



# COMPACT

83/4

## Computer en Accountant

Uit de inhoud:

Back-up, restart en recovery  
(deel 2 recovery en restart)  
door: R. Bron

Password-protectie  
door: A. van der Drift

Gebruikersparticipatie:  
op verschillende wijzen beschouwd  
door: H. Frijters

How cheap computers are affecting external  
audit  
door: W. List, Thomson Mclintock & Co.

AC-ADMINISTRATIEVE ZAKEN

COMPUTER EN ACCOUNTANT

INHOUDSOPGAVE

- ° VAN DE REDACTIE 1
- ° BACK-UP, RESTART EN RECOVERY  
(DEEL 2: RECOVERY EN RESTART)  
DOOR R. BRON 4
- ° PASSWORD-PROTECTIE  
DOOR A. VAN DER DRIFT 19
- ° GEBRUIKERSPARTICIPATIE:  
OP VERSCHILLENDE WIJZEN BESCHOUWD  
DOOR H. FRIJTERS 23
- ° VERANTWOORDING VAN DE ENQUETE VOOR COMPACT 31
- ° DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE  
DOOR H. VEENMAN 42
- ° HOW CHEAP COMPUTERS ARE AFFECTING EXTERNAL AUDIT  
DOOR W. LIST, THOMSON MCLINTOCK & CO 47
- ° BOEKEN 53
- ° TIJDSCHRIFTEN 55
- ° ABCNIEUWS 67
- ° ONDERWIJS 79

Herfst 1983

## VAN DE REDACTIE

De herfst in het 10e levensjaar van Compact is voorbijgegaan zonder het voor u hopelijk vertrouwde verschijnen van uw gids in AC-land. Wij zijn laat dit keer met Compact ten gevolge van overstelpende werkzaamheden. Onze excuses voor deze vertraging.

Wanneer u dit leest is het reeds 1984:

**"Wij wensen u allen een Goed 1984 met veel moed!"**

U heeft ons de spiegel voorgehouden, althans diegenen die zich de moeite hebben getroost ons uw ingevulde enqueteformulier terug te zenden.

Het invullen ervan bezorgde u een hoop werk, ons een bron van inspiratie.

Van harte dank voor uw medewerking.

Voor ons betekent de uitkomst van de enquête:

Bijsturen!

- de toepasbaarheid van de verschafte informatie moet meer aandacht krijgen;
- de leesbaarheid dient te worden vergroot.

Kunt u reeds de elementen van verbetering in dit nieuwe Compactnummer herkennen?

- \* "Backup, Recovery en Restart deel II door R. Bron.  
De schrijver heeft beoogd de helpende hand te bieden aan hen die in de praktijk met deze complexe problematiek geconfronteerd worden. Hoe kan het herstel en de herstart van tevoren zodanig georganiseerd zijn dat bij een calamiteit de continuïteit van de gegevensverwerking toch gewaarborgd blijft.
- \* "Password-protectie" door A. van der Drift.  
Het gebruik van passwords, de uitgifte ervan alsmede het beheer van de beveiligingsprogrammatuur. Deze concrete maatregelen zijn noodzakelijk om de veiligheid van het systeem te waarborgen tegen ongewenste ingrepen van buiten het systeem.
- \* "Gebruikersparticipatie: op verschillende wijzen beschouwd" door H. Frijters in diens doctoraalscriptie.  
De redactie van Nieuws-in-brief is zo vriendelijk geweest toe te staan dit artikel over de participatie van gebruikers tijdens de systeembouw in ons blad over te nemen.

1983

Herfst 1983

- \* "How cheap computers are affecting external audit" door William List CA, MBCS, partner van Thomson McIntock & Co. KMG United Kingdom. Door de komst van vele nieuwe mini- en microcomputers wordt de accountant voor tal van praktische problemen geplaatst bij de uitvoering van zijn controle-opdracht of bij het uitoefenen van zijn adviesfunctie. Kan hij op zinnige wijze ook de micro/mini gebruiken?
- \* Ook het gebruik van de persoonlijke computer verheugt zich in een toenemende belangstelling. Het gebruik van het pakket Multiplan verschaft de mogelijkheid om zelf staten te maken met zelfgemaakte formules. U kunt hiermede over de drempel heen geholpen worden voor eigen computergebruik. In de rubriek Micro is door H. Veenman aandacht besteed aan het hanteren van de diskettes, in de rubriek Onderwijs heeft M. Duym meer concreet Multiplan met zijn toepassingen besproken.
- \* In ons commentaar op het buitengebeuren hebben de rubrieksredacties aandacht besteed aan actuele zaken zoals gevonden in Boeken, Tijdschriften en ABC-Nieuws.

Wij ruimen gaarne een plaats in voor uw commentaar. Ook uw ervaringen zijn voor ons/anderen van belang. Wij garanderen uw anonimiteit en die van uw cliënt.

Schrijft u ons eens hoe u plotseling voor onvoorbereide problemen werd geplaatst.

Hoe hebt u die opgelost? Onze secretaris neemt uw bijdrage gaarne in ontvangst.

Met de verheugende mededeling dat wij in 1983 tot nu toe 168 nieuwe abonnees hebben genoteerd sluiten wij dit nummer af.

Herfst 1983

COMPACT is een uitgave van de Automatisering en Controle-groep van Klynveld Kraayenhof & Co. (KMG).

Het doel van deze uitgave is informatie te verstrekken over ontwikkelingen op het gebied van automatisering en controle in binnenland en buitenland. De vermelde artikelen in de rubrieken Tijdschriften/ABC Nieuws worden daarom soms geheel, soms verkort opgenomen, tevens als regel voorzien van commentaar.

Deze informatie is in de eerste plaats bestemd voor diegenen, die in de algemene controlepraktijk werkzaam zijn.

**Redactie:**

- Drs. J.E. Huizenga,
- A.W. Neisingh,
- Prof. D. Steeman en
- H.J.M. van der Wielen (secr.).

Kopij kunt u inleveren bij de secretaris van de redactie.

**Adres:**

Prinses Irenestraat 59,  
1077 WV Amsterdam.

**Postadres:**

Postbus 7137  
1007 JC Amsterdam.

© 1983 Klynveld Kraayenhof & Co. Amsterdam.  
Nadruk van deze uitgave is toegestaan mits de volgende bronvermelding plaatsvindt:  
Overgenomen uit COMPACT, uitgave van de Automatisering en Controle-groep van Klynveld Kraayenhof & Co. (KMG).

Indien u belangstelling heeft voor meerdere exemplaren kunt u deze aanvragen bij de secretaris van de redactie, evenwel zolang de voorraad strekt (telefoon 020 - 5461394).

**Internationaal KMG Klynveld Main Goerdeler**

Herfst 1983

BACK-UP, RESTART EN RECOVERY

(deel 2)

door R. Bron

4. Recovery en Restart

In het eerste deel van dit artikel is gesteld dat het niet meer terecht is Back-up, Recovery en Restart in één adem te noemen.

Voor het uitvoeren van een succesvolle Recovery en Restart zijn niet in alle gevallen back-up kopieën noodzakelijk. Dit is mede afhankelijk van de soort storing/calamiteit (variërend van deelbeschadiging van een object tot algehele vernietiging van de informatiedrager).

Deze uitspraak verdient nadere nuancering.

Voor de categorieën besturingssysteem, toepassingsprogrammatuur en job control language zal in alle gevallen teruggegrepen moeten worden op de laatst aanwezige kopie.

De recovery techniek dient parallel te lopen met de back-up techniek (object of medium gericht).

Bij de categorieën gegevensverzameling is de situatie zodanig gewijzigd dat bij de Recovery en Restart gebruik wordt gemaakt van technieken waarmee niet terug hoeft te worden gevallen op back-up kopieën. Dit is het geval wanneer sprake is van real time on-line-verwerking.

Alvorens op de aspecten bij real time on-line-verwerking wordt ingegaan, volgt eerst een uiteenzetting over een speciale recovery techniek die in de praktijk voorkomt en betrekking heeft op alle vier categorieën (de mengvorm object en medium gericht).

Hierbij is een tweetal varianten mogelijk (zie figuur 12).

Variant a

Ingeval van storing worden de gemuteerde objecten in tijdsvolgorde aangebracht op de laatst gemaakte kopie van de informatiedrager.

Variant b

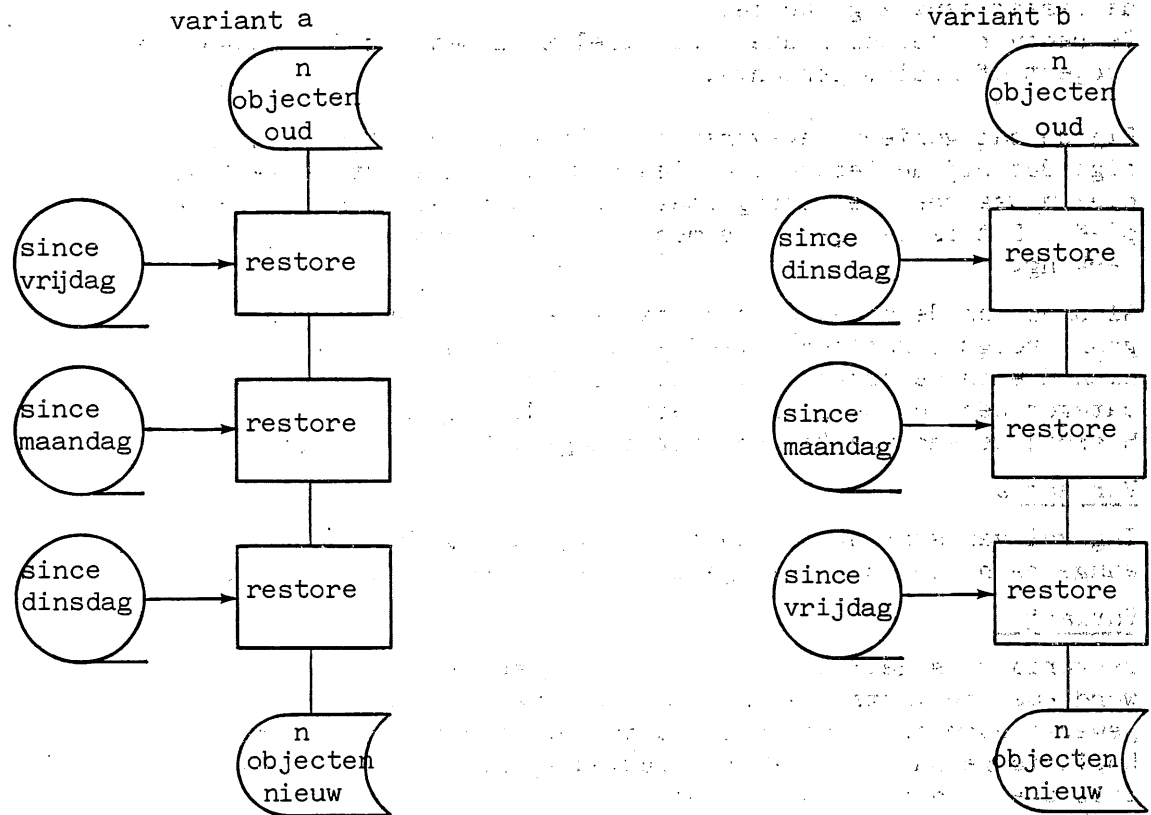
De variant is gelijk aan a met dit verschil dat bij Recovery gestart wordt met de laatst gemaakte since tape en vervolgens terug wordt gewerkt naar de oudste volgend op het tijdstip waarop een volledige kopie is gemaakt van de informatiedrager. De since tape bevat mutaties over een bepaalde periode.

Uit efficiency overwegingen is de variant b te verkiezen boven de variant a. Immers, bestanden op de "since-Vrijdag-tape", kunnen naderhand weer gemuteerd zijn en derhalve voorkomen op een latere "since-tape".

In de variant b wordt teruggewerkt en om deze reden speelt de datumregistratie voor de objecten in de index van de informatiedrager een grote rol. De "since-Dinsdag-tape" bevat de laatste versies van de gemuteerde objecten. Bij het terugzetten van de objecten wordt ook de datum van laatste wijziging weer teruggezet in de index. Zijn er op de "since-tapes" van oudere datum ook objecten welke reeds teruggezet zijn naar het te herstellen medium dan worden deze objecten op grond van de (oudere) datum overgeslagen.



BASIS SITUATIE



Figuur 12.

Herfst 1983

In een real time on-line omgeving wordt gebruik gemaakt van aanvullende (standaard) besturingsprogrammatuur (DBMS, TP-monitor), die technische faciliteiten bieden waardoor het gebruik van back-up kopieën bij de categorie gegevensbestanden niet altijd nodig is. De situatie wordt daardoor wel complexer. Doordat mutaties rechtstreeks op het bestand worden aangebracht, ontbreken de invoerbestanden. Bovendien zijn ingeval van storing de processen niet onder exact gelijke condities en omstandigheden te herhalen.

De standaardprogrammatuur biedt de mogelijkheid (stelt verplicht) gebruik te maken van de logfiles of de journalfiles. Bovendien bevat de standaardprogrammatuur standaard recovery-faciliteiten gebaseerd op het gebruik van logfiles of de journalfiles.

De functies van deze faciliteiten worden bepaald door de inhoud van de log- c.q. journalfile.

Deze logfile kan de volgende informatie bevatten:

1. before en after image;
2. alleen before images;
3. alleen after images;
4. mutaties zelf.

#### Ad 1.

Terminologie die hierbij ter sprake komt en enigerlei verduidelijking behoeft, is checkpoint, roll backward en roll forward.

Het principe van checkpoint is dat bepaalde informatie wordt weggeschreven op tape/schijf betrekking hebbend op de status van een actief proces (een programma in uitvoering).

Hierbij kan de situatie zich voordoen dat een checkpoint informatie bevat van alle op dat moment actieve processen (een foto van het totale interne geheugen van de machine dus inclusief opdrachtregisters, opdrachttellers, etc.) of informatie per proces.

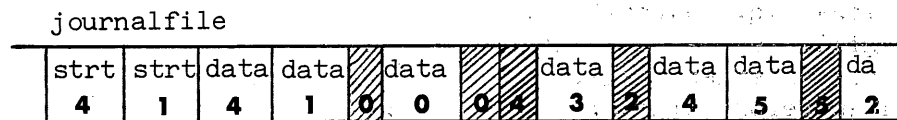
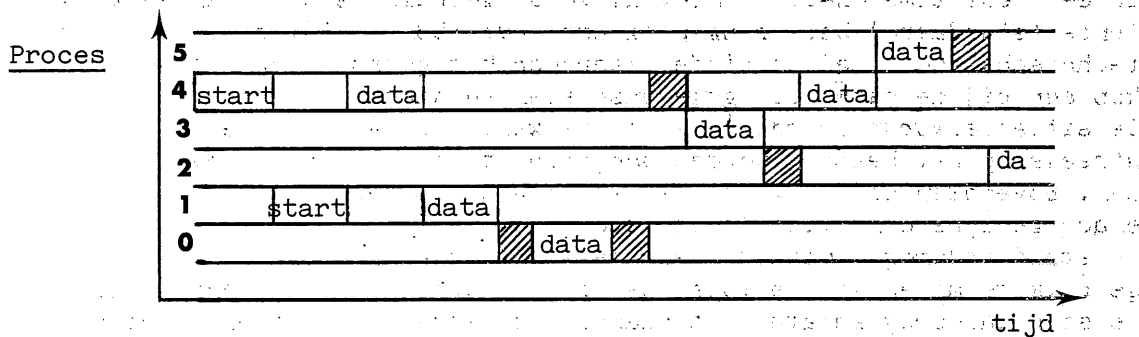
In het eerste geval wordt ook wel gesproken van een "snap shot". Deze "snap shot" informatie wordt over het algemeen gebruikt door systeemprogrammeurs bij storingen binnen de machine (trouble shooting). Als in dit artikel over checkpoint wordt gesproken wordt de statusinformatie per proces bedoeld.

Er zijn vier soorten checkpoints te onderkennen:

- een start checkpoint, welke altijd en automatisch wordt weggeschreven zodra een programma actief wordt;
- een einde checkpoint, eveneens altijd en automatisch aangebracht zodra een programma normaal beëindigd wordt;
- een commit checkpoint, een in de toepassingsprogrammatuur gedefinieerd checkpoint (dus optioneel);
- een abort checkpoint, een checkpoint dat gegenereerd wordt enerzijds zodra een programma stuk loopt, anderzijds op verzoek van het programma zelf op grond van een zogenaamd "Rollback-statement".

In figuur 13 wordt de volgtijdige inhoud van een journalfile weergegeven ten opzichte van de acties van actieve processen.





• 

strt
N

 = start checkpoint voor proces N

• 

--

 = commit checkpoint voor proces N

Figuur 13. Volgtijdige inhoud van een journalfile.

De statusinformatie wordt gebruikt om een verstoord proces (nadat de gegevens hersteld zijn tot op het punt van de checkpoint) te kunnen continueren.

