers. Wel zal eerder het punt bereikt worden waarop de noodzakelijke afweging tussen kosten en nut leidt tot de beslissing een mogelijke maatregel niet in te voeren. Een zorgvuldige analyse van de risico's die specifiek door de betrokken organisatie worden gelopen is daartoe noodzakelijk. Het risico dat wordt gelopen hangt af van de aard van het bedrijf en van de gegevens in het systeem alsmede van het mogelijk gebruik/misbruik van die gegevens.

Na inventarisatie van de risico's zal beslist moeten worden waar stringente maatregelen noodzakelijk zijn en op welke gebieden volstaan kan worden met minder of geen beveiliging. Alleen op deze laatste gebieden zal een afweging nut/kosten aanvaardbaar zijn, waarbij om economische redenen bewust risico's kunnen worden gelopen. In deze afweging zal in ieder geval mee moeten worden genomen de invloed op de mogelijkheden en kosten van de controle door de externe accountant.

In het kader van dit artikel kan niet bij alle specifieke interne controleaspecten van kleinschalige automatisering gedetailleerd worden stilgestaan. In het navolgende zullen een aantal hoofdzaken kort de revue passeren, waarbij aan de controleerbaarheid relatief iets meer aandacht zal worden besteed. Verwezen wordt verder naar eerdere publikaties hierover in de vakliteratuur².

3.3 Functiescheidingen

Genoemd zijn al de controletechnische functiescheidingen in en rondom de automatiseringsorganisatie welke niet direct verwacht mogen worden bij kleinschalige automatisering. Een voordeel is dat vaak de systeemontwikkeling en programmering niet binnen de organisatie zelf maar extern plaatsvindt. Wel zullen dan waarborgen moeten worden geschapen dat kleinere

systeemwijzigingen niet toch in huis plaatsvinden, tenzij onder gecontroleerde omstandigheden.

In het algemeen zullen de bevoegdheden van alle medewerkers nauwkeurig vastgelegd moeten worden, met zoveel mogelijk functiescheiding door het creëren van deelfuncties, waarbij is te voorkomen dat geen nieuwe uit controle-oogpunt ongewenste functiecombinaties ontstaan. Deze afbakening van bevoegdheden zal via effectieve maatregelen van toegangsbeveiliging (zie hierna) doorgetrokken moeten worden tot in de computerprogramma's en de gegevensverzamelingen (in het laatste geval liefst tot in de onderscheiden gegevensvelden). Indien mogelijk zal een afzonderlijke systeembeheerder moeten worden aangesteld; waar dat problematisch is kan voor een combinatie met een pure registrerende of controlerende deelfunctie worden gekozen. Hetzelfde geldt voor een - hoewel in deze omgevingen niet direct te verwachten - speciale beveiligingsfunctionaris ('security-officer').

Dat er op dit terrein in de praktijk echt wel mogelijkheden zijn moge blijken uit de eerste voorlopige resultaten van een thans lopend onderzoek via controlerend accountants ter zake van de situatie bij door hen gecontroleerde organisaties.³ Het betreft de tot op heden bekend zijnde gegevens van 42 (anonieme) kleinschalige organisaties, waarvan 9 productie- of productie- en handelsondernemingen, 10 handelsondernemingen, 13 commercieel dienstverlenende ondernemingen (i.c. financiële instellingen), 4 overheidsinstellingen en 6 private non-profit-instellingen. De gemiddelde personeelsomvang bedroeg 52 personen, welk gemiddelde echter nogal is beïnvloed door zes grotere organisaties met tussen de 100 en de 200 werknemers, voornamelijk in de groep productiebedrijven.⁴ Het gemiddelde van de overige 36 organisaties bedroeg ca. 37 personen.⁵

In ongeveer tweederde van de gevallen werd gemeld dat er sprake is van functiescheiding tussen de ontwikkeling van systemen (inclusief wijziging) en de feitelijke elektronische gegevensverwerking. Na eliminatie van de gevallen waarin alle systeemontwikkeling extern plaatsvindt wordt de uitkomst iets meer dan 50%. Nagenoeg dezelfde uitkomsten gelden voor de functiescheiding tussen systeemontwikkeling en de controlerende functie(s). (Dit betrof niet alle dezelfde organisaties). In bijna de helft van de gevallen werd functiescheiding gemeld tussen de feitelijke elektronische gegevensverwerking en de controle op deze verwerking. In toch nog bijna 40% van de situaties werd gesproken van functiescheiding tussen de feitelijke elektronische gegevensverwerking en de gebruikers ten behoeve waarvan deze verwerking plaatsvindt. In ruim 30% van de gevallen wordt voorts melding gemaakt van een van alle andere functies losstaande functie bewaring van documentatie, programma's en gegevensbestanden.

Kortom op zich in totaliteit geen ideale situatie, zoals ook was te verwachten, maar blijkbaar zijn er toch organisaties waarin een en ander ook economisch haalbaar is. In geen enkele situatie werden alle vijf genoemde functiescheidingen aanwezig gemeld doch in 10 gevallen wel vier van de vijf. Hiertoe behoorden slechts drie van de eerder genoemde zes grotere organisaties. Ter illustratie kan tevens genoemd worden dat bij vijf organisaties (en niet

alle de kleinste) geen enkele van deze vijf functiescheidingen werd geconstateerd.