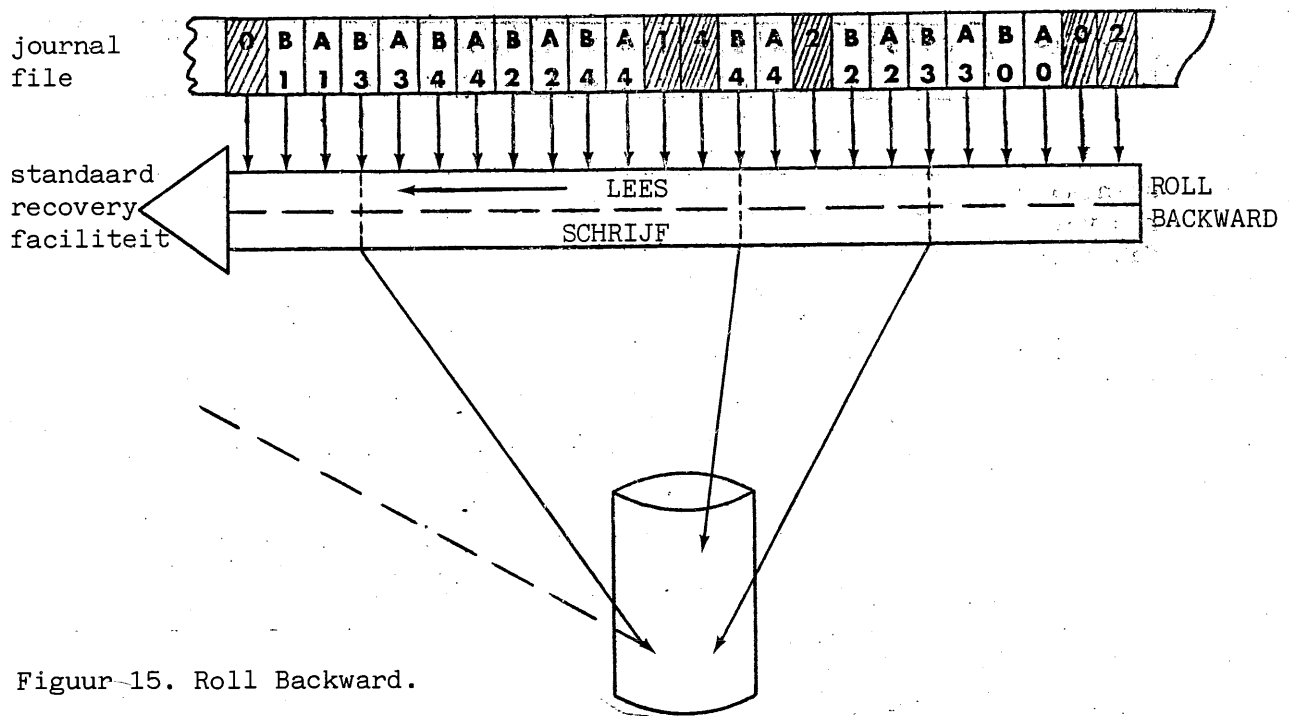
De terminologie van roll forward en roll backward wordt verduidelijkt met behulp van een voorbeeld ingeval van algehele vernietiging van de informatiedrager.

Bij recovery dient dus gebruik gemaakt te worden van een kopiebestand (zoon). Hierop dienen de verloren gegane mutaties te worden aangebracht. Dit geschiedt met gegevens voorkomend op de journalfile (in casu correcte before en after images).

Het meest efficiënt lijkt direct de after images weg te schrijven naar het kopiebestand om de situatie ten tijde van de calamiteit te bereiken (echter zoals vaak voorkomt: schijn bedriegt!).

De techniek die op deze wijze de situatie tracht te herstellen wordt "Roll Forward" genoemd (figuur 14).





Figuur 15. Roll Backward.

Als informatiedragers voor de journalfile worden gebruikt magneetband en magneetschijf.

Voor zover journalfiles op magneetschijf geregistreerd staan is het mogelijk dat met de signalering van een calamiteit door de harde software zonder menselijke tussenkomst Roll Backward uitgevoerd wordt waarna de verwerking opnieuw wordt voortgezet.

Deze herstelprocedure wordt ook wel "Recovery with warm restart" genoemd.

Wordt als medium de magneetband gebruikt dan is menselijke interventie nodig bij het plaatsen/verwisselen van de magneetbanden.

Een automatische restart is niet mogelijk.

Deze herstelprocedure wordt ook wel "Recovery with cold restart" genoemd.

### Ad 2. en 3.

Bevat de journalfile alléén before images of alléén after images dan wordt de problematiek alleen maar complexer.

Een Roll Forward alleen leidt niet tot herstel van de situatie vlak voor het optreden van de calamiteit.

Eigen programmatuur zal geschreven moeten worden om de Roll Backward faciliteit in enigerlei wijze te vervangen.

Het probleem is de vaststelling van de laatst correct verwerkte mutatie per proces.

Bij een Roll Backward, waarbij slechts after images beschikbaar

zijn, moet bedacht worden dat - aangekomen op de checkpoints - de direct na een checkpoint komende mutatie reeds verwerkt kan zijn.

Ook hier zal speciale programmatuur aanwezig moeten zijn om de laatst verwerkte mutatie te detecteren.

Herfst 1983

Ad 4.

Voor zover de logfile of de journalfile de mutaties zelf bevat, moeten uitgaande van de laatst genomen kopie van het gegevensbestand, de verwerkingsprocessen worden herhaald. Deze situatie komt echter zelden voor.

Wat wel voorkomt is dat de mutaties zelf deel uitmaken van het gegevensbestand en opgeslagen worden in een deelgebied van dat bestand. Dit wordt gedaan om een tweetal redenen. Enerzijds kunnen nu mutatieverslagen worden gecreëerd anderzijds kan het aantal journalfiles (in de tijd gezien) worden beperkt.

Tot slot wordt ingegaan op de situatie waarbij de calamiteit de informatiedrager treft. Deze kan de journalfile al of niet in combinatie met het gegevensbestand zelf bevatten.

Ingeval alleen de journalfile verloren is gegaan is er theoretisch nog niets aan de hand. Immers de gegevensverwerking kan gecontinueerd worden.

Zijn zowel de journalfile als het gegevensbestand betrokken bij de calamiteit dan zit er veelal niets anders op dan alle mutaties opnieuw in te brengen vanaf het tijdstip van de laatst genomen kopie.

In hoofdstuk 3 is uitgebreid ingegaan op Back-up; in dit hoofdstuk op Recovery en Restart.

De behandeling van de problematiek is tot nu toe niet uitputtend geweest. Dit is ook niet mogelijk door de aanwezigheid van specifieke aspecten, welke grote invloed hebben op de complexiteit als geheel.

Enkele van deze specifieke aspecten worden in het hierna volgend hoofdstuk nader besproken.

5. Specifieke aspectenA. Besturingssysteem en overige harde software (utilities)

Het besturingssysteem is over het algemeen ondergebracht op een verwisselbare magneetschijf (Eng.: Removable pack, Removable disk). Raakt de schijf in het ongerede als gevolg van een calamiteit dan is na schijfwisseling de machine weer beschikbaar voor produktie. De laatste tijd komt het gebruik van vaste schijven (snellere toegangstijd, grotere opslagcapaciteit) steeds meer in zwang. Dit heeft tot gevolg dat, indien deze schijf door een calamiteit onbruikbaar wordt, het besturingssysteem niet meer benaderbaar is. In deze gevallen zal een nieuwe systeemgeneratie moeten worden uitgevoerd met uitwijk naar een andere schijfveenheid.

Om bovenstaande reden is het aan te bevelen het besturingssysteem altijd aan te brengen op een verwisselbare magneetschijf.

## B. Gegevensbestanden

1. Logfile en/of journalfile kunnen in eerste instantie worden opgeslagen op een schijfgeheugen. In deze situatie is aandacht nodig voor het "wrap around" mechanisme hetgeen inhoudt dat als de bestandsruimte volgeschreven is, het systeem weer aan het begin van de bestandsruimte begint te registreren en daarmee oude mutaties overschrijft.  
In het besturingssysteem (of DBMS-software) dienen waarborgen te zijn opgenomen, welke het hiervoor aangegeven risico uitsluiten door periodiek te waarschuwen zodra bepaalde grenzen worden overschreden respectievelijk de verwerking te staken indien de bestandsruimte vol en geen andere vrije ruimte beschikbaar is. De verwerking mag pas worden voortgezet nadat de inhoud is gekopieerd op bijvoorbeeld een magneetband.  
Logfile en/of journalfile worden ook veelvuldig direct weggeschreven naar magneetband(en).  
Ook hier dient het besturingssysteem (of DBMS-software) te waarschuwen (en indien geen ander medium beschikbaar is, de verwerking te staken) indien de magneetband is volgeschreven. Dit om geen mutaties te verliezen.
2. Wordt bij geïntegreerde verwerking geen gebruik gemaakt van DBMS-software en staat het systeem naast real time on-line-verwerking ook batch-verwerking toe, dan kan niet zonder meer voor herstel van het bestand gebruik gemaakt worden van de logfile of de journalfile, aangezien de invloed van de batch-mutaties op ook middels real time on-line gewijzigde records niet bekend is. Herhaald wordt het reeds in hoofdstuk 4 gestelde "dat de processen niet onder exact gelijke condities en omstandigheden te herhalen zijn".  
Er zijn DBMS-systemen waarbij ook het batch-proces als een real time systeem gedefinieerd kan worden. In dit geval worden ook de batch-mutaties weggeschreven naar de journalfile en vervalt het hiervoren beschreven voorbehoud.
3. Met betrekking tot de recovery-problematiek bestaat een probleem als gevolg van het mogelijk niet synchroon lopen van log- c.q. journalfile.  
Ingeval gebruik wordt gemaakt van locale databases in combinatie met een centrale database moeten de mutaties in de locale databases ook terug te vinden zijn in de centrale database.  
Elke database heeft haar eigen journalfile. Is de gezamenlijke inhoudelijke waarde van de mutaties op de "locale journalfiles" gelijk aan de inhoudelijke waarde van de journalfile van de centrale database?  
  
In een configuratie waarbij meerdere processoren de aangeboden jobs (processen) verwerken geldt een synchronisatieprobleem van andere orde. Hoe wordt de registratie op de journalfiles uitgevoerd? Door één of door elke processor afzonderlijk? Indien dit gebeurt door één processor is volledigheid gewaarborgd.

Voor zover mutaties twee keer geregistreerd worden op gescheiden log- en/of journalfiles (het zogenaamde dual-logging system) kan de vraag gesteld worden: of de log- en/of journalfiles qua inhoud en volgorde identiek zijn (tijdverschillen in registratie!).

De problematiek wordt complexer naarmate er meerdere processoren aanwezig zijn voor de gegevensverwerking.

Dit kan uit recovery-oogpunt problemen opleveren als geen aandacht is geschonken aan de synchronisatie van de processen en de synchronisatie in de volgtijdelijkheid van de before en after images op de logfiles (journalfiles).

In dit hoofdstuk zijn tot dus verre kort een aantal specifieke aspecten behandeld welke de problematiek inzake recovery en restart complexer maken.

De problemen zijn in vele gevallen door de computerleveranciers onderkend waardoor software beschikbaar is om de problemen te voorkomen. Daarnaast zal de oplossing gevonden moeten worden in organisatorische maatregelen en procedures.

Hierna zal kort worden ingegaan op de invloed van de programmeerwijze op het recovery- en restartproces.

## C. Conversationeel/pseudoconversationeel programmeren en de invloed hiervan op het recovery- en restartproces

---

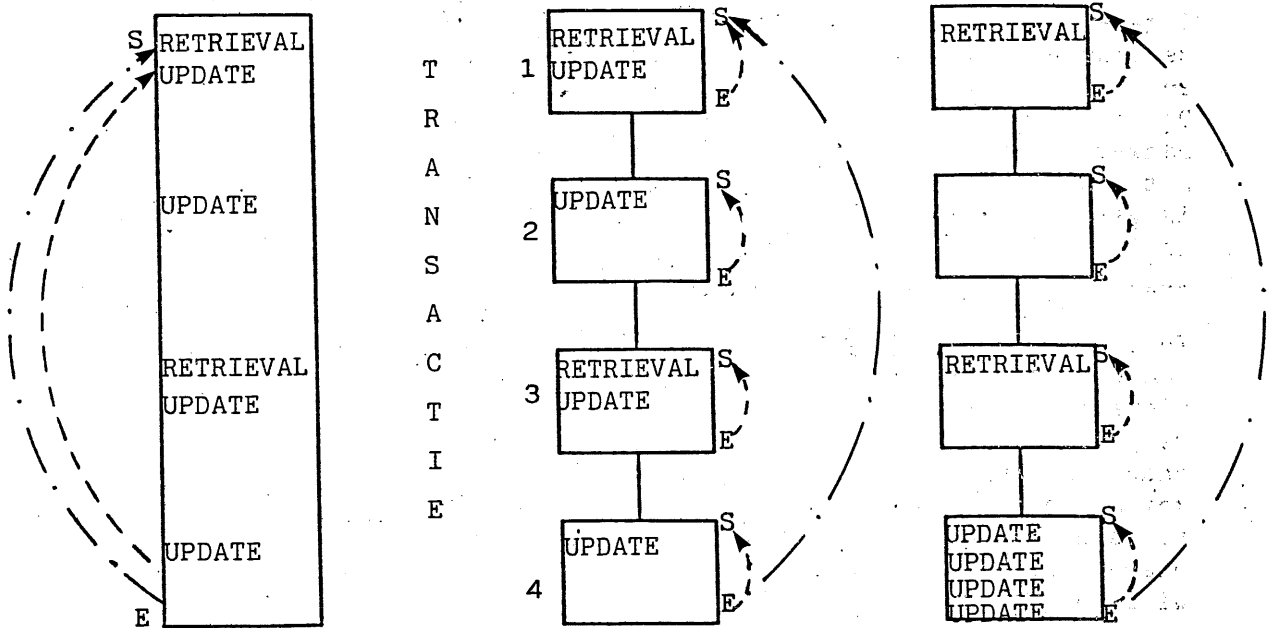
In hoofdstuk 4 is bij de verduidelijking van de begrippen roll forward en roll backward gesteld dat gebruikers - na herstel - een bericht dienen te ontvangen van de laatst goed verwerkte mutatie. En dat was dan dat!

Als echter niet op doordachte wijze is geprogrammeerd dan is dit doorgeven van de laatst goed verwerkte mutatie moeilijk realiseerbaar.

Een voorbeeld maakt dit duidelijk. Daarbij is het nodig dat de aard van een tweetal programmeringstechnieken nader worden beschreven. Bij conversationeel programmeren wordt alle coding behorende tot één transactie in één groot programma ondergebracht in tegenstelling tot pseudo-conversationeel waar de coding is "verknipt" tot kleinere logische eenheden ter verhoging van de efficiency van het computersysteem.

De processor van het computersysteem ziet zowel het "grote" programma als de "kleine" logische eenheden als aparte processen en handelt daar ook naar door het genereren van de respectievelijke checkpoints (start, einde en abort); zie voor een schematische weergave figuur 16.

Orderverwerking.



- transactie voor het computersysteem
- .-.-. transactie voor de gebruiker
- S - Start checkpoint
- E - Einde checkpoint

Figuur 16.

Stel bijvoorbeeld een orderverwerkingsproces waarbij zowel afnemer-gegevens ten aanzien van het totaal orderbedrag, ordergegevens als artikelgegevens ten aanzien van bestelde aantallen e.d. worden bijgewerkt.

De gebruiker heeft geen idee wanneer effectief gegevens worden bijgewerkt en kent slechts de order behorende bij een bepaalde afnemer. Als er iets fout gegaan is in de verwerking verwacht de gebruiker dat het systeem de laatste goed verwerkte order meldt.

Het systeem keert terug zoals beschreven is in hoofdstuk 4 tot het start-checkpoint van een proces en is zoals in het middendeel van figuur 16 is weergegeven niet in staat terug te keren tot het begin van de totale transactie.

De transactie is deels verwerkt; de gebruiker weet niet welk deel! De integriteit van de gegevens is niet meer gewaarborgd.

De oplossing hiervoor is dat alle wijzigingen op de gegevens zolang mogelijk worden tegengehouden en worden doorgeschoven tot het laatste "logische" deel alwaar dan de eigenlijke wijzigingen effectief worden gemaakt.

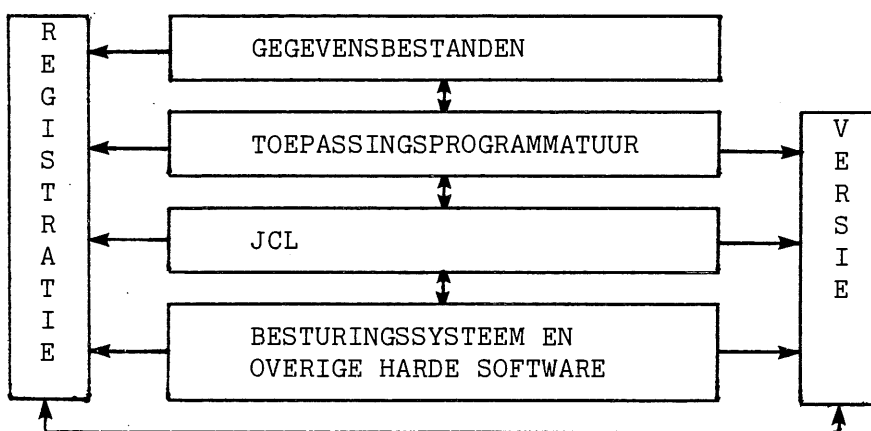
## 6. Controle-implicaties

In voorgaande hoofdstukken is uiteengezet "wat" er bij back-up, recovery en restart zoal komt kijken. Daarbij heeft de schrijver zich beperkt tot beschrijvende zaken. In dit hoofdstuk wordt ingegaan op een aantal controle-implicaties die back-up, recovery en restart met zich brengen. Die controle-implicaties zijn gericht op de continuïteit van de geautomatiseerde gegevensverwerking. Anders gezegd: waaraan dient aandacht te worden besteed uit oogpunt van continuïteit?

### 1. Procedures en voorschriften

Binnen de automatiseringsorganisatie zijn meestal één of meerdere procedures aanwezig waarin wordt aangegeven, welke acties ondernomen moeten worden om de continuïteit van de gegevensverwerking ingeval van calamiteiten/storingen in redelijke mate te waarborgen. Meestal zijn deze onvolledig en slechts gericht op de beveiliging van gegevens. Bovendien worden procedures niet aangepast aan veranderende (complexe) situaties. Om de continuïteit van de gegevensverwerking in redelijke mate te kunnen waarborgen dienen binnen de back-up-, recovery- en restart-procedures aandacht besteed te worden aan de vier categorieën besturingssysteem, programmatuur, JCL en gegevensbestanden alsmede de daarbij behorende bestandsregistraties. (In figuur 17 is de relatie welke bestaat tussen de categorieën schematisch weergegeven.) In het voorgaande is niet over deze registratie gesproken; zij is echter wel van eminent belang. In 6.3 wordt nader op het belang van de registratie ingegaan.

Een ander aspect dat in dit kader de aandacht verdient is de naleving van de procedures en voorschriften gericht op de continuïteit. De praktijk wijst uit dat er meestal wel procedures en voorschriften bestaan doch dat deze niet worden aangepast aan veranderende omstandigheden. Dit blijkt meestal uit het feit dat controle op de naleving van bestaande procedures niet wordt uitgevoerd. Als dit wel het geval is dan worden veranderde situaties eerder onderkend hetgeen dan aanpassing van de procedures tot gevolg heeft. Dit is echter geen ideale situatie.



Figuur 17.



Het is aan te bevelen binnen de automatiseringsorganisatie een functie te creëren die verantwoordelijk is voor de beveiligingsaspecten in brede zin. Deze dient op de hoogte te zijn van veranderingen die in apparatuur en programmatuur uit hoofde van beveiliging consequenties met zich brengen en derhalve zorg te dragen voor aanpassing alsmede naleving van procedures. Hier vallen back-up-, recovery- en restart-procedures ook onder.

## 2.A Besturingssysteem en overige harde software

Bij het besturingssysteem kunnen zich een aantal complicaties voordoen.

Een besturingssysteem wordt door de leverancier geleverd. Hierop wordt, evenals op andere programmatuur, onderhoud gepleegd.

Wijzigingen (PTF's) worden eveneens door de leverancier geleverd. Welke van die wijzigingen worden aangebracht is per situatie verschillend.

Daarnaast kunnen door de eigen organisatie wijzigingen c.q. aanvullingen (o.a. patches) worden aangebracht. Uit continuïteitsoverwegingen zijn een aantal situaties te onderkennen.

1. de meest ideale is dat alleen gebruik wordt gemaakt van het ongewijzigde besturingssysteem van de leverancier zonder eigen wijzigingen/aanvullingen (dit impliceert dat ook alle wijzigingen van de leverancier (PTF's) worden aangebracht.  
In geval van een calamiteit kan altijd worden teruggevallen op de leverancier.
2. minder ideaal wordt het als gebruik wordt gemaakt van het standaard besturingssysteem zonder eigen wijzigingen doch met een selectie uit de PTF's.  
Terugvallen op de leverancier wordt dan moeilijker tenzij bekend is welke selectie is gemaakt uit welke wijzigingen. Hierbij komt tevens het probleem dat de wijzigingen van de leverancier voorzien zijn van versienummering (release).  
In dit geval is het raadzaam na het aanbrengen van veranderingen een kopie van het bestand te maken.  
Bovendien is registratie noodzakelijk van de plaats waar de kopie van het bestand wordt bewaard. (Dit is meestal niet het geval.)
3. in het laatste geval worden op het besturingssysteem van de leverancier (inclusief alle of een selectie uit de PTF's) eigen wijzigingen/aanvullingen aangebracht.  
Terugvallen op de leverancier is ingeval van een calamiteit bijna niet mogelijk.  
De oplossing voor het continuïteitsprobleem moet binnen de automatiseringsorganisatie zelf worden gevonden.  
Kopieën van het besturingssysteem inclusief alle daarop aangebrachte wijzigingen, dienen aanwezig te zijn.  
Het volledigheidaspect van eigen wijzigingen verdient aandacht evenals de registratie van locaties waar bestanden zich bevinden.

Beklemtoond dient te worden dat, indien in de gevallen 2 en 3 geen kopieën worden gemaakt van de mutaties, de registratie zéér belangrijk is.

Indien de registratie handmatig plaatsvindt, is aan te bevelen deze in duplo te voeren en gescheiden op te slaan.

## 2.B Toepassingsprogrammatuur (source-coding)

Over het algemeen levert deze categorie niet zoveel problemen op als na het aanbrengen van mutaties in de produktie-omgeving twee kopieën worden getrokken welke gescheiden worden opgeslagen. Dit dient te geschieden direct na het aanbrengen van de wijziging. Wordt dit niet direct gedaan doch met een vaste periodiciteit dan kan het voorkomen dat, indien teruggevallen moet worden op back-up kopieën, met verouderde programmaversies wordt gewerkt. De back-up procedure dient er in te voorzien dat, alvorens produktie wordt gedraaid, de tussentijds geëffectueerde wijzigingen wederom worden aangebracht.

## 2.C Job Control Language

Deze categorie krijgt in het kader van de continuïteit vrijwel geen aandacht en komt in de back-up procedures niet voor. Toch is deze categorie belangrijk en wel met betrekking tot het volgtijdig gebruik van gegevensbestanden (in casu de versies van de bestanden). Als van alle overige categorieën kopieën, etc. beschikbaar zijn en de JCL ontbreekt dan is produktie niet mogelijk. De reproductietijd van de JCL dient niet te worden onderschat. De reproductie is in het geheel niet mogelijk als geen documentatie wordt bijgehouden. In het kader van de back-up en recovery dient aan de documentatie van de JCL derhalve aandacht te worden besteed.

## 2.D Gegevensbestanden

Deze categorie krijgt in het kader van continuïteit altijd de meeste aandacht.

Als over back-up, recovery en restart procedures wordt gesproken wordt meestal alleen aan deze categorie gedacht.

Er bestaat, als over gegevensbestanden wordt gesproken, de neiging alleen te denken aan stam- en mutatiebestanden en niet aan bestanden die met een speciale naam worden aangeduid (bijvoorbeeld journal-files). Dergelijke gegevensbestanden behoren eveneens aandacht te krijgen in de back-up en recovery procedure.

Het verdient aanbeveling de opslag zodanig te regelen dat generatie-versies met de daarop aansluitende mutatiebestanden bij elkaar worden gearhiveerd.

Bovendien dienen identieke bewaartermijnen in acht te worden genomen bij bestanden welke invloed op elkaar uitoefenen.

## 3. Registratie van bestanden

In het voorgaande is herhaaldelijk gesproken over registratie van bestanden.

Alhoewel deze registratie voor de continuïteit van groot belang is, krijgt zij niet de aandacht die zij eigenlijk zou moeten hebben. Immers als van alle categorieën back-up kopieën beschikbaar zijn doch niet bekend is waar zij zich bevinden dan is in geval van calamiteit de continuïteit van de gegevensverwerking niet gewaarborgd.

Benadrukt moet worden dat om een drietal redenen de registratie aandacht verdient.

1. Zoals hierboven is aangegeven is registratie noodzakelijk om aan te geven waar welke bestanden zich op welk moment bevinden. Wellicht is het overbodig te vermelden dat de registratie up-to-date moet zijn.
2. De registratie dient zelf beveiligd te worden en dient derhalve de aandacht te hebben bij het opstellen van back-up en recovery-procedures. In de praktijk komen zowel handmatige als geautomatiseerde registraties voor.  
In het eerste geval dienen stringente maatregelen te worden getroffen dat die handmatige registratie op een beveiligde (brandvrije, hittebestendige) plaats wordt bewaard. Dit vanwege het feit dat het praktisch ondoenlijk is de registratie in duplo te voeren en de kopie elders te bewaren. Als de registratie is geautomatiseerd dan valt de registratie onder de categorieën "programmatuur" en "gegevensbestanden".  
Zij dienen dan ook onder de desbetreffende back-up en recovery-procedures te vallen.
3. Last but not least het controle-aspect dat aan registratie kan worden ontleend.  
Door middel van de registratie kan de naleving van voorschriften en procedures worden gecontroleerd. Een probaat middel is het periodiek inventariseren van de inhoud van de opslaglocaties. Tevens kan de beweging worden gecontroleerd van de gegevensbestanden tussen de locaties.  
Voor het uitvoeren van deze inventarisatie is geen automatiseringskennis vereist. Tapes en schijven zijn herkenbaar aan externe labels die dienen voor te komen op de registratie zelf. Ingewikkeldheid dient te worden vermeden omdat het ingeval van calamiteit tot grote problemen aanleiding kan geven.

#### 4. Bruikbaarheid van back-up kopieën

Als voldaan is aan alle aspecten genoemd in voorgaande hoofdstukken en paragrafen, zou de indruk kunnen ontstaan dat rustig kan worden geslapen en er niets meer valt te vrezen. Ook hier levert de techniek haar bijdrage tot het ongewisse.

Immers hoe wordt vastgesteld dat de produktie van back-up kopieën feilloos is verlopen?

Op welke manier wordt gecontroleerd of de back-up kopieën als zij gebruikt moeten worden te lezen zijn? Meestal wordt aangenomen dat bij het maken van deze kopieën de techniek feilloos heeft gewerkt. Aan te bevelen is om aangemaakte kopieën terug te lezen of althans een steekproef hierop te houden.

Dit om onaangename verrassingen in toch al penibele situaties zoveel mogelijk te vermijden.

## Tenslotte

Getracht is in dit artikel een tip van de sluier op te lichten die er naar de mening van de auteur hangt over de complexe problematiek van back-up en recovery. Een poging is gedaan om de zaken op een rij te zetten en de lezer een indruk te geven van voornoemde complexiteit en bovendien diegenen de helpende hand te bieden die in de praktijk uit hoofde van hun beroepsuitoefening geconfronteerd worden met deze problematiek.

Daarnaast is getracht aan te geven waaraan aandacht moet worden besteed indien een oordeel moet worden gegeven over hoe het gesteld is met de continuïteit van de gegevensverwerking ingeval van calamiteit.

**COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.**

## PASSWORD-PROTECTIE

door A. van der Drift

### 1. Inleiding

In de journalistiek doet de automatisering duidelijk zijn intrede niet alleen door de automatiseringsondersteuning voor de totstandkoming van onder meer dagbladen, maar ook doordat er over geschreven wordt.

Het schrijven richt zich ditmaal niet zozeer op de techniek of op de werkeloosheid die automatisering ten gevolge heeft maar heden ten dage meer nadrukkelijk juist op het spektakel. Wat is immers meer spectaculair dan "criminaliteit"; bankinbraken per home-computer of atoombomlogje door verbindingen tussen deze computers en de Pentagon-apparatuur!

Hieraan wordt heel wat publiciteit gegeven. "Adviseurs" terzake verdienen er weer forse boterhammen mee; de filmindustrie speelt hier aardig op in.

Kortom er zou bijna sprake kunnen zijn van een "mode"-verschijnsel onder de naam van "Crime by Home-Computer".

Om de indruk uit menig persbericht ietwat te relativeren volgt een korte uiteenzetting over het samenspel tussen techniek en organisatie in het kader van password-protectie; een beveiliging die gebaseerd is op een geautomatiseerde herkenning van een persoon door de wachtwoordcontrole, aan de hand waarvan de bevoegdheden worden vastgesteld door de beveiligingsprogrammatuur.

### 2. Techniek en organisatie

De computerbeveiliging stoelt op twee hoofdpeilers:

- de techniek of technische ondersteuning;
- de organisatie en de daarin bestaande procedures en voorschriften.

Een simpele kluis dient hier als voorbeeld. De techniek wordt onder meer gevormd door de moeilijk doordringbare wanden alsmede het veelal geavanceerde slot.

De organisatie daaromheen wordt onder meer gevormd door de beperkte uitgifte van sleutels, de locatie van de kluis alsmede bijvoorbeeld de integriteit van de desbetreffende slotenmaker om geen kopie-sleutels achter te houden.

Bedenk echter dat geen slot perfect is; er bestaan immers "spectaculaire" meesterkrakers.

Analoog met het kluisvoorbeeld wordt bij geprogrammeerde toegangsbeveiliging de techniek gevormd door de beveiligingsprogrammatuur, de sleutel door het password en de organisatie door de wijze waarop deze programmatuur wordt gebruikt, de omgeving waarin deze programmatuur actief is alsmede de integriteit van de bouwer(s).

Herfst 1983

Bedenk ook hierbij dat (nog los gezien van gewone programmafouten) geen beveiligingsprogramma perfect is; er blijken immers "spectaculaire" meesterkrakers of zelfs krakertjes te bestaan.

Er zullen adequate organisatorische maatregelen dienen te worden getroffen teneinde elk risico zo veel mogelijk te beperken. Zo ook zullen er adequate technische ondersteuning door beveiligingsprogramma-tuur moeten worden geboden ten einde voortdurend ongeautoriseerde ingrepen te voorkomen.

### 3. Betekenis passwords

Een password heeft primair en veelal louter en alleen tot doel de beveiligingsprogrammatuur een mogelijkheid te bieden voor het vaststellen van de authenticiteit van de persoon, die in verbinding staat met de computer (middels een terminal).

Bijna altijd heeft men de beschikking over een toetsenbord, waarop het password desgevraagd kan worden ingetoetst.

Indien men de beschikking heeft over stem-, handschrift- of vingerafdruk-herkenningsapparatuur, gebruikt men dienovereenkomstige "passwords".

(Zou men een "algemeen" password willen invoeren ten behoeve van de continuïteit in geval van een onvoorziene afwezigheid van de gebruiker, dan kan men ook op deze geavanceerde apparatuur de vindingrijkheid botvieren. Denk bijvoorbeeld aan cassette-opname van stemgeluiden, simpele lijnen met behulp van een lineaal of handschoenafdrukken. Het zij echter toegegeven dat gebruik van dergelijke apparatuur de beveiliging ten goede kan komen, maar getuige de voorbeelden nog steeds in combinatie met adequate organisatorische maatregelen.)

### 4. Effectiviteit passwords

Ten behoeve van de gebruikers van passwords kunnen de navolgende eisen worden genoemd:

- kies geen algemeen voor de hand liggende passwords zoals initialen, e.d.;
- kies passwords met verschillende en meerdere tekens (bijvoorbeeld 5 tot 8 alfanumerieke tekens);
- houdt het password geheim en wijzig het frequent.

De navolgende ondersteuning van voornoemde eisen zou door de beveiligingsprogrammatuur kunnen worden geboden:

- accepteer geen passwords, die ouder zijn dan bijvoorbeeld 6 weken;
- accepteer geen passwords van identieke en/of minder dan vijf tekens;
- accepteer geen nieuwe passwords, die recentelijk reeds eerder zijn gebruikt.

## 5. Gebruik passwords

De volgende faciliteiten zouden door beveiligingsprogrammatuur kunnen worden geboden:

- maak een password nooit zichtbaar, noch op papier, noch op de terminal;
- sla de passwords versluierd (encrypted) op en/of beveilig de toegang tot deze opslag;
- accepteer geen initieel toegekende passwords; dwing eerst een wijziging af door de eigenaar;
- accepteer maximaal 3 pogingen tot het goed invoeren van het password per persoonsidentificatie. Log de foutieve pogingen met vermelding van persoonsidentificatie, terminalidentificatie, datum en tijd. Geef een duidelijk signaal van overschrijding aan standby computerpersoneel.