Waar echter het probleem van de nodige functiescheidingen niet volledig kan worden opgelost zal een serie andere maatregelen moeten worden genomen om de ergste consequenties te voorkomen. In de navolgende subparagrafen zal hier mede op worden ingegaan.

3.4 Beheersing van de systeemontwikkeling

In veel kleinschalige organisaties zal gewerkt worden met gekochte standaardprogrammatuur en/of vindt systeemontwikkeling (inclusief het onderhoud) extern plaats. De vrees voor ongeauthoriseerde wijzigingen behoeft in dat geval minder groot te zijn, mits gezorgd wordt dat de programma's niet in broncodevorm ter beschikking staan. Het nadeel hiervan, namelijk de grote afhankelijkheid van externe leveranciers die mogelijk in continuïteitsproblemen kunnen komen, kan opgelost worden door bijvoorbeeld deponering van de source bij een onafhankelijke derde (notaris of anderen). Belangrijk is wel dat gebruikers voldoende kunnen participeren in de besluitvorming tot aanschaf c.q. wijzigingsopdracht, om latere gebruikersproblemen te voorkomen. Deze zouden, afgezien van de directe nadelige invloed op de kwaliteit van de informatieverzorging, een bron van ongeauthoriseerde wijzigingspogingen kunnen zijn. De hoogste leiding zal in dit besluitvormingsproces zelf ten nauwste betrokken moeten zijn, gezien haar normaliter controlerende rol in de kleinere organisatie, alsmede voor de afweging inzake de prioriteiten van de diverse gebruikerswensen en de kosten versus baten. Een sluitend contract met de externe ontwikkelaar(s) met duidelijk afgebakende verantwoordelijkheden en aansprakelijkheden is van wezensbelang (ook ten aanzien van het noodzakelijk onderhoud in de toekomst) evenals het uitgebreid testen door de gebruikers vóór acceptatie.

Bij interne ontwikkeling zal - afgezien van zaken als gebruikersparticipatie en testen - bij gebrek aan adequate functiescheiding de nadruk moeten liggen op afdoende toegangsbeveiliging tot de voor productie geaccepteerde programma's en de documentatie daarvan, en op maatregelen als het verbieden van interpreters en het onder onafhankelijk beheer stellen van compilers en van utilityprogrammatuur. Naast dergelijke preventief werkende maatregelen zal er behoefte aan zijn, dat eventuele programmawijzigingen of pogingen daartoe volledig geregistreerd worden. Dit kan via een stringent voorschrift om alle wijzigingen te documenteren (zonder meer al nodig voor effectieve en efficiënte systeemontwikkeling in de toekomst) en een adequate systeemlogging (zie verder onder controleerbaarheid hierna). Deze maatregelen zullen niet afdoende zijn tegen kwaadwillenden, doch zal hun activiteiten wel bemoeilijken (bijv. noodzaak om op externe apparatuur te ontwikkelen). In ieder geval zal het onopzettelijke ongewenste wijzigingen kunnen voorkomen of achteraf traceren.

Door de beperkte automatiseringsdeskundigheid en het geringe bewustzijn van controlenoodzaak intern, zal een relatief belangrijke rol kunnen zijn weg-

gelegd voor externe deskundigen bij de systeemontwikkeling. Hiertoe behoort ook de accountant waar het betreft het tijdig rekening houden met interne controlemaatregelen als toegangsbeheersing, ingebouwde en geprogrammeerde controles, loggingvoorzieningen, waarborg voor een audit-trail en dergelijke.

3.5 Toegangsbeheersing

De beheersing van de toegang tot de apparatuur, de programmatuur, de gegevensverzamelingen (bestanden) en de documentatie betreft alle mogelijke vormen van benadering (fysiek, via raadpleeg- en/of wijzigfuncties enz.). De lokatie van de apparatuur bij kleinschalige automatisering (doorgaans op de gebruikersafdeling) roept extra problemen op. Zonder de dagelijkse gang van zaken al te veel te verstoren dient toch zoveel mogelijk tot isolering of afsluiting te worden gekomen. Te denken valt aan sleutels, plaatsing achter glaswanden, verzegeling van bepaalde essentiële aansluitingen (console) en dergelijke.

Meestal bevinden ook de programmatuur en de gegevensbestanden zich in de onmiddellijke nabijheid van de computer, veelal op diskettes. Een goede maatregel kan dan zijn om één persoon (als deelfunctie) de verantwoordelijkheid voor het beheer daarvan te geven (vooral de uitgifte en inname na bevoegd gebruik en de zorgvuldige bewaring waarbij programma's en gegevensbestanden gescheiden zijn), mits betrokkene geen daarmee incompatibele nevendeelfuncties heeft. Bij multi-user-systemen bevinden de belangrijkste programma's en gegevensverzamelingen zich veelal continu online op de computer. De toegangsbeveiliging zal dan in het systeem dienen te zijn verankerd. Toepassing van wachtwoorden is in de besturingsprogramma's van veel kleinere computers van hedentendage (nog) niet ingebouwd. Soms is het dan wel optioneel te verkrijgen. In andere gevallen kan getracht worden in de applicatieprogrammatuur bepaalde log-in-routines in te (laten) bouwen. Wel zal toepassing van (geheel op het principe van geheimhouding stoelende) wachtwoorden binnen de kleinschalige informele sfeer eerder ineffectief blijken te zijn dan in grotere strak gereguleerde organisaties. Om die reden verdient het aanbeveling alleen echt gevoelige of essentiële zaken af te scherpen. De toegangsbeveiligingssystemen van de (nabije) toekomst als vingerafdruk- en stemherkenning zullen vanwege het kostenaspect vooralsnog niet binnen het bereik van de kleinere organisaties komen.