Koppel zo mogelijk bij overschrijding de verbindinglijn af, totdat geautoriseerd computerpersoneel dit herstelt;

- ondersteun zo nodig dubbele aanlog-procedures (aanmeldprocedures) vanaf meer dan één terminal;
- laat de terminal vermelden wie aan- en aflogd en zo mogelijk wanneer de persoon voor het laatst heeft aangelogd.

De eisen in dit verband zijn:

- beveilig de versluisingsberekening;
- beveilig fysiek de computerbestanden, waarop de passwords kunnen zijn vastgelegd (ook de back-up files);
- creëer zo nodig een aanlog-procedure bestaande uit twee gescheiden onderdelen;
- onderneem zo mogelijk direct actie op signalen betreffende het overschreden aantal pogingen.

## 6. Aanvullende maatregelen

De navolgende additionele faciliteiten zouden door beveiligingsprogrammatuur kunnen worden geboden:

- forceer een automatische log-off (afmelding gebruiker) na een bepaalde tijd waarin de persoon op de terminal niet actief is geweest;
- stel personen uitsluitend in de gelegenheid te communiceren met de computer op bepaalde uren van de dag met behulp van bepaalde door de beveiligingsprogrammatuur fysiek te herkennen terminals;
- accepteer geen actieve "applicatie-"programmatuur in het computergeheugen, die niet volgens de voorgeschreven toegangsregels in directe verbinding staat met een fysiek aangesloten terminal, die aanstaat.

Belangrijke organisatorische maatregelen zijn:

- het steeds uitschakelen van de terminal en pas aanzetten als men daadwerkelijk gaat communiceren met de computer;
- het eventueel fysiek beveiligen van de terminal.

## 7. Uitgifte passwords en beheer beveiligingsprogrammatuur

In de organisatie dienen procedures te bestaan en te worden nageleefd voor wat betreft:

- het verkrijgen van een persoonsidentificatie en initieel password;
- het herkrijgen van een door de eigenaar vergeten password door bijvoorbeeld het wederom verkrijgen van een nieuw initieel password of het toepassen van een envelopprocedure (het noteren van het actuele password en deze notitie deponeren in een gesloten envelop bij de direct hogere chef);
- het beveiligen van de beveiligingsprogrammatuur al dan niet met behulp van (andere) beveiligingsprogrammatuur;
- het verwijderen van de persoonsidentificatie en het password uit de computer, indien iemand wordt overgeplaatst of het bedrijf verlaat.
- het aanpassen van bevoegdheidsprofielen ingeval van wijzigingen in de organisatie.

## 8. Slot

De genoemde technische en organisatorische maatregelen zullen nauwelijks of niet allemaal binnen één omgeving worden aangetroffen. Dit is ook niet direct noodzakelijk, omdat enkele maatregelen compenserend werken voor de anderen.

Zo ook zal niet in elke organisatie een zo grote noodzaak tot optimale beveiliging door middel van password-protectie aanwezig zijn.

Tevens bieden lang niet alle beveiligingsprogramma's de genoemde faciliteiten en zal niet elke organisatie de discipline voor het naleven van de voorgestelde organisatorische maatregelen kunnen opbrengen, danwel geen controle op de naleving van genoemde maatregelen adequaat kunnen uitvoeren.

Overigens zij opgemerkt dat niet alle maatregelen terzake zijn vermeld. "No program (lees ook: procedure) is perfect".

Lezen wij echter de in de inleiding genoemde "spectaculaire" persberichten, dan kan per bericht geconstateerd worden, dat niet aan ten minste één van de, in die specifieke situatie relevante, genoemde maatregelen is voldaan.

De eerlijkheid gebiedt te vermelden dat de genoemde berichten ten minste één positieve functie vervullen.

Zij vestigen de aandacht op de noodzaak van geprogrammeerde toegangsbeveiliging voor wat betreft het onderdeel password-protectie.

**COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.**



## Gebruikersparticipatie: op verschillende wijzen beschouwd

door H. Frijters

(met welwillende toestemming van de Redactie van Nieuws-in-Brief overgenomen uit 83/4, 8e jaargang, augustus 1983)

### 1. Inleiding

Dit artikel vormt een verkorte weergave van een doctoraalscriptie (1).

Deze scriptie is geschreven in het kader van een afstudeeronderzoek voor de Interuniversitaire Interfaculteit Bedrijfskunde (I.I.B.) te Delft. Dit onderzoek is tijdens een stage uitgevoerd bij Klynveld Kraayenhof & Co., Organisatie-adviseurs (K.K.C.-O.A.) te Amsterdam. Ik ben daarbij vele mensen dank verschuldigd. Speciaal zou ik Aad Kranendonk R.A. (K.K.C.-O.A.) en prof. ir. H. Bosch (I.I.B.) willen danken voor de begeleiding van de afstudeerstage. De scriptie is in de documentatie van K.K.C.-O.A. aanwezig, evenals de literatuur waarnaar verwezen wordt.

Het onderzoek was gericht op de samenhang tussen de participatie van de gebruiker tijdens het ontwikkelingsproject en de centralisatiegraad van het te ontwerpen informatiesysteem. De centrale vraag daarbij was: Wat draagt die gebruiker bij in het ontwerpproces en onder welke omstandigheden vindt dit plaats?

Dit artikel heeft als centraal thema het ontwikkelingsproject van een informatiesysteem. In dit thema staan de aanpak van zo'n project en de consequenties daarvan voor het uiteindelijke informatiesysteem in de belangstelling. De vaak gehoorde ontevredenheid in de gebruikersorganisatie is de motivatie geweest voor de aandacht in dit onderzoek voor de rol van de gebruiker en de aanpak van het ontwikkelingsproject. Deze problemen tracht men in de automatiseringsliteratuur te voorkomen, door de nadruk te leggen op een methodische aanpak van een ontwikkelingsproject van een informatiesysteem (2).

De rol van de gebruiker krijgt in deze bespreking veel aandacht. Aangezien de verschillende gebruikers een aantal typische rollen in het project spelen, was het mijns inziens verhelderend om de gebruikers in vier types in de delen (3).

De vier groepen zijn:

- De beleidsbepalende of de beleidsvormende gebruiker (de leidinggevenden van de groep)
- de operationele gebruiker (deze persoon vervult een taak direct in het systeem)
- de passieve gebruiker (deze persoon maakt gebruik van de informatie die uit het systeem komt)
- de functionele gebruiker (deze persoon draagt verantwoording voor de materiële kwaliteit van het systeem).

Elk type speelt een specifieke rol in het project, maar een verdere uitsplitsing is zeker nog mogelijk.

De sociale en organisatorische consequenties van een ontwikkelingsproject blijken belangrijke implicaties te hebben voor de verhoudingen binnen de organisatie. De technische ontwikkelingen laten de geautomatiseerde informatiesystemen steeds "dieper" in de organisatie ingrijpen. De gebruiker zal daarom steeds meer keuzen moeten maken in het ontwerpproces. Daarmee wordt de rol van de gebruiker groter.

De opbouw van dit artikel is als volgt. Allereerst bespreek ik de organisatie via een invalshoek die erg verhelderend was voor het onderzoek. De daarop volgende paragraaf 3 schenkt aandacht aan de ontwikkeling van het informatiesysteem en daarna komt de relatie tussen de organisatie en het informatiesysteem aan de orde in paragraaf 4. Aangezien het afstudeeronderzoek ook twee case-studies bevatte, geeft paragraaf 5 een beschrijving van deze case-studies. Er wordt aandacht besteed aan het onderzoeksmodel, de gevolgde methode en het resultaat van het onderzoek: de conclusies uit de cases.

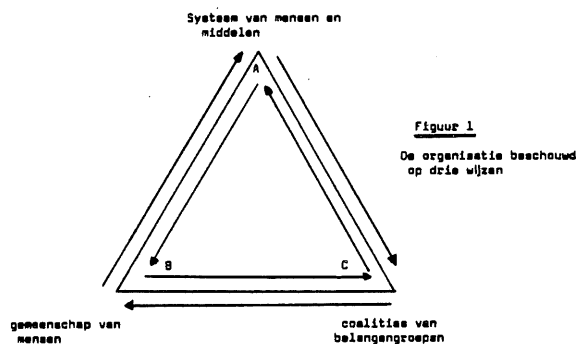
In paragraaf 6 is geprobeerd de theoretische en de praktische bevindingen te combineren tot conclusies. In de laatste paragraaf geef ik een richting aan die mogelijk een oplossing vormt voor de geconstateerde problemen.

## 2. De organisatie

Een informatiesysteem wordt ontwikkeld in een organisatie en beïnvloedt die organisatie op allerlei wijzen. Zoals in de inleiding is beschreven, wordt de invloed van het informatiesysteem op de organisatie steeds groter. In het onderzoek wordt de organisatie (in navolging van Bosch) op drie wijzen beschouwd (4). De organisatie wordt gezien:

- als een systeem van mensen en middelen, of
- als gemeenschap van mensen met eigen normen en waarden, of
- als coalities van belangengroepen.

De verhoudingen tussen deze drie zienswijzen beïnvloeden elkaar in de organisatie. In mijn scriptie is dit weergegeven als een "driehoek" (zie figuur 1).



De organisatie beschouwd op deze drie wijzen, tracht in wisselwerking met de omgeving de doelstellingen te verwezenlijken. Het organisatieveranderingsaspect van een ontwikkelingsproject is eveneens op drie wijzen te beschouwen. Dit kan een makkelijk hulpmiddel vormen bij de analyse van een project.

Meer in het algemeen kan men alle veranderingsprocessen binnen de organisatie in deze drie zienswijzen beschouwen. Zo wordt het ontwikkelingsproject van een informatiesysteem door deze drie beïnvloed. De automatiseringsdeskundige zal zich in eerste instantie concentreren op het ontwerpen van het informatiesysteem binnen de organisatie als systeem van mensen en middelen. Het ontwerpproces van het informatiesysteem heeft aldus een onmiddellijk zichtbare invloed op de verhouding t.o.v. de andere zienswijzen.

In navolging van Ganzevoort (5) en De Vries (6) wordt hier de nadruk gelegd op de irrationele aspecten van de organisatie. In het model (zie figuur 1) komt deze irrationaliteit vanuit de twee hoekpunten (b, c) in de driehoek. Het ontwikkelingsproject doorkruist allerlei verhoudingen in de organisatie. Deze aspecten komt de automatiseringsdeskundige ongewild tegen tijdens het ontwikkelen van een informatiesysteem. Het gedrag van de participanten raakt immers beïnvloed door de veranderende verhoudingen en hun posities daarbinnen.

## 3. De ontwikkeling van informatiesystemen

In de automatiseringsliteratuur wordt voor een ontwikkelingsproject van een informatiesysteem onderscheid gemaakt tussen de instrumentele aanpak en de ontwikkelingsaanpak (7). De rol van de gebruiker is bij de instrumentele aanpak kleiner, dan zijn rol bij de ontwikkelingsaanpak.

Bij de instrumentele aanpak ligt de verantwoordelijkheid voor het ontwerpproces volledig bij de deskundige. Tijdens de invoering moet de gebruiker of de opdrachtgever het ontwerp overnemen en daarna is het hun verantwoordelijkheid. Zij moeten besluiten of ze het ontwerp invoeren of niet. In de ontwikkelingsaanpak tracht men een leerstrategie te realiseren. Deze aanpak streeft ernaar dat iedereen een evenredige bijdrage levert aan het ontwerpproces. Het tracht zo én een leereffect voor de organisatieleden én een beter systeem te realiseren.

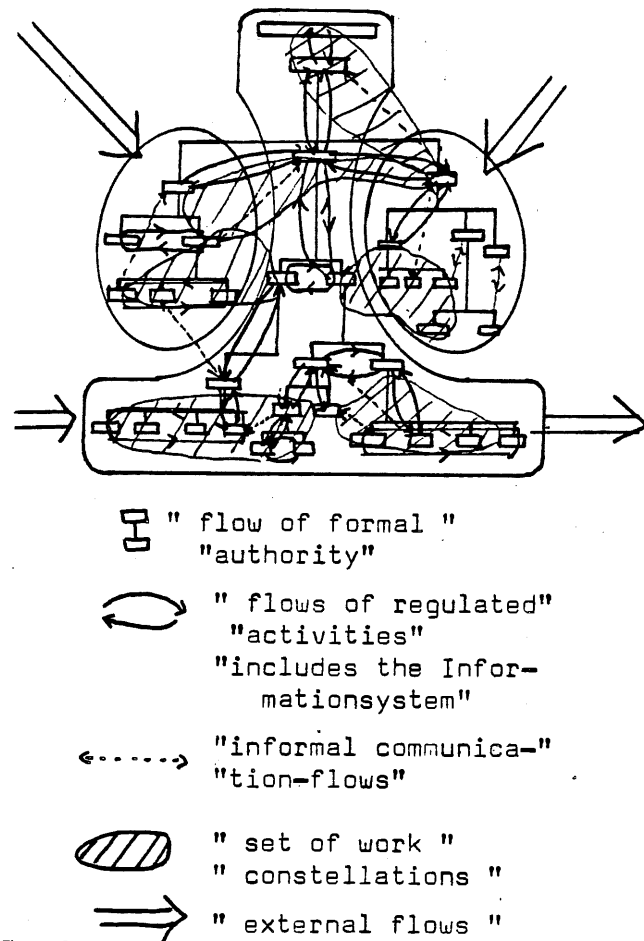
De beide aanpakken zijn uitersten die niet in hun extreme vorm in werkelijkheid zullen voorkomen. De aanpak in de praktijk bevat in meer of mindere mate aspecten van de beide uitersten.

De rol van de gebruiker neemt toe naarmate de aanpak meer aspecten van de ontwikkelingsaanpak bevat. De rol van de gebruiker wordt beïnvloed door de verhoudingen in de organisatie. Deze verhoudingen zijn te bezien binnen de drie zienswijzen van de organisatie en deze vragen de aandacht van de betrokkenen bij het project.

#### **4. Het informatiesysteem**

Het informatiesysteem is een van de middelen die een organisatie in staat stelt de informatie beter te verzamelen en te beheren. Deze informatie is noodzakelijk voor de bedrijfsvoering. In de organisatie kan men de informatie op meer wijzen verzamelen, verwerken en opslaan. Een deel van de informatie wordt op een formele, systematische wijze verwerkt. Dit vindt plaats via diverse processen, waaronder ook de geautomatiseerde verwerking m.b.v. de computer. Een conceptuele weergave van het stelsel van formele informatieverwerking vormt het informatiesysteem.

Het informatiesysteem is een aspectsysteem van het organisatiesysteem. De beïnvloeding vanuit de verhoudingen binnen de drie zienswijzen zal haar uitwerking hebben op de wijze waarop men een informatiesysteem ontwerpt en gebruikt. In het onderzoek werd de centralisatiegraad gebruikt als een voorbeeld van één aspect van een informatiesysteem. Het informatiesysteem was een té complex begrip om het volledig uit te werken in het tijdsbestek van het onderzoek. De centralisatiegraad is in het onderzoek praktisch ingevuld met behulp van het concept van Oonincx (8). Hij definieert de centralisatiegraad en met name een verschuiving daarvan als een verschuiving van activiteiten binnen het systeem. Deze activiteiten zijn: de in- en output, de gegevensverzameling, de gegevensverwerking, het systeemontwerp en de programmering, het beheer van de gegevensverzamelingen, en de beslissingsbevoegdheid tot het ontwikkelen van een eigen informatiesysteem. Met het verschuiven van de activiteiten (objecten) verschuiven vaak ook de bevoegdheden in de organisatie. Mintzberg (9) geeft een beeld van de organisatie (zie figuur 2), waarbij de organisatie is opgesplitst in diverse aspectsystemen waarin diverse functies en processen plaatsvinden. Het geheel geeft de samenhang weer tussen het informatiesysteem en de andere aspectsystemen van de organisatie.



Figuur 2  
Het functioneren van de organisatie volgens een aantal aspectsystemen  
Uit: Mintzberg, H. The structuring of organisations 1979

Een belangrijk criterium rond de centralisatiegraad is de antwoordtijd binnen het systeem. Dit vormt in de praktijk voor diverse gebruikers een argument om het ontwerp in decentrale richting te beïnvloeden. Dit functionele argument zou men kunnen plaatsen binnen de zienswijze op de organisatie als systeem van mensen en middelen. Maar binnen de andere zienswijzen heeft de centralisatiegraad ook betekenis. Het unieke bezit van informatie geeft een bron van invloed aan een groep of individu in de organisatie als coalities van belangengroepen. De organisatie als gemeenschap van mensen plaatst de decentralisatie in een ander kader. Decentralisatie van de activiteiten binnen het informatiesysteem geeft daar enerzijds een stuk vrijheid van handelen en daarmee status maar anderzijds geeft het ook een stuk rolonzekerheid en verantwoordelijkheid. Het individu weet deze aspecten verschillend te waarderen.

## 5. De cases.

### 5.1. Het onderzoeksmodel

Automatiseringsprojecten verlopen in de praktijk vaak anders dan men theoretisch zou verwachten. Naast de theoretische beschouwingen wordt in deze paragraaf dus aandacht besteed aan enige praktische aspecten. In het onderzoek zijn twee praktijkgevallen onderzocht, die hier verder cases worden genoemd.

In deze beide organisaties had men als uitgangspunt het ontwikkelen van een informatiesysteem met gebruikersparticipatie.

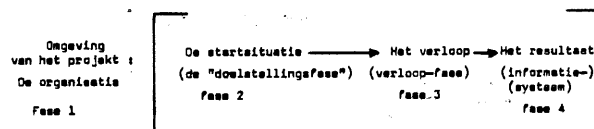
Deze cases zijn in het onderzoek onderzocht met een onderzoeksmodel. Dat model is uitgewerkt in een groot aantal aandachtspunten (10). Het model bestaat uit vier fasen (zie figuur 3), die elk van belang zijn voor de evaluatie van een ontwikkelingsproject.

In fase 1 wordt de organisatie beschreven. In de beide case-studies kwam de invloed van de organisatie op het project sterk naar voren. Een belangrijk aspect van die invloed is in de scriptie omschreven als het veranderingsvermogen van de organisatie. Het veranderingsvermogen geeft een indruk van de drempels die een verandering ondervindt, wanneer men een wijziging in de organisatie tracht te verwezenlijken. Deze drempels komen voort uit de structuur en de cultuur van de organisatie, maar vaak ook uit het beleid.

De startsituatie van een project (fase 2) kan de verhoudingen in een project in hoge mate bepalen. In deze fase moeten de doelstellingen, beleidskaders, de veranderingshulporganisatie maar ook de aanleiding worden geëvalueerd. Deze tweede fase van het model tracht inzicht in de situatie rond de start van een project te verkrijgen.

De daarop volgende fase 3 van het onderzoeksmodel analyseert het verloop van het project. Hierin wordt een aantal belangrijke factoren geanalyseerd, zoals het uiteenlopen van de werkelijke voortgang en de planning alsmede de wijzigingen in de uitgangspunten van de startsituatie. In deze fase wordt de visie van de betrokkenen belangrijk ten behoeve van het verkrijgen van inzicht in de processen binnen het project.

Als laatste fase van het onderzoeksmodel wordt een analyse gemaakt van het resultaat, het informatiesysteem. Daarbij wordt het resultaat doorgelicht en de mening van de betrokkenen over dat resultaat gepeild.



**Figuur 3**

Schematische voorstelling van het onderzoeksmodel voor de case-studies.

Het onderzoeksmodel tracht met deze vier fasen inzicht te verkrijgen in het onderzochte project om zo iets meer over de rol van de gebruiker te weten te komen. Het model tracht met een groot aantal aandachtspunten een richtlijn te vormen, zodat men de grote hoeveelheid onderzoeksmateriaal kan verwerken.

## 5.2. De onderzoeksmethode

Het verzamelen van onderzoeksmateriaal vond plaats via een groot aantal interviews met betrokkenen binnen het project. Tevens werd de schriftelijke informatie (verslagen en rapporten) uit het project aan een onderzoek onderworpen. Uit dit schriftelijke materiaal zijn een aantal knelpunten geselecteerd, die tijdens het interview aan de betrokkenen zijn voorgelegd. Het resultaat vormde een kort verslag van het gevondene.

## 5.3 Het onderzoeksresultaat

Uit de cases kwam naar voren dat de relatie tussen de gebruikersparticipatie en de centralisatiegraad niet zonder meer was vast te stellen. De gebruiker blijkt in eerste instantie problemen te krijgen met de participatie. Deze komen voort uit de ongewone werksituatie en de vaak ongewone werkzaamheden. Maar wanneer de gebruiker deze problemen overwint, dan geeft dit nog geen directe verschuiving van de centralisatiegraad.

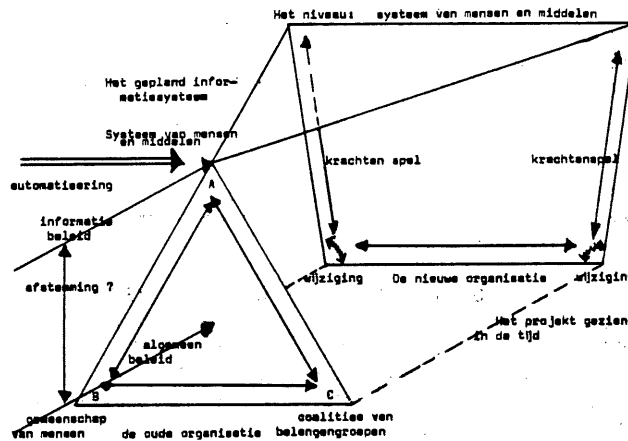
Uit de twee case-studies kwam naar voren, dat de oude structuren met hun vertegenwoordigers een conservatieve kracht vormen in het ontwerpproces. Deze vertegenwoordigers trachten via de participatie een spreiding en decentralisatie tegen te gaan. Als de projectleiding het organisatieveranderingsaspect onderwaardeert, dan kan het ontwerpproces ondoorzichtig worden. Het project kan zo ernstige vertraging oplopen. Allerlei groepen gebruikers benaderen het project verschillend en ze trachten het ontwerpproces verschillend te beïnvloeden. Zo blijkt het participeren "tegen het eigen belang in" erg moeizaam te verlopen. De houdingen van de gebruikers worden door deze fenomenen in het project beïnvloed. In de beide case-organisaties werd het participatieve ontwikkelingsproject door deze factoren beïnvloed. Ook de ervaringen van adviseurs wijzen in deze richting.

De argumentatie van gebruikers is (in de meeste gevallen) functioneel, maar de motivatie achter de argumenten komt voort uit eigen inzichten, doelen en verhoudingen. Deze zijn te beschrijven met behulp van het analysemodel dat de organisatie op drie wijzen beschouwt. In de volgende paragraaf wordt dit nader uitgewerkt.

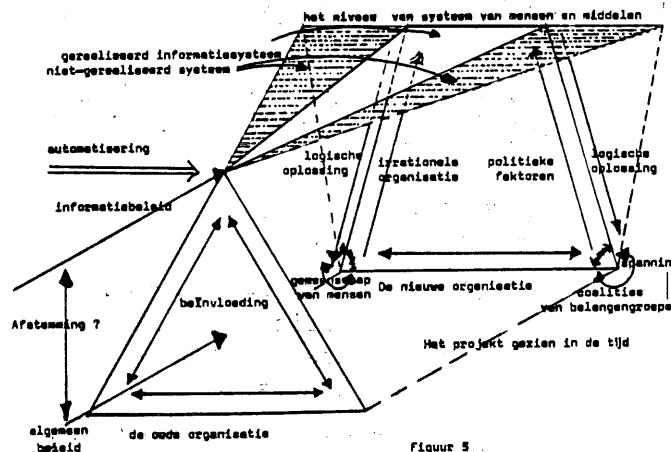
## **6. Analyse en eindconclusies**

Zoals uit het praktisch gedeelte van het onderzoek bleek, geeft de gebruikersparticipatie niet de volledige oplossing van de problemen rond de informatiesystemen. Deze situatie is via het analysemodel op basis van de definitie van Bosch op een inzichtelijke wijze te verklaren. Wanneer men de organisatie op drie wijzen beschouwt, dan geeft dit inzicht in de verhoudingen tijdens een project. De gebruiker participeert niet alleen vanuit de optiek op de organisatie als systeem van mensen en middelen. De argumenten of de motivatie achter de argumenten worden eveneens gevonden binnen de andere zienswijzen op de organisatie. Wanneer men de organisatie opvat als coalities van belangengroepen of als gemeenschap van mensen, dan geeft dit meer inzicht in de andere verhoudingen in de organisatie. Gebruikers schatten hun posities in vanuit al deze verhoudingen. Dit geheel beïnvloedt dus de participatie en de resultaten daarvan zeer sterk (11).

In de figuren 4 en 5 wordt het project in het organisatiebeeld geplaatst zoals dat in figuur 1 is geschetst. De "driehoek" is een conceptueel beeld van de organisatie bij de start van het project. De "vierhoek" is een conceptuele afbeelding van de organisatie in een latere fase, waarin het informatiesysteem is gerealiseerd. Om binnen deze figuren het gewijzigde informatiesysteem aan te geven is de hoekpunt, welke het systeem van mensen en middelen aangeeft, gewijzigd in een lijn in de "vierhoek". In figuur 4 wordt de geplande wijziging aangegeven als een lange lijn. In figuur 5 wordt de gerealiseerde wijziging binnen de geplande wijziging aangegeven. In figuur 5 wordt de lijn die het niveau van het informatiesysteem aangeeft, verdeeld in een gerealiseerd en een niet gerealiseerd deel.



**Figuur 4**  
De geplande gang van het project voor de ontwikkeling van een informatiesysteem.



**Figuur 5**  
De confrontatie van de geplande en de gereeliseerde gang van het project voor de ontwikkeling van een informatiesysteem en het te bereiken niveau van het informatiesysteem.

Deze maar gedeeltelijke realisatie wordt mede veroorzaakt door de spanningen in de verhoudingen tussen de organisatie als coalities van belangengroepen en de gemeenschap van mensen.

De logische oplossingen vanuit het informatiesysteem worden niet geheel aanvaard. De "irrationele" organisatie biedt weerstand aan deze "logische" oplossingen. De participatie op het niveau zoals dat in veel projecten wordt toegestaan, biedt hierop geen volledig antwoord.

Zowel uit de theoretische als de praktische inzichten blijkt dus dat de participatie niet de volledige oplossing geeft. Daarbij moet men echter de conclusies uit de beide cases met de nodige voorzichtigheid gebruiken, omdat ze slechts op basis van twee case-studies zijn getrokken. **Maar in het algemeen kan men wél stellen, dat de participatie veel aandacht vereist, wil het tot een succesvol project leiden.** In het onderzoek kwam verder naar voren, dat vooral het organisatieveranderingsaspect een probleem vormt binnen de participatie. De leiding van de organisatie beschouwt het project vooral als een informatie-technisch probleem.

De participanten in het project bleken echter het project wél in de organisatorische consequenties te vertalen. De daaruit voortvloeiende onzekerheid rond de gevolgen van een project was bij deze participanten een groot probleem. De verhoudingen binnen de organisatie ondervonden door deze situatie veel spanningen.

## 7. Hoe nu verder?

Een oplossing voor deze problemen rond de participatie zou men in de opstelling van de leiding van de organisatie moeten vinden. De participanten trachten het ontwerp zo te beïnvloeden, dat het zo gunstig mogelijk is voor hun situatie in de organisatie. Maar vanuit de diverse optieken van die participerende gebruikers komt men tot een ongelijke invulling van het ontwerp. Deze verschillende visies zullen met elkaar in conflict raken. Dit leidt in veel projecten tot frustraties en vertragingen.

De leiding zal ten aanzien van de organisatorische consequenties duidelijke richtlijnen moeten opstellen in de doelstelling van het project. Iedere participant moet weten binnen welke kaders het ontwerp mag worden gerealiseerd. Dit vraagt inzicht in de functie van het deel van de organisatie dat men ontwerpt tijdens het ontwikkelingsproject. Men moet vanuit de stuurgroep een duidelijke evaluatie van het ontwerp maken en dat toetsen aan de organisatievorm die men wenst te realiseren. Het is tevens belangrijk dat men de doelstelling van het project laat aansluiten bij het beleid. Dit geldt zowel voor de informatie-technische doelstelling als voor de organisatorische. Dit beleid moet op een detailniveau worden uitgewerkt, zodat het een praktische handreiking wordt voor de projectleiding en de betrokkenen. Het moet evenwichtige aandacht besteden aan de informatie-technische aspecten en de organisatorische aspecten van het project (12).

De leiding moet erop toezien, dat het project ook procesmatig onder de meest gunstige omstandigheden verloopt. Problemen rond kennis en vaardigheden van de participanten moeten op tijd worden onderkend. Deze kan men delegeren aan professionele procesbegeleiders.

Ook moet de leiding erop toezien, dat het informatiesysteem zo wordt ontwikkeld dat het "passend" is in het licht van de doelstelling van de organisatie. Maar het moet tevens de ruimte bieden aan de gebruikers, zodat zij het ontwerp in een voor hun "passende" richting kunnen beïnvloeden.

Zo kunnen allen in de toekomst een bijdrage leveren aan het ontwikkelen van betere informatiesystemen.

## Literatuur

1. Frijters, H.: Participatie: de hele of de halve oplossing? Doctoraalscriptie d.d. 23 januari 1983
2. Bemelmans, Prof. Dr. T.M.A., Ir. J.G. de Boer: "Het ontwikkelen van informatiesystemen" uit: Informatie februari 1981
3. Hertog, Drs. J. den, E. van der Wee: "gebruikersparticipatie: etc." pag. 144 uit: Informatie maart 1982
4. Bosch, Prof. Ir. H.: "Vakbekwaamheid en opleiding van de organisatie-adviseur" uit: M.A.B. september/oktober 1978
5. Ganzevoort, W.: "Organisatie-ideologieën - fictie van de rationaliteit van het organiseren" uit: Intermediair 4 september 1981
6. Vries, Drs. M. de: "Informatiebehoeften zijn organisatiebehoeften" uit: Informatie april 1981
7. Graaf, Prof. Mr. Drs. M.H.K. van der: "Menselijke aspecten van de automatisering" uit: Bedrijf/techniek mei 1977
8. Oonincx, Prof. Drs. J.A.M.: "Decentralisatie/centralisatie van de gegevensverwerking en informatieverzorging" 4300-9 e.v. uit: Handboek Informatieverzorging Samson 1981
9. Mintzberg, H.: The structuring of organisations 1979 hoofdstuk 3 Prentice-Hall
10. idem 1: bijlage 3
11. Dee, Drs. G.M. van, Drs. G.R.A. de Jong, A. Kranendonk RA, M. Verschuijl: "De organisatie: een verzameling optieken" uit: 00A Jaarboek 1982/1983
12. Kranendonk RA, A.: "Automatisering voor de rechter hersenhelft" uit: Informatie september 1982 (zie ook Compact no. 30)



Herfst 1983

## Verantwoording van de enquête voor Compact

De resultaten van de Compact-enquête zijn in 3 fasen tot stand gekomen.

1. De verzending alsmede terugontvangst van de door respondenten ingevulde formulieren.  
De enveloppen onder antwoordnummer zijn door een afzonderlijk werkgroepje geopend alsmede geregistreerd. Tijdens de daarop volgende verwerking zijn de formulieren ontdaan van persoonlijke referentiegegevens, zodat de anonimiteit van de deelnemers gewaarborgd kan blijven.
2. Wij hebben de heer P. Schmidt bereid gevonden de technische verwerking ter hand te nemen. Zijn onbevungen oordeel als niet-AC-er stellen wij op hoge prijs. Ofschoon wij van mening zijn dat het cijfermateriaal van de enquête niet voor iedereen interessant is menen wij als genoegdoening alsmede verantwoording voor degenen die wel het enquêteformulier hebben teruggezonden, dat het goed is het verslag onverkort af te drukken.
3. Met behulp van dit rapport is de redactie bij zichzelf te rade gegaan. Onze conclusie alsmede essentiële beleidsvoornemens vindt u eveneens in Compact afgedrukt.

## Uitkomsten van de enquête naar de appreciatie van Compact door P. Schmidt

De enquête had betrekking op Compact 29, zowel wat betreft het nummer als geheel als de daarin opgenomen artikelen afzonderlijk. Tevens is de vraag gesteld welke onderwerpen in Compact werden gemist.

### 1. Verzonden en terugontvangen formulieren

	<u>verzonden</u>	<u>ingevuld terugontvangen</u>	<u>%</u>
Externe lezers	241	29	12
Interne lezers	<u>567</u>	<u>58</u>	<u>10</u>
	808	87	11
	===	==	==

Deze response is voor schriftelijke enquêtes niet abnormaal, al valt met name de reactie van de interne lezers tegen. Naar de oorzaken daarvan kan niet meer dan worden gegist; genoemd kunnen worden:

- enquetemoeheid;
- de enquête werd niet of te laat opgemerkt;
- gemakzucht;
- het afwezig achten van een voldoende kritisch oordeel om medewerking te verlenen;
- beperktheid van het door potentiële deelnemers bestreken gebied van werkzaamheden.

Wat betreft de interne lezers is de response hoog bij de categorieën organisatie-adviseurs (21%) en AC-parttimers (17%). De AC-kern is met minder dan 10% zelfs beneden het gemiddelde gebleven. Tenzij de omstandigheid een rol speelt, dat AC-kernleden veelvuldig als auteur optreden en daardoor menen niet onbevangen te staan ten opzichte van de beantwoording der vragen, lijkt de vraag gerechtvaardigd of er sprake is van een mindere betrokkenheid bij het werk dan normaliter van "specialisten" zou mogen worden verwacht. Als troost moge wellicht gelden, dat de externe lezers het gemiddeld niet beter hebben gedaan dan de interne lezers.