Bijzondere aandacht verdient de utilityprogrammatuur waarmee rechtstreeks in gegevensbestanden kan worden gemuteerd; een oplossing is loskoppeling van het systeem en beheer op onafhankelijk voldoende hoog niveau (bijv. de leiding).

De kleinschalige omgeving heeft in dit kader echter ook voordelen ten opzichte van de grotere organisatie; omdat iedereen iedereen kent en weet wat zijn taak is, is het oogtoezicht een vaak doeltreffend middel.

3.6 Controle op invoer, verwerking en uitvoer

De tekortkomingen op het punt van de functiescheidingen alsmede de informele organisatie bemoeilijken het hanteren van invoerauthorisatiepro-

cedures, hetgeen bij interactieve transactiegewijze verwerking toch al een probleem is. Vaak is het wel mogelijk om kleine series (batches) basisgegevens tegelijk te verwerken en dan ook met voortellingen te werken, of ingevoerde transacties tijdelijk op een transactiebestand te zetten en pas na controle te laten verwerken (on-line invoer, batch-verwerking). Ook is een mogelijkheid om de ingevoerde transacties achteraf te sorteren en te tellen ter vergelijking met de invoerverslagen of uitvoer. Wenselijk is dan dat de computer bij invoer aan elke transactie een unieke identificatie toekent.

Daarmee komen wij op het punt dat de kleinere systemen tot op heden veelal niet het grote scala aan ingebouwde en geprogrammeerde controles ten aanzien van de juistheid en de volledigheid van de invoer kennen als bij de grootschalige automatisering, in het bijzonder niet in de besturings-programmatuur. Getracht moet worden de meest fundamentele invoercontroles te installeren in in ieder geval de applicatieprogrammatuur.

Hetzelfde geldt ten aanzien van geautomatiseerde controles op de juistheid en volledigheid van de verwerking van de ingevoerde gegevens door de computer. De feitelijke verwerking heeft voorts verhoogde risico's vanwege het ontbreken van gespecialiseerde werkvoorbereiders en operateurs en de veelal onduidelijke of onvolledige gebruikershandleidingen. Ter voorkoming dat programma's en gegevensbestanden onnodig lang aan allerlei risico's zijn blootgesteld, verdient het aanbeveling, dat ondanks het streven naar directe verwerking (waar dat voor een goed bedrijfsproces nodig is), er voor minder dringende zaken duidelijke roosters worden opgesteld wanneer wat verwerkt kan worden. In aansluiting hierop kan dan (bij gebreke van een automatische systeemlogging) een logboek bijgehouden worden (wie, wanneer, wat, met behulp van welk programma, hoeveel en dergelijke).

In deze omgeving met een relatief groot gebruik van kwetsbare floppy-disks is het belangrijk dat gezorgd wordt voor veilige opberging van de informatiedragers buiten de directe verwerkingstijd en voor een sluitend identificatiesysteem (doorgaans alleen mogelijk met externe labels) met bijbehorende administratie.

Ten aanzien van de uitvoer zal ook de kleinschalige organisatie niet kunnen ontkomen aan een zekere formalisering zoals duidelijke en unieke identificatie met volledigheidscntrole op het aantal kopieën en beheersing van de verspreiding. Een voordeel van de kleinere organisatie kan soms weer zijn, dat doorgaans bij velen bekend is wie tot wat bevoegd is, waardoor in de directe werkrelaties grof misbruik eerder zal worden geconstateerd.

Bijzonder belangrijk gezien de diverse zwakheden in de interne controle zal zijn de kritische beoordeling van de uitvoer (met inbegrip van de daaraan voorafgaande mutatielijsten) door de bevoegde gebruiker, dan wel door een afzonderlijke controlefunctionaris (eventueel als deelfunctie).

3.7 Waarborgen voor de continuïteit

Een aantal zaken is hiervoor al aan de orde geweest (onder andere fysieke bescherming apparatuur en programma- en gegevensbestanden en bepaalde andere toegangsbeheersingsmaatregelen).

De noodzakelijke back-up (op een andere lokatie) van programma's en

gegevensbestanden (vooral bij interactieve transactiegewijze verwerking frequent nodig) wordt in de kleinschalige omgeving bemoeilijkt bij het hanteren van uitsluitend diskettes als opslagmedium. Dit wordt al snel een moeizaam en onoverzichtelijk gebeuren. Investering in bijvoorbeeld magneetbandvoorzieningen zal dan nodig zijn, dan wel is men aangewezen op regelmatige uitdraai op papier. Het laatste geeft echter weer minder snelle en dus kostbaarder herstel mogelijkheden wanneer er werkelijk wat mis gaat.

Vaak wordt ten onrechte gedacht dat uitwijk naar andere apparatuur geen probleem zal zijn omdat gewerkt wordt met veel voorkomende apparatuur en standaardprogrammatuur. In de praktijk blijkt door andere versies en individuele programmatuuraanpassingen, andere informatiedragers, of door pure capaciteitsbezettingsproblemen, een niet of weinig onderbroken voortzetting van de verwerking bij bijvoorbeeld relaties met soortgelijke apparatuur vaak niet te lukken. Tijdige vervanging door de leverancier is meestal ook niet goed mogelijk. Ter voorkoming zou gedacht kunnen worden aan de aanschaf van een tweede computer. De kosten hiervan kunnen in het niet vallen bij de mogelijke schade in geval van calamiteiten. Een adequate schadeverzekering (inclusief uitwijk- en reconstructiekosten) blijft overigens een aanbevelenswaardige zaak.