Gegeven de omvang van de response kunnen de uitkomsten van het onderzoek zeker niet worden geacht representatief te zijn voor de lezersgroepen van Compact. Nochtans is het van betekenis enige tendensen, welke uit het cijfermateriaal kunnen worden afgeleid te signaleren.

Bij de weergave van de resultaten is de hierboven reeds gehanteerde tweedeling van in- en externe lezers aangehouden.

## 2. Algemeen oordeel omtrent inhoud

### 2.1

	in procenten van het aantal respondenten							
	goed		bevredigend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
1. Actualiteit	52	62	37	26	10	10	1	2
2. Kwaliteit	50	45	37	44	12	11	1	-
3. Diepgang	29	33	51	48	19	18	1	1
4. Toepasbaarheid	24	33	45	38	28	26	3	3
5. Totaal 1 t/m 4	39	44	42	39	17	16	2	1
6. Algemeen	48	48	44	41	8	10	-	1
	==	==	==	==	==	==	=	=

Het algemeen oordeel opgebouwd uit de onderliggende facetten en het gegeven algemeen oordeel sluiten wat betreft de interne lezers goed op elkaar aan.

Bij de externe lezers ligt dit blijkbaar anders. Immers in het gegeven algemeen oordeel ligt de modus bij het oordeel goed, doch deze modus verschuift naar bevredigend indien het algemeen oordeel wordt gerelateerd aan de som der onderliggende delen. De oorzaken voor deze verschuiving liggen duidelijk in de gevoelens omtrent diepgang en toepasbaarheid, welke laatste bij de externe lezers in meerdere mate als bevredigend zijn ervaren.

Het lijkt in deze van betekenis, dat de redactie nagaat in hoeverre de diepgang en de toepasbaarheid der publicaties in overeenstemming zijn met eisen welke zij daaraan stelt.

Bij de respondenten leeft wel duidelijk de gedachte dat Compact in zijn algemeenheid qua inhoud aanzienlijk meer dan voldoende is.

## 2.2 Oordeel inzake de onderscheiden artikelen

### 2.2.1 Anticiperen op conversie

	goed		bevredigend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
Actualiteit	71	60	21	31	8	9	-	-
Kwaliteit	54	56	42	41	4	3	-	-
Diepgang	36	53	44	38	20	9	-	-
Toepasbaarheid	33	28	59	34	4	31	4	7
<b>Te zamen</b>	<b>49</b>	<b>49</b>	<b>41</b>	<b>36</b>	<b>9</b>	<b>13</b>	<b>1</b>	<b>2</b>
<b>Algemeen oordeel</b>	<b>65</b>	<b>54</b>	<b>31</b>	<b>41</b>	<b>4</b>	<b>5</b>	<b>-</b>	<b>-</b>
	==	==	==	==	==	==	=	=

Het algemeen oordeel valt wat de externe lezers betreft enigszins beter uit dan dat opgebouwd uit de onderdelen. Met betrekking tot de diepgang oordelen de externe lezers in meerderheid "bevredigend", zulks in tegenstelling tot de interne lezers, die in meerderheid de kwalificatie "goed" gaven. Ten aanzien van de toepasbaarheid blijken de interne lezers veel meer genuanceerd te oordelen; 31% achtte de toepasbaarheid matig; de modus ligt voor beide groepen overigens op "bevredigend".

### 2.2.2 Interne controle bij financiële systemen op een minicomputer

	goed		bevredigend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
Actualiteit	73	72	9	22	9	6	9	-
Kwaliteit	66	50	17	39	17	11	-	-
Diepgang	48	32	30	46	22	22	-	-
Toepasbaarheid	39	56	35	25	26	19	-	-
<b>Te zamen</b>	<b>57</b>	<b>53</b>	<b>23</b>	<b>33</b>	<b>18</b>	<b>14</b>	<b>2</b>	<b>-</b>
<b>Algemeen oordeel</b>	<b>64</b>	<b>64</b>	<b>24</b>	<b>31</b>	<b>12</b>	<b>5</b>	<b>-</b>	<b>-</b>
	==	==	==	==	==	==	=	=

Het is opvallend, dat de interne lezers minder tevreden waren over de diepgang van dit artikel, hoewel beide groepen voor "goed" en "bevredigend" samen gelijk scoorden. Opvallend is ook, dat de interne lezers de toepasbaarheid van het artikel goed vonden. Zowel voor diepgang en als toepasbaarheid gaven 20-25% van alle respondenten een matig oordeel.

## 2.2.3 Bescherming van software tegen ongeautoriseerd kopiëren

	goed		bevredigend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
Actualiteit	43	70	48	20	9	10	-	-
Kwaliteit	43	44	48	44	9	12	-	-
Diepgang	29	39	52	32	19	29	-	-
Toepasbaarheid	9	29	33	29	48	39	10	3
<b>Te zamen</b>	<b>31</b>	<b>46</b>	<b>46</b>	<b>31</b>	<b>21</b>	<b>22</b>	<b>2</b>	<b>1</b>
<b>Algemeen oordeel</b>	<b>65</b>	<b>54</b>	<b>31</b>	<b>41</b>	<b>4</b>	<b>5</b>	<b>-</b>	<b>-</b>
	==	==	==	==	==	==	=	=

Ook hier wordt het afwijkend beeld in eerste instantie gevonden in de diepgang en de toepasbaarheid. Wat dat laatste betreft zijn de externe lezers voor bijna 50% slechts matig tevreden, terwijl intern 60% een matig of slecht oordeel heeft.

In beginsel wijkt het interne oordeel daar veel vanaf, maar het komt belangrijk minder genuanceerd naar voren.

In de tweede plaats valt het op, dat het facet actualiteit door 70% der interne lezers als goed werd aangeduid, terwijl het modale oordeel der interne lezers bevredigend luidde.

## 2.2.4 Computer related risks

	goed		bevredigend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
Actualiteit	50	47	40	41	5	9	5	3
Kwaliteit	40	36	50	52	10	9	-	3
Diepgang	20	15	50	64	30	18	-	3
Toepasbaarheid	20	23	45	45	35	22	-	10
<b>Te zamen</b>	<b>33</b>	<b>30</b>	<b>46</b>	<b>50</b>	<b>20</b>	<b>15</b>	<b>1</b>	<b>5</b>
<b>Algemeen oordeel</b>	<b>43</b>	<b>43</b>	<b>48</b>	<b>57</b>	<b>9</b>	<b>-</b>	<b>-</b>	<b>-</b>
	==	==	==	==	==	==	=	=

De oordelen voor de onderscheiden onderdelen zijn hier in redelijke overeenstemming; het oordeel "bevredigend" is overheersend. De oordeelsvorming voor de onderdelen diepgang en toepasbaarheid was voor de externe lezers respectievelijk 30 en 35% matig.

## 2.2.5 Culprit library of routines: EDP-AUDITOR

	goed		bevredigend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
Actualiteit	48	52	26	33	26	15	-	-
Kwaliteit	42	38	32	38	21	24	5	-
Diepgang	26	14	43	57	26	25	5	4
Toepasbaarheid	16	32	32	32	42	36	10	-
<b>Te zamen</b>	<b>33</b>	<b>34</b>	<b>33</b>	<b>40</b>	<b>29</b>	<b>25</b>	<b>5</b>	<b>1</b>
<b>Algemeen oordeel</b>	<b>36</b>	<b>38</b>	<b>46</b>	<b>50</b>	<b>18</b>	<b>12</b>	<b>-</b>	<b>-</b>
	<b>==</b>	<b>==</b>	<b>==</b>	<b>==</b>	<b>==</b>	<b>==</b>	<b>=</b>	<b>=</b>

Opvallend is hier dat de externe lezers de toepasbaarheid van dit onderdeel in overwegende mate als matig beoordelen, terwijl het oordeel van de andere lezers meer regelmatig is gespreid over de onderscheiden oordeelsaanduidingen.

Het opgebouwde en gegeven algemeen oordeel lijken redelijk met elkaar in overeenstemming, doch meer dan 25% van de deelnemers scoort matig over alle onderdelen. Blijkbaar bevredigt dit onderdeel minder dan andere.

## 2.2.6 Boeken

	goed		bevredigend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
Actualiteit	45	68	45	24	10	4	-	4
Kwaliteit	70	46	20	54	10	-	-	-
Diepgang	25	35	60	65	15	-	-	-
Toepasbaarheid	35	29	45	42	15	29	5	-
<b>Te zamen</b>	<b>44</b>	<b>45</b>	<b>42</b>	<b>47</b>	<b>13</b>	<b>7</b>	<b>1</b>	<b>1</b>
<b>Algemeen oordeel</b>	<b>50</b>	<b>55</b>	<b>42</b>	<b>42</b>	<b>8</b>	<b>3</b>	<b>-</b>	<b>-</b>
	<b>==</b>	<b>==</b>	<b>==</b>	<b>==</b>	<b>==</b>	<b>==</b>	<b>=</b>	<b>=</b>

Opvallend is bij deze vraag dat de externe lezers de kwaliteit voor 70% goed achten, terwijl 54% van de interne lezers niet verder komt dan bevredigend.

Herfst 1983

## 2.2.7 Tijdschriften

	goed		bevredegend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
Actualiteit	40	68	53	24	7	8	-	-
Kwaliteit	53	46	47	46	-	8	-	-
Diepgang	13	50	80	38	7	12	-	-
Toepasbaarheid	7	22	60	57	33	21	-	-
<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>
Te zamen	28	47	60	41	12	12	-	-
<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>
Algemeen oordeel	45	50	50	41	5	9	-	-
	==	==	==	==	==	==	=	=

Opvallend is het verschil in waardering ten aanzien van de aspecten actualiteit en toepasbaarheid. Wat dit laatste facet betreft verdient ook de 33% matig wellicht aandacht.

In dat verband past in samenhang met de punten 2.2.5 en 2.2.6 de vraag in hoeverre diepgang en/of toepasbaarheid wel relevant te achten kwalificaties kunnen zijn. Veeleer gaat het hierbij om de signalering van een aanbod, los van de vraag of er van directe toepasbaarheid sprake behoeft te zijn.

## 2.2.8 ABC-Nieuws

	goed		bevredegend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
Actualiteit	44	70	56	13	-	17	-	-
Kwaliteit	44	56	56	34	-	10	-	-
Diepgang	28	41	61	48	11	11	-	-
Toepasbaarheid	22	42	61	35	17	19	-	4
<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>
Te zamen	35	53	58	32	7	14	-	1
<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>	<hr/>
Algemeen oordeel	41	51	59	43	-	6	-	-
	==	==	==	==	==	==	=	=

Blijkbaar wordt het ABC-Nieuws door de externe lezers systematisch lager gewaardeerd dan door de interne. Een onderzoek naar de oorzaken van dit (gradueel) verschil in waardering zou wellicht de weg kunnen wijzen naar een meer eensluidend gevoelen omtrent die items.

## 2.2.9 Onderwijs

	goed		bevredigend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
Actualiteit	29	48	50	28	21	16	-	8
Kwaliteit	38	29	31	50	31	21	-	-
Diepgang	23	17	54	48	23	35	-	-
Toepasbaarheid	21	27	36	46	36	27	7	-
<b>Te zamen</b>	<b>28</b>	<b>31</b>	<b>42</b>	<b>43</b>	<b>28</b>	<b>24</b>	<b>2</b>	<b>2</b>
<b>Algemeen oordeel</b>	<b>33</b>	<b>28</b>	<b>45</b>	<b>41</b>	<b>22</b>	<b>28</b>	<b>-</b>	<b>3</b>
	==	==	==	==	==	==	=	=

Behoudens het aspect kwaliteit dat uiteindelijk extern lager werd gewaardeerd dan intern lopen de oordelen vrijwel parallel, waarbij bovendien moet worden gewezen op de relatief hoge score van "matig".

## 3. Rubricering naar aspect

	goed		bevredigend		matig		slecht	
	ext	int	ext	int	ext	int	ext	int
Actualiteit	51	62	37	26	10	10	2	2
Kwaliteit	48	45	40	44	12	11	-	-
Diepgang	29	33	51	48	20	18	-	1
Toepasbaarheid	24	33	44	37	28	27	4	3
<b>Te zamen</b>	<b>38</b>	<b>44</b>	<b>43</b>	<b>39</b>	<b>17</b>	<b>16</b>	<b>2</b>	<b>1</b>
<b>Algemeen oordeel</b>	<b>48</b>	<b>49</b>	<b>43</b>	<b>42</b>	<b>9</b>	<b>9</b>	<b>-</b>	<b>-</b>
	==	==	==	==	==	==	=	=

In deze opstelling zijn alle facetten over alle vragen samengevat. Wat betreft de actualiteit komen de interne lezers tot een hogere "goed" score dan de externe, maar te zamen met "bevredigend" is de score precies gelijk.

Het aspect "kwaliteit" loopt vrijwel parallel. Hetzelfde geldt voor de "diepgang", terwijl wat "toepasbaarheid" betreft hetzelfde verschijnsel als opgemerkt bij "actualiteit" zich voordoet.

Het algemene oordeel vertoont een grote mate van overeenstemming.

## 4. Conclusies

Het geheel overziende kan worden geconcludeerd, dat het oordeel van alle respondenten over vrijwel alle rubrieken "goed" respectievelijk "bevredigend" is. In procenten uitgedrukt was deze kwalificatie gegeven door minimaal 80% der deelnemers.

De laag scorende aspecten moeten worden gezocht in de sfeer van diepgang en toepasbaarheid. Het is duidelijk dat, met name wanneer het gaat om boeken, tijdschriften, ABC-Nieuws en Onderwijs, de auteurs noch de redactie van binnenuit hieraan veel kunnen veranderen, ook reeds omdat rekening moet worden gehouden met een breed scala van interessen en super specialisaties. Nochtans zou kunnen worden overwogen, dat bij de terzake van genoemde onderwerpen op te nemen artikelen indicaties worden gegeven omtrent de facetten diepgang en toepasbaarheid.

## 5. Ontvangen suggesties

Ondanks de beperkte deelname werden een vrij groot aantal suggesties ontvangen. In hoofdlijnen hadden deze betrekking op de volgende onderwerpen:

### 5.1 Automatisering

#### **Opzet**

- omvang testbestanden;
- bewaring programmaversies;
- ontwikkelen van informatiesystemen;
- misinvesteringen in computers.

#### **Hardware**

- analyses mini's en micro's;
- personal computers;
- tekstverwerkers.

#### **Software**

- beoordeling software pakketten;
- operating system voor micro's etc.;
- vorm programmadocumentatie.

#### **Testen**

- tagging (Combi voor niet doorlopen programmatakken; tagged transacties bij live testing);
- tracing technieken;
- Integrated Test Facility (ITF).

#### **Conversie**

- algemene problematiek;
- van doorschrijfsysteem naar micro.



## **Beveiliging**

- beveiligingssoftware;
- operating systems micro's/mini's;
- security in IDMS;
- beveiliging en noodprocedures bij uitval computer;

## **Datacommunicatie**

- netwerkbeheer;
- betrouwbaarheid.

## **5.2 Accountantscontrole**

### **Filosofie en achtergronden**

- reikwijdte van de verantwoordelijkheid;
- hantering van een uniform AC-jargon;
- EDP-audit USA-Europa overeenkomsten en verschillen;
- analytische accountantscontrole met behulp van de computer;
- verband tussen accountantsfunctie en EDP-auditor.

### **Interne organisatie/-controle**

- betekenis van het accounting systeem voor de accountantscontrole;
- het vergaren van evidence inzake interne controlemaatregelen;
- voorzorgsmaatregelen bij nieuwe systemen om met vrucht geautomatiseerde controle te kunnen toepassen;
- interne controle-aspecten bij systemen voor financiële administratie.

### **Technieken**

- tools voor de AC-accountant;
- audit software-produkten;
- legislative auditing;
- comprehensive auditing;
- opzet en selectie bij de toepassing van steekproeven;
- project management controle standaard pakketten;
- vastlegging geautomatiseerde processen in het dossier;
- voorwaarden voor een betrouwbaar audit trail;
- kosten- en batenanalyse van projecten/systemen.

### **Ervaringen**

- praktijkbesprekingen;
- uniformering van interne controle-aspecten;
- bij gebruik van grote en kleine systemen;
- met VisiCalc;
- business graphics.

Herfst 1983

## 5.3 Diversen

### **AC-groep**

- beschrijving samenstelling;
- structurering samenwerking AC- en algemene sector bij systeembeoordeling;
- I.S.O. standards;
- teletex PAD DN-1;
- business graphics en accountant.