Beveiliging tegen brand, waterschade en dergelijke zal zich om dezelfde prijstechnische redenen naar verhouding meer moeten richten op de gegevensverzamelingen en sommige programmatuur dan op de apparatuur. De investering in bijvoorbeeld datasafes voor de informatiedragers en beveiliging van de stroomtoevoer (met name als relatief langdurig gebruik van interne geheugenruimte plaatsvindt) zal ook in kleinere organisaties niet achterwege mogen blijven.

Een bijzonder probleem in de kleinschalige automatiseringsomgeving kan voorts nog zijn dat kennis van de bediening van de computer slechts bij één persoon aanwezig is met alle consequenties van dien bij ziekte of vakantie. Tijdige training van voldoende personen is dan ook noodzakelijk naast goede schriftelijke handleidingen. Het voordeel daarvan is bovendien, dat roulering van werkzaamheden kan plaatsvinden hetgeen een doeltreffend middel kan zijn voor de controleerbaarheid.

3.8 Controleerbaarheid

Tot de maatregelen van interne controle behoort ook het treffen van voorzieningen, die het mogelijk maken dat een onafhankelijke beoordeling (primair intern door de leiding of speciale controlefunctie, secundair door de externe accountant) kan plaatsvinden van de juistheid en volledigheid van de gegevensverwerking (in continuïteit) met inbegrip van de naleving van de andere interne controlevoorschriften.

In de eerste plaats zal daartoe nodig zijn een goede beschrijving van de organisatie (onder andere taken, bevoegdheden) en verdere documentatie van het informatiesysteem. Door de informele wijze van werken zal dit in kleinschalige organisaties nog wel eens problematisch zijn. Ook als de systeemontwikkeling buitenshuis plaatsvindt zijn er op dit punt tekortkomingen te verwachten, omdat veel leveranciers in dit marktgebied te weinig

documentatie beschikbaar stellen (mede ter zelfbescherming). Uit het eerder genoemde praktijkonderzoek blijkt dat ten aanzien van een zestal onderscheiden delen van de systeemvastlegging in circa 10% van de onderzochte kleinschalige organisaties alle delen ontbraken en in circa 30% slechts 1 of 2 delen aanwezig waren en in nog eens 30% 3 onderdelen. In slechts 10% van de gevallen waren alle gevraagde onderdelen aanwezig. Het meest ontbrak een vastlegging van de wijze en resultaten van systeem- en programmatesten, conversie en schaduwdraaien.⁶

De in de vorige subparagraaf genoemde roulering van medewerkers is een effectief controlemiddel maar blijkt (wellicht begrijpelijk) in de praktijk niet vaak voor te komen (iets meer dan 10%). Verplichte vakantie (waarbij taken niet worden stilgelegd maar door anderen overgenomen) komt gelukkig vaker voor (in het onderzoek bij ruim 40% van de organisaties).

Zeer belangrijk is een automatische volledige vastlegging van alle op het systeem verrichte handelingen (in het bijzonder de wijzigingen in programma's en bestanden en de doorbreking van allerlei controles waaronder de passwordbeveiliging, ongeoorloofde toegangspogingen en dergelijke). Deze registratie dient te geschieden in een slechts voor bevoegden toegankelijk logbestand (met een adequate oplossing voor 'vollopen'), en de analyse van dat bestand dient met behulp van geschikte programmatuur effectief mogelijk te zijn. Helaas is zo'n voorziening in kleinere computers veelal niet ingebouwd en wordt uit kostenoverwegingen ook niet meer achteraf (indien mogelijk) aangebracht. Overigens heeft een dergelijke loggingsvoorziening ook alleen zin indien het gebruik van de computer niet mogelijk is zonder dat de logging functioneert. In het eerdergenoemde onderzoek werd toch nog in belangrijke mate (ca. 40% van de situaties) een automatische systeemlogging gemeld, welke niet omzeild, onderdrukt of overschreven kon worden. Minimaal dient een manuele logging (in een logboek) plaats te vinden; ook al is dit verre van waterdicht toch heeft het een zekere preventieve werking en detectiemogelijkheden. De daarvoor nodige discipline is echter blijkbaar toch een groot probleem in dit soort omgevingen, van handmatige logging bleek vrijwel nergens sprake in de onderzochte organisaties (waar het gebeurde ging het meestal alleen om abnormale zaken als reruns, herstarts en dergelijke). Soortgelijke conclusies gelden voor de automatische respectievelijk handmatige vastlegging van fouten en foutsignaleringen tijdens het gegevensverwerkingsproces.

De audit-trail waardoor elementen uit de uitvoer terug gevolgd kunnen worden naar de basisgegevens en indien nodig omgekeerd, is een onmisbaar onderdeel van het geheel van controleerbaarheidsmaatregelen. Bij veel financieel-administratieve standaardprogrammatuur voor mini- en microcomputers ontbreekt er tot op heden nogal wat aan auditrailmogelijkheden, wat het belang aantoont van aan de aanschaf voorafgaand overleg met bijvoorbeeld de externe accountant (c.q. de IAD van het concern). Belangrijk is ook dat deze controleerbare vastleggingen voldoende lang bewaard blijven (in voldoende onverdichte vorm) totdat de latere onafhankelijke controle heeft kunnen plaatsvinden. Het gebruik van diskettes als opslagmedium kan hierbij een probleem vormen. In het eerder genoemde praktijkonderzoek wordt door de respondenten in slechts een gering aantal situaties tot

een onvoldoende audit-trail, respectievelijk te korte bewaartermijnen, geconcludeerd.

In geval van massaliteit van de te controleren gegevens of het feit dat zij slechts machinaal leesbaar zijn (bijv. bij programmavergelijking) zal in het kader van de controleerbaarheid de behoefte bestaan aan controleprogrammatuur. Dit kan specifiek ontwikkelde controleprogrammatuur zijn doch dit zal voor kleinschalige organisaties doorgaans te duur zijn. Standaard-auditsoftware is voor mini- en zeker voor microcomputers momenteel ook nog slechts in uitzonderingsgevallen verkrijgbaar, nog afgezien van de toch nog relatief hoge kosten. Meestal kan veel van het gevraagde ook bereikt worden met bij het systeem behorende retrieval- of inquiry-programmatuur. Van de onderzochte organisaties blijkt dat laatste in ruim 40% het geval te zijn. In circa 10% beschikt men over of standaard-auditsoftware of specifiek ontwikkelde controleprogrammatuur. In enkele gevallen wordt ook ITF (integrated test facilities), embedded auditroutines, tagging en tracing toegepast. In ruim 10% van de organisaties had men de beschikking over meerdere van deze hulpmiddelen. In bijna 20% van de organisaties echter waren (afgezien van de vraag of dit noodzakelijk was voor de controleerbaarheid) op dit gebied geen faciliteiten aanwezig, noch werd daartoe een beroep gedaan op externe instanties (externe accountant, concern-IAD, leverancier en dergelijke).

Vanwege de zwakke functiescheidingen en andere i.c.-maatregelen zal in de kleinschalige omgeving controle achteraf aan de hand van de uitvoer en met bewijsmateriaal een belangrijke rol spelen. Doelmatig is om buiten de computer om totalen en dergelijke vast te leggen, bijvoorbeeld in standenregisters, ter vergelijking (periodiek) met uit de bestanden te maken tellingen. Van de onderzochte organisaties bleek in slechts circa 30% een dergelijke controle op een of andere wijze plaats te vinden. Fraai is als in het computersysteem zelf al een netwerk van controletotalen en verbandcontroles wordt opgebouwd en waarvan de resultaten worden weggeschreven in een speciaal, alleen voor bevoegde personen toegankelijk, bestand. In de kleinschalige automatiseringsomgeving is dit echter een nauwelijks voorkomend fenomeen (in het onderzoek in twee organisaties, beide overheidsinstellingen).

4. De invloed op de accountantscontrole

Het accent blijft in het navolgende liggen op het bijzondere van de kleinschalige automatisering versus de grootschalige automatisering, en dus niet op de verschillen in controle-aanpak ten opzichte van een niet-geautomatiseerde kleinschalige organisatie.⁷ Ook wordt niet meer ingegaan op de vraag of de zogenaamde kleinschalige organisatie überhaupt voor controle vatbaar is en tot wat voor soort verklaring een controle aldaar kan leiden.⁸ Verondersteld wordt een op goede gronden - met name de aanwezigheid van een informatieverzorgingssysteem met voldoende controleerbare vastleggingen (audit-trail) - aanvaarde controle-opdracht. De met ingang van 1984 uitgebreide wettelijke accountantscontroleplicht voor rechtspersonen zal ook een aantal van de in het begin van dit artikel gedefinieerde geau-

tomatiseerde kleinschalige organisaties betreffen, omdat, ook al is er sprake van een personeelsomvang van meer dan 50 personen (één van de drie wettelijke criteria), toch de typische kenmerken van kleinschalige automatisering aanwezig zijn, dan wel omdat bij een geringer aantal personeelsleden de twee andere wettelijke criteria (ten aanzien van omzet en balanstelling) worden overschreden.

De bespreking zal plaatsvinden aan de hand van de doorgaans gevolgde lijn: algemene oriëntatie op de te controleren organisatie en in het bijzonder de te controleren verantwoording, beoordeling opzet en goede werking van de interne organisatie (in het bijzonder de interne controle), opstellen controleplan.

4.1 Algemene oriëntatie op de te controleren organisatie en verantwoording

In feite zal deze oriëntatie in grote lijnen al vóór aanvaarding van de opdracht plaatsvinden, met name ten aanzien van de aspecten als hiervoor onder controleerbaarheid genoemd. Nadien zal meer in detail op zaken worden ingegaan. Bij deze oriëntatie is van bijzonder belang om de houding van de hoogste leiding onder de loep te nemen. De integriteit van de leiding zal boven alle twijfel verheven moeten zijn, er zal op dit niveau voldoende automatiseringskennis aanwezig moeten zijn alsmede een voldoende bewustzijn van de noodzaak tot interne controle. Voorts zal moeten blijken de correcte inzet van de leiding (eventueel met inschakeling van externe deskundigen) ten aanzien van belangrijke zaken als de systeemontwikkeling, het toezicht op de naleving van bepaalde voorschriften, het beheer van essentiële zaken als broncodeprogramma's, compilers, utilityprogramma's en dergelijke, de kritische beoordeling van de met het systeem verkregen informatie enz. maar ook met betrekking tot vanouds bekende zaken als het tekenen en verzenden van betaalopdrachten (na beoordeling van de bewijzen van verschuldigdheid, juiste tenaamstelling en bankrekening en dergelijke). Immers de bemoeienis van de leiding kan een compensatie zijn voor een op zich zwak intern controlesysteem.