Beleidsvoornemens van de redactie naar aanleiding van de uitkomsten van de enquête

1. Als object van de enquête is door de redactie gekozen voor Compact-nummer 29. Met nadruk wordt gesteld dat de artikelen zijn gepubliceerd onder verantwoordelijkheid van de redactie van Compact. Dit houdt in de bepaling van de keuze van de artikelen/schrijvers, de inhoud en de mate van diepgang. De enquête is derhalve niet geëigend om een oordeel over de schrijvers te formuleren. Aangezien Compact 29 voor "Elck wat wils" biedt is deze kans benut om een breed veld van interesse te raken.

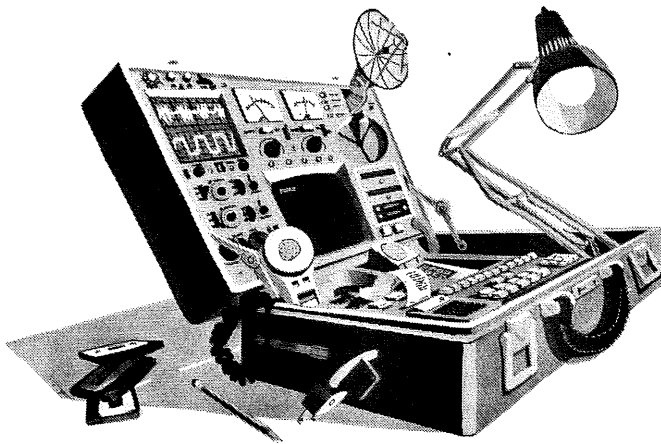
Wij citeren uit "Van de Redactie" van nummer 29: "Reeds geruime tijd hebben wij u Compact toegezonden. Er is ons als redactie, als drager van de eindverantwoordelijkheid voor de inhoud, veel aan gelegen dat Compact beantwoordt aan zijn doel. Dit zowel ten aanzien van de actualiteit, de kwaliteit, de diepgang en de toepasbaarheid van de artikelen".

"Teneinde een indruk te verkrijgen of de redactie van Compact op de goede weg is, willen wij u ook vragen in welke hoedanigheid u Compact leest."

2. Teneinde de afstemming op onze lezerskring met meer vrucht te laten verlopen stellen wij ons het volgende voor:
  - 2.1 In het voorwoord van de redactie een korte aanduiding van de inhoud van de hoofdartikelen te geven.
  - 2.2 De inhoudsopgave van tot nog toe verschenen Compacten bij te werken ter raadpleging op onderwerp, zodat bij navraag in gevallen van toepassing van de informatie deze beschikbaar is.
  - 2.3 In de kop van de hoofdartikelen, eventueel ook bij de rubrieken indien van belang een aanduiding te geven van het behandelde door middel van trefwoorden alsmede een aanduiding van de drie aspecten actualiteit, diepgang en toepasbaarheid zoals de redactie die facetten ziet. Wij vertrouwen erop u hiermede een toetsingsmogelijkheid te verschaffen. U kunt deze notities ook gebruiken wanneer over enkele jaren wederom door ons een enquête gehouden zal worden.
  - 2.4 De rubrieken zullen wij qua inhoud zo veel mogelijk beperken. Daarvoor in de plaats eigen hoofdartikelen doen schrijven. Hiermede zijn we als AC-groep beter in staat om onze eigen ervaringen in de praktijk naar voren te brengen. Overigens met behoud van de ons vertrouwde geheimhouding. Wij hopen ook hiermede de toepasbaarheid van de artikelen te vergroten.
3. Wij danken alle medewerkers aan de enquête van harte voor hun werkelijke belangstelling. Met bovenstaande maatregelen, gevoegd bij nieuwe inzichten zal het met onze Compact "waarachtig wel gaan".  
Redactie



COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.



## DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE

door H. Veenman

1. Nieuws van het audit micro front
- 1.1 **Multiplan cursus voor algemene sector**

Vanaf begin oktober wordt in Amsterdam de cursus Multiplan gegeven. Dit software pakket kan gebruikt worden op onder andere de IBM Personal Computer ten behoeve van het vastleggen van consolidaties, budgetgegevens en dergelijke. Enkele weken later is ook op de kantoren Rotterdam en 's Gravenhage dezelfde cursus gestart. De cursussen worden ook aan externe deelnemers gegeven. De cursusduur is één week bestaande uit twee dagen theorie met praktisch werken aan een case onder toezicht van de docent, gevolgd door drie dagen voor zelf oefenen met de mogelijkheid van raadpleging van de docent of van het AC-kernlid dat in die week als begeleider/ster fungeert.

Een aantal personen, dat de cursus Multiplan heeft gevolgd, past de opgedane kennis reeds toe in de controlepraktijk.

Hiertoe staan, behalve de vijf IBM Personal Computers welke ook voor de opleiding worden gebruikt, een beperkt aantal Hyperion-computers ter beschikking. Met deze draagbare computer kan het werken met de zogenaamde Multiplan worksheets ook bij de cliënt of thuis plaatsvinden. Daar een aantal van de controletoeepassingen, welke met behulp van Multiplan worden gerealiseerd, vrij omvangrijk kunnen worden ten aanzien van het geheugengebruik van de computer, zijn alle IBM Personal Computers op de kantoren uitgebreid tot 128 kB.

Voor meer gegevens omtrent Multiplan wordt verwezen naar de rubriek **Onderwijs**.

- 1.2 **Diskettes**

Sinds een aantal jaren is het aantal computers, dat van diskettes als opslagmedium gebruik maakt, sterk toegenomen. Dit heeft als logisch gevolg gehad, dat ook de hoeveelheid AC-toepassingen met diskettes is verveelvoudigd. Helaas was het tot nu toe vaak zeer moeilijk en soms zelfs onmogelijk om cliëntengegevens, die op diskettes werden aangeleverd, te verwerken.

Om deze reden is door de Microgroep onderzoek verricht naar de mogelijkheden om dit probleem op te lossen. Als oplossing is gekozen voor een microcomputer, die de mogelijkheid biedt om een breed scala van diskettes te kunnen lezen, beschrijven of converteren naar voor door onze huiscomputer te lezen media.

Zo zullen met deze apparatuur in de toekomst bijvoorbeeld kunnen worden verwerkt:

IBM System 3, IBM System 34, 36, 38, IBM PC, Wang, Philips (onder andere de tekstverwerkers), Hermes, Exidy, MAI, Tandy, Apple en Altos. Gepland is deze apparatuur, voorzien van de benodigde programmatuur, voor gebruik beschikbaar te hebben in het begin van 1984.

Voor diegenen, die wat meer willen weten over het fenomeen diskette, over de toegepaste technieken en de mogelijkheden, volgt hierna een artikel aangaande dit onderwerp.

## 2. Hoe werkt een diskette

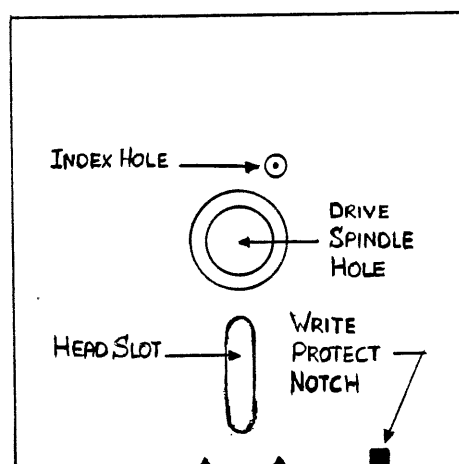
In dit artikel zullen we ingaan op de diskette, ook wel floppy of floppy-disk genoemd, het medium voor gegevensopslag waarvan gedurende de laatste jaren voor allerlei toepassingen gebruik wordt gemaakt.

### **De diskette**

Een diskette is een cirkelvormige flexibele schijf (vandaar het woord "floppy") met een diameter die varieert van 5 tot 20 centimeter en een dikte van ongeveer 0,08 mm. Deze schijf is aan beide zijden voorzien van een magnetiseerbare laag, met een dikte van 0,00254 mm. U kunt dit vergelijken met het oppervlak van een band, zoals die wordt gebruikt bij bandrecorders of cassetterecorders.

Wanneer we deze vergelijking nog even doortrekken, ontdekken we dat ook een diskette gelezen en beschreven wordt met een lees/schrijfkop en dat het gemagnetiseerde oppervlak langs deze kop wordt bewogen. Aangezien de lees/schrijfkop het diskette-oppervlak raakt, is de magnetische laag beschermd met een antistatisch smeermiddel, dat de wrijving reduceert.

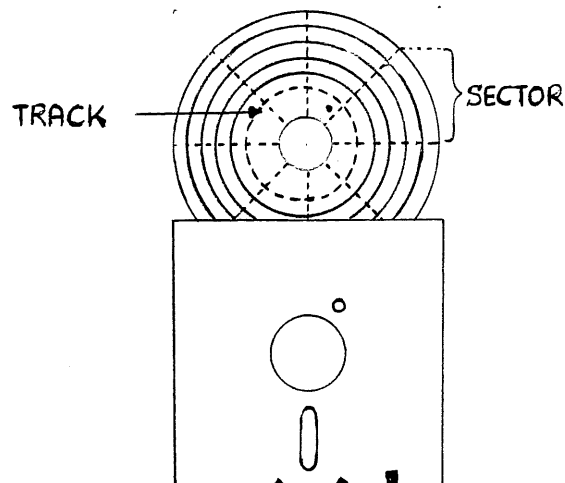
Om de diskette mechanisch te beschermen is deze schijf gehuld in een kunststofenvelop (zie figuur 1).



Figuur 1.

## De opslagstructuur

Op het cirkelvormige oppervlak van een diskette zijn, afhankelijk van het type en het formaat, enkele tientallen sporen (ook wel track genoemd) te onderscheiden, die gelijkmatig en concentrisch over het oppervlak zijn verdeeld. Ieder spoor is onderverdeeld in een aantal sectoren (zie figuur 2).



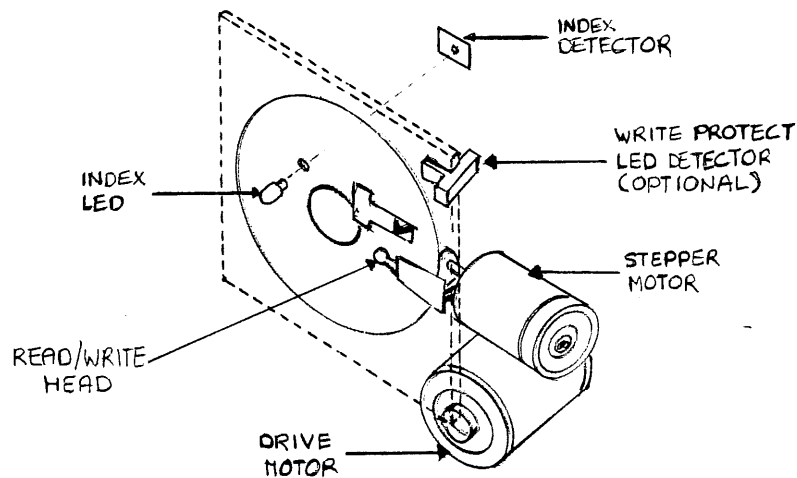
Figuur 2.

Een sector is op zijn beurt onderverdeeld in twee velden: het identificatieveld het zogenaamde ID-veld, waarin een aantal technische gegevens zijn opgenomen over de betreffende sector, en het data veld. In het data veld van zo'n sector kunnen gegevens worden opgeslagen, zoals stukjes programma, grootboekgegevens of een stukje tekst.

Aangezien het aantal sectoren per spoor voor alle sporen op een diskette gelijk is, kunt u zich voorstellen dat de sectoren, die dichterbij het middelpunt van de diskette liggen, korter zijn dan de sectoren, die verder van het middelpunt weg liggen; echter de opslagruimte binnen iedere sector op een diskette is gelijk!

De sectoren zijn per spoor genummerd (bijvoorbeeld 1 tot 26).

Wanneer een bepaalde plek op een diskette door de computer moet worden gevonden, moet bekend zijn welke sector nummer 1 is, welke nummer 2, enz. Daartoe is in de diskette een klein gaatje gemaakt, het zogenaamde "index hole" (zie figuur 1). Wanneer de diskette ronddraait, omdat gegevens op de diskette moeten worden gelezen of geschreven, draait ook het gaatje rond; met behulp van een lampje, meestal een lichtgevende diode of LED, en met een lichtgevoelige cel kan zodoende bepaald worden wanneer het gaatje voorbij komt. Als afspraak geldt, dat de eerste sector "na het gaatje" sector nummer 1 is. Daar de draaisnelheid van de diskette bij de computer bekend is, is het nu mogelijk om te bepalen waar iedere sector zich op een spoor bevindt. Om een gewenst spoor te bereiken kan de lees/schrijfkop haaks op de sporen worden bewogen met behulp van een stappenmotor (zie figuur 3).



Figuur 3.

De hoeveelheid gegevens die op deze manier op een diskette kan worden bewaard varieert, afhankelijk van het type, van enkele duizenden tekens tot enkele miljoenen.

### De directory

Normaal gesproken zullen gegevens in verzamelingen op de diskette staan; dit kunnen bestanden zijn maar ook programma's of ingetikte brieven.

Om een bepaalde verzameling te kunnen vinden op een diskette, is op een aantal sporen (meestal tracks 0 en 1) een inhoudsopgave van de diskette opgenomen, die wij hierna "directory" zullen noemen.

In deze directory staat per file (verzameling) een aantal gegevens, waaronder de naam van de file, op welke plek de file begint (dus tracknummer en sectornummer) en de lengte ervan.

Wanneer een computerprogramma dus een bestand op diskette wil gaan lezen, zal het eerst naar de naam van het bestand zoeken in de directory, vervolgens de bijbehorende startpositie en lengte van de file lezen alvorens de eerste sector van het bestand te lezen.

### Verschillende formaten

Hoe meer computers gebruik gingen maken van diskettes, des te meer soorten kwamen er. Zo zijn er op het ogenblik reeds een zevental maten diskettes, te weten 8, 5 1/4, 4, 3 3/4, 3 1/2, 3 1/4 en 3 inch.

Tevens kunnen diskettes van een fysiek gelijk formaat op vele manieren worden beschreven; zo is het mogelijk om diskettes aan één kant of aan twee kanten te beschrijven, om een verschillend aantal sporen te onderscheiden, om verschillende hoeveelheden gegevens per spoor en zelfs per sector tegen te komen, kortom van enige standaardisatie is vrijwel geen sprake. Als uitzondering daarop kan genoemd worden het Basic-exchange 3740 formaat van IBM, dat ook op een aantal niet-IBM computers kan worden verwerkt.

## **Betrouwbaarheid**

De diskettes zijn gefabriceerd uit zeer dun materiaal, dat zeer gevoelig is voor vette vingers, stof, e.d. Alhoewel de diskettes door de hoes redelijk worden beschermd, is het nog altijd van groot belang dat de diskettes met zorg worden behandeld. Het dubbel vouwen van een diskette, het vastpakken van de diskette in plaats van de hoes of het in aanraking brengen ervan met een magneet zal de gegevens op de betreffende diskette zeer waarschijnlijk onherstelbaar verminken.

Maar ook al vertoetelt u uw diskettes, toch moet altijd gezorgd worden voor een kopie van de gegevens op een andere diskette, of eventueel op een ander medium, omdat de gegarandeerde levensduur voor de meeste diskettes niet meer dan een jaar bedraagt.

## **Toekomstverwachtingen**

De diskette heeft zich de afgelopen jaren een ruime plaats verworven wanneer het gaat om de opslag van gegevens in machinaal leesbare vorm. De voornaamste redenen zijn dat diskettes niet duur zijn (10 tot 15 gulden), dat deze eenvoudig te vervoeren zijn en dat de betrouwbaarheid toch zodanig is, dat men ze zeer goed voor kopie-opslag (back-up) kan gebruiken. We verwachten dat het aandeel van de diskettes in de mediamarkt de komende jaren nog zal toenemen, samen met dat van de personal computers. Echter ook het aantal verschillende formaten zal nog toenemen en van een standaardisatie zal voorlopig nog geen sprake zijn.

3. Tot slot volgt hierna een artikel van de hand van mr. William List, partner van het London office van Thomson McLintock & Co. KMG en voorzitter van de "British Computer Society's Auditing by Computer Group", waarin hij zijn visie geeft over het gebruik van kleine computers in de controlepraktijk.



## How cheap computers are affecting external audit

William List, CA, MBCS

---

*The use of cheap computing power, either as a stand alone device or as part of a large network, is having an increasing effect on how audit clients maintain their accounting records. Willie List identifies how these developments are changing the way in which auditors evaluate accounting systems and how they perform their work.*

---

In this article I shall first identify some general matters which affect cheap computers in any environment. Then I shall discuss the effect of the introduction of cheap computers in three main classes of client: small, medium and large. In each of these circumstances I shall postulate the type of computing environment which will exist and therefore the matters which auditors must bear in mind when performing their work.