Tegen een dergelijke bemoeienis pleit de kans op doorbreking van bepaalde dagelijkse procedures door een dominerende leiding (veelal aanwezig in kleinere organisaties) met als doel manipulatie van de cijfers. In de eerste oriëntatie op de te controleren verantwoording zelf zal de accountant dan ook met name moeten kijken naar de mogelijkheden en waarschijnlijkheden van overwaardering van activa en onderwaardering van schulden (of omgekeerd indien door bepaalde omstandigheden de leiding gebaat zou kunnen zijn met minder rooskleurige cijfers). Verder naar het bestaan van eventuele transacties met verbonden vennootschappen en de privé-kring van de leiding, eventuele bijzondere transacties of saldi rondom of op de balansdatum (vergelijking met eerdere cijfers, branchegegevens enz.) en dergelijke.

Van wezenlijk belang voor zijn later op te stellen controleplan is dat de accountant bij de oriëntatie op de verantwoording de 'materiality' van de verschillende te controleren posten vaststelt. Het gevaar van overmatige controle door de accountant is immers bij de kleinere organisatie met zijn zwakke interne controle zeer sterk aanwezig.

4.2 *Beoordeling opzet interne organisatie / interne controle*

De ten opzichte van grootschalige automatisering bijzondere aandachtspunten voor deze beoordeling zijn in paragraaf 3 hiervóór beschreven. Voor een meer op zichzelf staande checklist voor de kleinschalige automatisering kan daarnaast verwezen worden naar bijlage 1 van het begin dit jaar uitgekomen NIVRA-studierapport 17 'Kleinschalige automatisering en accountant'.⁹

Direct starten met het invullen van een vragenlijst (welke dan ook) is in het kader van een effectief en efficiënt uit te voeren controle-opdracht echter niet aan te raden. De waarschijnlijkheid is groot dat in veel kleinschalige organisaties immers tot de conclusie moet worden gekomen, dat de accountant niet of slechts op enkele onderdelen gebruik kan maken van interne controlemaatregelen. Met name bij gebrekkige functiescheidingen zal het vaak moeilijk zo niet onmogelijk zijn om via andere controlemaatregelen voldoende compensatie te vinden. Als dan besloten moet worden om voornamelijk gegevensgericht te controleren is vanuit het doel van de accountantscontrole gezien het uitgebreid analyseren (laat staan het ook nog beoordelen van de goede werking) van de interne controle verspilde tijd. Illustratief in deze is de opmerkelijke uitkomst van een enkele jaren geleden gehouden onderzoek onder Amerikaanse openbare accountants, waarbij meer dan 66% van de respondenten meldden, dat zij de goede werking van de interne controle hadden getoetst (compliance testing), ook als een vooronderzoek hen tot de conclusie had gebracht dat zij niet op het systeem konden steunen.¹⁰ Verwacht mag worden dat het in Nederland met deze vorm van overmatig controleren nog wel mee zal vallen, mede omdat in ons land er nauwelijks beïnvloeding is van gedetailleerde auditing standards.¹¹

Van overbodige werkzaamheden hoeft op dit punt geen sprake te zijn gezien vanuit de meer algemene functie van de accountant, waarbinnen hij via een managementletter de leiding kan wijzen op een aantal zwakheden bij de beheersing van het informatieverzorgingssysteem, de risico's die de organisatie daarmee loopt, en hij aanbevelingen kan doen ter verbetering. In zoverre kunnen deze werkzaamheden dan ook invloed hebben op de effectiviteit en efficiency van de accountantscontrole, zij het in toekomstige jaren.

Voor de korte termijn doet de accountant er verstandig aan om de risico's met betrekking tot het getrouwe beeld van de jaarrekening te inventariseren. De basis daarvoor heeft hij al gelegd bij de eerder genoemde oriëntatie op de organisatie en in het bijzonder op de te controleren verantwoording (met name de bepaling van de 'materiality'). Een doeltreffend en relatief eenvoudig te hanteren hulpmiddel is het opstellen van een transactiestroomschema, waarin het verband zichtbaar is tussen de belangrijkste transactiesoorten (zoals inkopen, verkopen, betalingen, ontvangsten) en de debet- en creditboekingen in het grootboek. Bij dit verband kunnen de belangrijkste tussenstappen aangegeven worden (bijv. facturen, betaalopdrachten, mutatieverslagen en dergelijke). Bedoeling is om de voor het opstellen van het controleplan benodigde meest kritische informatie in overzichtelijke goed leesbare vorm vast te leggen. Dit zal in het algemeen

heel wat minder tijd vergen dan de uitgebreide formulierenloopschema's en dergelijke die doorgaans bij de beschrijving van een systeem worden gemaakt.

Vervolgens dient de accountant zich een globaal inzicht te verwerven hoe deze trajecten (en met name de daarmee gerelateerde onderscheiden posten van de jaarrekening) beïnvloed worden door aanwezige of juist niet aanwezige interne controlemaatregelen. Op basis daarvan kan hij in een vroeg stadium bepalen, tot welke interne controlemaatregelen hij zich qua beoordeling van opzet en goede werking kan beperken teneinde er op te kunnen steunen.

Dit kan ook inhouden dat bepaalde posten van de jaarrekening, ondanks dat zij via een goede interne controleweg tot stand komen toch geheel gegevensgericht worden gecontroleerd, bijvoorbeeld omdat dat de snelste wijze is.

Een en ander wil niet zeggen dat de accountant in veel gevallen van kleinschalige automatisering nauwelijks naar de automatiseringsaspecten zou behoeven te kijken.

Hij zal soms meer dan globaal daarvan kennis moeten nemen, teneinde de omgeving waarin hij controleert te kennen en om te zien of hij bepaalde gegevens die hij bij zijn beoordelings- en verificatiewerkzaamheden wil gebruiken daartoe wel kan gebruiken. Veel cijfermateriaal komt tenslotte via het geautomatiseerd systeem beschikbaar en kan onderhevig zijn geweest aan opzettelijke of onopzettelijke fouten. Een ander belangrijk facet kan zijn de continuïteitswaarborging (back-ups, uitwijk- en reconstructiemogelijkheden en dergelijke). Als een organisatie sterk afhankelijk is geworden van haar automatisering kunnen problemen op dit terrein het voortbestaan van de organisatie direct in gevaar brengen, hetgeen ook van invloed kan zijn op de accountantsverklaring. In toenemende mate wordt de automatisering ook in kleinere organisaties bovendien steeds complexer en geïntegreerder, met minder mogelijkheden om gegevensgericht te controleren. Tenslotte zal de accountant ook vanuit zijn controlerende functie nog meer dan voorheen bij de systeemontwikkeling moeten worden betrokken, om tijdig de nodige waarborgen voor controleerbaarheid te laten inbouwen. Ook daarbij zal hij niet zonder een bepaalde kennis van het geautomatiseerde systeem van de cliënt kunnen opereren.

4.3 Opstellen controleplan

In aansluiting op de beoordeling van de interne controle per onderscheiden traject als hierboven genoemd, kan de accountant de keuze maken of hij de daar bijbehorende jaarrekeningposten systeemgericht of gegevensgericht (dan wel gemengd met accentverschillen) zal controleren. Zo zal hij ten aanzien van zaken die erg van belang zijn of hoge risico's in zich dragen maar onderworpen zijn aan een hoge mate van interne controle kunnen concluderen, dat hij - na vaststelling dat het systeem goed heeft gewerkt in de periode onder controle - vertrouwen kan stellen in de uitkomsten van het systeem (rekeninghoudend met het feit dat hij ook nog andere controlemiddelen toepast, zoals cijferbeoordeling). Voor het vaststellen van de

goede werking zijn een aantal instrumenten binnen de interne controle nodig, als genoemd onder het hoofd controleerbaarheid hiervóór. Met name ook een volledige systeemlogging die ook goed analyseerbaar is.

Waar sprake is van lage risico's c.q. een gering belang voor de jaarrekening, maar toch een sterke interne controle, kan hij op vergelijkbare wijze te werk gaan, en wellicht zonder uitgebreide toetsing van de goede werking. Zelfs zal hij de onderneming dan kunnen adviseren eventueel de interne controle te reduceren ter besparing van kosten. Waar lage risico's en belangen spelen en ook de interne controle niet sterk is kan het eveneens zijn dat hij gezien de immateriality mag besluiten om niet verder te controleren.

Waar echter sprake is van een hoog risicogebied (gezien vanuit het uiteindelijk doel, het oordeel over de jaarrekening) maar een zwakke interne controle zal de accountant zijn controle daarentegen duidelijk moeten intensiveren. Hij kan omdat hij geen steun kan vinden in de interne controle in dat geval overwegen om te trachten de goede werking van de computerprogramma's zelf, die de betreffende cijfers opleveren, vast te stellen. Een mogelijkheid is daarbij soms om zelfstandig de basisgegevens in te voeren met een eigen kopie van het geteste en goedgekeurde programma. Soms kan rechtstreekse beoordeling van het in productie zijnde programma plaatsvinden, hetgeen - afgezien van de wellicht overblijvende onzekerheid of alle takken van het programma gezien zijn - alleen zin heeft als er zekerheid bestaat dat tijdens de verwerking niet met een ander programma is gewerkt. Dit vereist weer een bepaald niveau van interne controle.

Meer waarschijnlijk is dat de accountant zijn toevlucht zal moeten nemen tot cijferbeoordeling, verbandscontroles, totalencontroles buiten de computer om, en verificatiewerkzaamheden in detail. Bij de uitvoering van laatstgenoemde soorten werkzaamheden kan het zeer effectief en efficiënt zijn om gebruik te maken van de computer van de te controleren organisatie of van een eigen computer. Een bijzonder probleem voor de accountant (met name de externe accountant) is wel dat hij te maken heeft met een erg grote variëteit aan apparatuur en programmatuur bij al zijn verschillende cliënten met evenveel op te lossen aansluitings- of conversieproblemen als hij zijn eigen audit-computer zou willen gebruiken. Mogelijk kan gebruik van de computer van de cliënt uitkomst bieden, mits daarop bruikbare controleprogrammatuur toepasbaar is (standaard audit-software of utilityprogrammatuur). Juist in de kleinschalige omgeving met zijn niet zo sterke procedures en controles kan dit diverse andere problemen met zich meebrengen, zoals het risico om bestanden van cliënten te verminken (de accountant zou dan ook moeten weigeren met een utilityprogramma te werken waarop nog een wijzigfunctie aanwezig is) en de mogelijkheid van manipulatie van de beoogde controletoeassing door personeel van de cliënt. In ieder geval is er het probleem van de noodzaak om zich in diverse verschillende computersystemen van verschillende cliënten te verdiepen.

Tot slot van een beschouwing over door de accountant toe te passen controlemiddelen mag wellicht nog genoemd worden de 'schriftelijke bevestiging' ('letter of representation') van de leiding, dat naar haar beste weten alle relevante zaken in de jaarrekening zijn opgenomen. Hoewel nooit een

substituut voor door de accountant zelf uit te voeren controles is het - zeker in de kleinschalige omgeving waar het extra moeilijk zo niet onmogelijk is voor de accountant om 'de volledigheid' vast te stellen - een bruikbaar element in de totale oordeelsvorming van de accountant. Het lijkt een goede zaak dat dit fenomeen thans in Nederland meer terrein lijkt te gaan winnen.

5. Slotopmerking

In feite is een dergelijke zeer sterk doelgerichte controle-aanpak bij elke organisatie groot of klein relevant; bij de kleinschalige organisatie zal dit echter op grond van kostenverhoudingen onontkoombaar zijn. Voorkomen moet ook worden dat uit vrees voor de zwakke interne controles er een soort van overcompensatie ontstaat door de aandacht te verleggen naar het controleren van alles wat maar controleerbaar is, ook van zaken die niet wezenlijk zijn voor het beeld van de jaarrekening of waarvan de controle-resultaten niet bijdragen aan de oordeelsvorming die daarover nodig is. Het gaat tenslotte om controle van processen en de uitkomsten van die processen en niet om controle van een machine.

Noten

1 Voor een meer gedetailleerd overzicht van de kenmerken van kleinschalige organisaties en van kleinschalige automatisering wordt verwezen naar een eerder artikel van de schrijver in *De Accountant*, juni 1984, blz. 720 t/m 725 en juli/aug. 1984, blz. 802 t/m 809 'Kleinschalige automatisering en betrouwbaarheid' (in het bijzonder blz. 721 t/m 724 en de daarin genoemde literatuur).

2 Zie het onder noot 1 genoemde artikel. Zie voorts onder meer H.B. Moonen en H. Mooy: 'Interne controle-aspecten bij kleinere organisaties, die gebruik maken van een small business computer', *De Accountant*, december 1983.

3 Het onderzoek wordt uitgevoerd door schrijver dezes binnen de activiteiten van de vakgroep accountancy van de Vrije Universiteit.

4 Criterium in het onderzoek is om praktische redenen een personele omvang van 50 behoudens in de gevallen dat een groter aantal (veroorzaakt door relatief veel uitvoerend lager personeel) duidelijk niet meer mogelijkheden tot controletechnische functiescheidingen biedt. Een tweede criterium is daarbij dan gehanteerd namelijk het ontbreken van een grotendeels of geheel bemand rekencentrum met de functies systeemontwikkeling, programmering, verwerking en tapebeheer en dergelijke. Naar een eventuele scheiding van deze laatstgenoemde functies is in het onderzoek dan ook niet meer gevraagd omdat zij a priori geacht worden niet gescheiden aanwezig te zijn.

5 Nader gepreciseerd betref het 8 organisaties met tussen 10 en 20 personeelsleden, 9 met tussen 20 en 30, 11 met tussen 30 en 50, en 8 met tussen 50 en 100 personeelsleden (n.b. alles inclusief de leiding ook als dat eigenaren betref).

6 Onderscheiden werden 1) organisatieschema's, 2) procedure- en transactiestroomschema's, 3) documentatie omtrent het geautomatiseerde deel van de gegevensverwerking, 4) functiebeschrijvingen, 5) schriftelijke procedures en voorschriften, 6) wijze en resultaten van systeem- en programmatesten, conversie en schaduwdraaien.

7 Voor een beschouwing hieromtrent wordt verwezen naar 'Audit and Control Considerations in a Minicomputer or Small Business Computer Environment' uit de serie Computer Services Guidelines van het AICPA, New York 1981.

8 Zie hieromtrent: J. H. Blokdijs: 'Accountantscontrole bij kleine ondernemingen', *De Accountant*, november 1983 (blz. 150 e.v.) en een reactie hierop van Drs. A. Schilder: 'Accountantscontrole bij niet-grote ondernemingen', *De Accountant*, juli/augustus 1984 (blz. 816 e.v.).

9 Belangstellenden voor een meer gedetailleerde lijst, te weten die welke gebruikt wordt in het eerdergenoemde praktijkonderzoek, kunnen deze bij schrijver dezes bekomen, zij het onder de - volgens opvatting van de schrijver - niet onredelijke voorwaarde, dat de vragenlijst binnen een termijn van enkele maanden ook werkelijk in een praktijkgeval wordt toegepast en de gegevens van de ingevulde lijst binnen die termijn ter beschikking worden gesteld voor het onderzoek.

10 D. D. Raiborn: 'Audit problems encountered in small business engagements', Auditing Research Monograph, no 5 AICPA, New York, 1982.

11 De Auditing Standards Board van het Amerikaanse Instituut heeft overigens ook SAS 43, Omnibus Statement on Auditing Standards uitgegeven. Hierin wordt een beperkte review van de interne controle toegestaan 'to obtaining an understanding of the control environment and the flow of transactions and to documenting the basis for the auditor's decision not (onderstreept H.v.d.P.) to rely on internal control'.