### Packages

A package is a suite of application programs purchased from outside the business. There are many hundreds of packages available, varying in scope from the total business accounting needs to specific areas, such as purchase ledger. What packages do, their inherent data processing quality and their cost vary enormously. In general terms purchasers buy what they pay for: the cheaper the package the less it will do and the poorer the quality.

*Willie List is a partner in the London office of Thomson McLintock & Co, KMG and is Chairman of the British Computer Society's Auditing by Computer Group.*

One factor which will affect business computing is the relative cost of producing the programs to perform accounting work. As this increases, the pressure to use packages increases and I believe the majority of small/medium users will use packages in the future (modified if necessary to meet specific needs) simply on cost grounds.

There are three areas which auditors must be particularly wary of when clients use packages.

(1) The method of processing transactions must fit the package. This will often mean changing a business's traditional methods of working. In particular the procedures to record business events which are not catered for in the package may, at first sight, seem peculiar, eg, a bill of exchange must be processed as cash in most UK sales ledger packages.

(2) Many of the packages now being sold have been written by data processors and not by accountants, and therefore may not maintain double entry book-keeping in a proper or sensible manner. Auditors must be very sure that any entries generated by the packages (eg, the total of sales for posting to the general ledger) are computed correctly.

(3) Many packages do not produce printed output in a form which is amenable to examination by the regulatory authorities. For example, in the UK there is a requirement to produce schedules of invoices together with the VAT in a form acceptable to the Customs and Excise. This is often difficult to achieve!

### Programs

The programs in cheap computers are either fixed or variable.

(1) Fixed programs are wired into the computer on the silicon chips (firmware), or they are purchased in a form where nobody can tamper with them (compiled

form). If our clients' programs are in these forms, then there is a reasonable presumption that what they do is unlikely to be tampered with by the people using the computer. However, it is still possible for people using the computer to write additional programs which tamper with the data on the files or to adjust the data that is printed out.

(2) Variable programs are specially held in the computer in source form. Many cheap computers come with their own programming language—often BASIC. If there is a compiler on the cheap computer which the auditor is auditing, then he must approach his work on the presumption that the computer user will have used the language to write or modify programs which process the accounting data. It is very easy for accountants to learn enough BASIC to write simple programs—two hours from no knowledge is sufficient. Considerable practice is required to write sophisticated programs, but this is well within the capability of all intelligent people.

### Audit costs

In the United Kingdom a micro-processor can be bought for £70, but the user cannot do very much on that one; the cheapest that will keep accounting records is about £600. It is therefore well within the compass of any business to purchase such a machine to keep some or all of its accounting records. It is true, but unfortunate, that the costs to the auditor of fully understanding the manner in which the accounting records are maintained is a function of the complexity of the system—not of the cost of the computer. The possibility exists therefore that the cost to the auditor of finding out what the computer is actually doing may exceed the cost to the auditee of buying the computer and the necessary programs. If this happens, auditors will be under great pressure to find new ways of doing their job which are commercially acceptable to their audit clients. I regret there is no simple solution to this problem at all.

### Control

If the computer user is its "owner", able to write extra programs (or amend the purchased software), he may not be retaining adequate copies of the computer files, etc, and this presents the auditor with problems which are very different from those set out in the auditing and computing textbooks. The method by which controls are established over the application will also be subject to change, as methods of processing the data change (eg, in real time application the use of batch totals to demonstrate completeness is often inappropriate). In particular the requirement for control procedures to be effected within a limited period of time (*ie*, before it is too late to recover from any error) will be a major factor in the change of present techniques to enable an equivalent quality of control to exist in any future application.

Since many of the applications will be written by people who are new to computing as a discipline, I also foresee a period when application controls are weak and those writing the programs are learning the need for much tighter control procedures than those used in previous manual systems.

It seems to me, therefore, that the accounting profession as a whole needs to re-think the control techniques which it expects to find within enterprises, in order to establish in its own mind those techniques which are capable of producing an audit-reliable control. This must be a pre-requisite to any reliance upon them. In addition, I believe that the profession must consider far more carefully the nature of accounting processing and records which it is reasonable to expect when records are maintained on cheap computers rather than as a pile of vouchers in a box somewhere (or on the back of an envelope).

## **The skills of the auditor**

For many years now the large accounting firms, and many of the smaller ones as well, have had on their staffs a number of technical computer audit experts. Some of these experts have also acted as management consultants to the firm's clients. In these circumstances it has been convenient for the majority of the other members of staff to pay less attention to computers than they would have done had the specialists not been there. It is my belief that this happy period for the majority of the profession is now over and that all new-accountants must be capable of dealing with computer systems. Indeed many will have used computers at school or university and therefore will be conversant with them. The difficulty may arise with those accountants who have not been so fortunate and who now have to learn how to use computers. The role of the technical computer audit experts will change materially as the majority of staff become familiar with computers, and it is quite possible that as a separate group they will progressively cease to exist.

## **Computer audit techniques**

Much has been written on the two basic methods of using the computer to assist the auditor in the performance of his duties: the use of audit software and the test data method. Both methods are appropriate for cheap computers.

### *Audit software*

The vast majority of the commercially available generalised audit software packages cannot be used on cheap computers. However, most cheap computers have a computer language (normally BASIC or FORTRAN) and there seems to me no reason why auditors cannot write their own audit software program(s). Some of our staff now do so. We anticipate that, as the development of non-procedural languages increases, then the writing of audit programs will become far simpler—as will the development of accounting applications.

### *Test data method*

It may well be that the easiest way for auditors to find out what the computer system is doing is to process a number of transactions through it. Obviously the nor-

mal caveats of having separate files, not corrupting the client's files, etc, must be borne in mind. Using the test data method has proved an effective way to see just what is going on, what can happen and what should happen and clearly will be used by auditors in the future.

## **Small clients**

A small enterprise is defined in paragraph 2.2 of UEC Draft Auditing Statement No 13, which states:

- management is in the hands of one person or a few people who combine all or most of the essential functions of marketing, manufacturing, personnel, finance and accounting;
- management and their families own all or a large part of the enterprise;
- because of its talents and ownership, management dominates the enterprise in all essential aspects;
- the owner/manager is generally involved in many of the day-to-day operations;
- a small number of employees often offers little possibility for an adequate segregation of functions;
- from an accounting point of view the systems tend to be relatively uncomplicated.

This results in:

- simple book-keeping and accounting controls;
- emphasis on personal participation by management;
- informal procedures or reporting, analysis, planning and control;
- easy access by accounting and administrative personnel to assets.

The majority of small enterprises are likely to purchase a small computer and the accounting packages to run on it to perform record-keeping functions. It is likely that the computer will also have a word processing package to take financial information from the record keeping packages and to render invoices, statements, letters, etc, directly. The owner/manager is likely, in addition, to program the computer to do extra things, or to tailor the packages to better meet his business needs.

The need to have back-up files containing data and programs to effect recovery from errors is obvious to anybody who has considered the point, but many small businesses—particularly where the owner is dealing with the matter himself—have not appreciated this. If such back-up is not carried out, there is a danger that the accounting records will be completely lost, and equally, if the procedures to recover from the back-up copies are not thorough, there is a danger that accounting records will be incomplete.

The introduction of a computer is unlikely to improve the situation if there is no guarantee of completeness or accuracy in the records maintained by the enterprise. The auditor is therefore in much the same position as he was before—with two important exceptions.

(1) The majority of the records will now be on computer printed paper. There is a very great temptation for auditors to assume that computer-generated paper work is more reliable than handwritten paperwork (particularly if the latter is badly written and untidy). Computer output always looks neat and tidy, even when its contents are rubbish.

(2) Exactly what information has been printed out (and kept) may constitute less than was previously available for audit and may constitute loss of accounting records and audit trail.

### **Medium clients**

Medium-sized clients will still generally be using relatively cheap computers, but slightly larger business packages which they will have modified to meet their needs. There will probably be two or three staff specifically assigned to looking after the computer—to make sure the programs are processed in the right order and that they make printouts when they are supposed to. They will probably also do most of the necessary programming.

It is likely that there will be more formal procedures for amending and running programs than will exist in the small businesses. Whether these will be of reliable quality is an open question. Those controls on which auditing reliance can be placed are likely to be found in the applications; since management will have delegated work to others, it will require evidence that the work has been performed satisfactorily.

### **Large clients**

Large clients use cheap computers in two entirely different ways—firstly, by attaching them to a network connected to their main central computer, and secondly, as stand-alone devices which have no connection to anything.

#### *Cheap computers connected to a network*

In the majority of cases these devices are sophisticated input machines (eg, cash registers in a supermarket connected to the supermarket central computer for replenishment of stock, etc). Most of the software supplied on these machines is of a fixed nature, probably programmed by the firm's central data processing unit. There is often little need to have copies of various data files maintained on such machines as the full files are transmitted to the central computer at regular intervals—if not immediately.

However, they are increasingly being used by local management to produce locally information which they need to assist them in the performance of their duties. It is therefore probable that such machines will have a programming capability limited to reading the data that has been accumulated for the main system and producing local management reports. Auditors therefore must be clear in their minds when examining computer output at branches of large companies as to whether this forms part of the main system or whether it is a special report produced locally. Various large companies have tried to control the writing of such programs and have found it completely impossible.

In my view this type of implementation is not going to cause a material audit problem. The main accounting system will be developed centrally, therefore it can be reviewed once, and the audit costs of such a review are reasonable in relation to the total development costs. This is not to say that it is necessarily easy for an auditor to comprehend precisely what is going on or, more importantly, to record it clearly in the audit work papers. There will be a formal series of procedures for all matters affecting the main system; physical security of local equipment, back-up and recovery, extensive error detection procedures, etc. These are relied upon by management to function satisfactorily and may not provide much visible evidence of performance, which makes the auditor's task more difficult.

The majority of individual reports produced specifically for local management outwith the main system will not be of audit significance; company-wide summaries of the information will be of more value to the external auditor and these can be obtained from the central machine.

So far as auditing is concerned, it is likely that the approach used in the past will still be applicable and that the large generalised audit software programs can be used on the central computer with the necessary information transmitted to the central machine for use if necessary. There will be changes in detailed techniques, there will be more planning work, and new audit procedures will be devised to meet changed circumstances, but these changes are well within the capability of auditors to adapt to without major problems.

#### *Many separate cheap computers*

It is interesting to note the number of departments in large companies which are less than pleased with the performance of the central data processing department and which are now in a position to purchase cheap computers within their departmental budgets. This is causing substantial concern because individual departments are writing their own little systems to do their own thing. One medium-sized group of companies had a central processor which it got rid of; now everybody has their own little processors and the auditors have to review fifteen sales ledgers instead of one. As stated earlier, the costs of a review do not necessarily bear any relationship to the size of the undertaking, and auditors can have severe difficulties in coming to grips properly with understanding a multiplicity of small systems at a cost acceptable to the client!

In essence the effect of the fragmentation of central applications is to remove the ability of auditors to take advantage of the economies of scale which they have used to good effect in the past. Auditors must now deal with the applications as a series of activities on the scale of small or medium clients and adapt their audit methods accordingly.

#### **General**

Methods of maintaining records change, but the objective of keeping them does not; the auditor must consider changes in his audit methods so that they are appropriate to the client's business and systems.

The changes the auditors must consider are as follows.

- The greater use of computer programs will give rise to a higher probability of systematic error in the records—what effect does that have on statistical sampling plans?
- Management are likely to understand better the processing of the data—what effect does that have on effective control?
- Data is kept in magnetic form and possibly not printed out, rather than being kept in manual records—what effect does that have on audit methods?
- What systems do may vary more than previous manual systems.
- Programs may be easy to change and may be written and run in an uncontrolled environment—what effect does that have on the ability of the auditor to rely on controls (particularly programmed controls) throughout the audit period?

#### **The future**

This article has tried briefly to describe the present situation as I see it. The future holds some very interesting technological advances. The micro-processor is now in mass production and the precise effect that it is going to have on society (including the auditor) is far from clear, even to the futurologists who are addressing this problem.

It is also interesting to consider the effect of the micro-processor on the way in which just about everything is done—including the maintenance of accounting records, when a great deal more information is more readily available than it was before. There are now on the market machines which will accept voice communication: imagine instructing the computer to make journal entries by speaking to it—without any supporting documentation!

There are programs, known as generators, which will permit the creation of accounting systems without the formal procedure of the development cycle which auditors are used to on large computers; what effect will they have? The future will face us with more change—the technological pace is becoming faster; but auditors all over the world have the intellectual capability to understand these changes and make the best use of them.

Nevertheless auditors need help from their professional bodies to define a reasonable way, given the new and potential technological means available to maintain adequate accounting records, to comply with government legislation. Given those means of maintaining records, what constitutes acceptable control over the records, and how should this be achieved? Is it reasonable to rely on the technology to control itself or should we be recommending new techniques to assist management to control the activities themselves?

We also need encouragement and training to equip all accountants who qualify from now onwards to use these machines constructively (should auditors and accountants be able to type as a matter of course? should examinations be conducted using cheap computers?) and to learn the skills necessary to enable the auditors of the future to use and deal with them. The profession can meet the technological challenge and adapt its methods to perform the audit function expected by society, but only if members respond positively to the opportunities provided by technology. □





## Boeken

### Boekbespreking.

Auditing & EDP, Second edition door:

Gordon B. Davis CPA;

Donald L. Adams CPA;

Carol A. Schaller CPA.

Uitgave van het American Institute of Certified Public Accountants (1983). Aantal pagina's: 413.

Besproken door H.J.M. van der Wielen

### Korte inhoudsopgave:

- The audit and computer data processing;
- General controls for computer data processing;
- Processing methods and controls for applications;
- Computer audit tools and techniques;
- Other data processing environments and EDP auditing activities;
- Appendices.

De eerste editie werd in 1968 uitgegeven eveneens door het AICPA. Schrijver Gordon B. Davis CPA, Phd.

Vergelijking van de tweede editie (1983) met die van de eerste editie leert het volgende.

### In de tweede editie meer aandacht voor:

- planning alsmede aanhouden van controleprocedures bij geautomatiseerde systemen;
- systeem software alsmede data base management systems;
- duidelijker onderscheid tussen general controls en application controls;
- gebruik audit software;
- computer audit tools en technieken voor toepassing nadat de verwerking heeft plaatsgevonden;
- idem gedurende de verwerking;
- idem ingeval van data base management systems;
- controle-overwegingen alsmede de aanpak van de accountantscontrole terzake van mini- en microcomputertoepassingen;
- twee nieuwe checklisten:
  1. checklist ten behoeve van evaluatie van de "audit trail";
  2. evaluatie van de controlemaatregelen in het geval de gegevensverwerking door een servicebureau wordt verzorgd.

# COMPACT

Het boek is samengesteld met als doel:

- de CPA's te begeleiden bij de controle van de jaarrekening van bedrijven die geautomatiseerde gegevensverwerking toepassen. Het is bedoeld voor CPA's, die reeds voldoende inzicht in de samenhang van EDP en accountantscontrole hebben verkregen;
- het verschaffen van grondmateriaal voor training alsmede professionele ontwikkeling;
- verschaft een scala van overwegingen hoe de accountantscontrole aan te pakken zowel qua concept als voor de procedures in geval van snel evoluerende computeromgevingen.

De eerste editie is tot stand gebracht met behulp van een commissie met 8 deelnemers. De tweede editie is becommentarieerd door 200 CPA's.

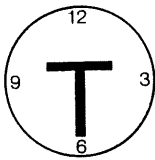
Het boek is een standaardwerk van hoog gehalte.

Het is niet te verwonderen dat het niet in een adem kan worden uitgelezen. Wij stellen ons voor in de komende afleveringen van Compact bepaalde delen van het boek te behandelen.



**COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.**





## TIJDSCHRIFTEN

door D. Jansen Heijtmajer, J.L.H. Kooijman en L.N.M. Straathof

### **ELEKTRONISCH BETALINGSVERKEER (ELECTRONIC FUND TRANSFER SYSTEMS): JURIDISCHE ASPECTEN VAN ELEKTRONISCH GELD**

door Mr. J.M.A. Berkvens

Bron: Informatie, september 1983.

Bij het opzetten van een systeem van elektronisch betalingsverkeer wordt men over het algemeen geconfronteerd met beheersings-, controle-, beveiligings- en juridische aspecten.

In de rubriek Tijdschriften van Compact nummer 29 is een artikel (Auditor concerns with EFTS) besproken, dat handelt over de middelen ter beheersing en controle van Electronic Funds Transfer Systemen (EFTS). In nummer 30 van Compact is eveneens een dergelijk artikel besproken onder dezelfde rubriek, waarin de beveiligings- en controleaspecten aan de orde komen bij ECOBS (Elektronisch Consumenten Betaal Systeem).

In het bovengenoemde artikel van de heer Mr. J.M.A. Berkvens is ingegaan op de juridische aspecten van elektronisch betalingsverkeer.

Nadat in het kort de ontwikkeling van de automatisering van het conventionele betalingsverkeer wordt behandeld, hetgeen vooral betrekking heeft op de geautomatiseerde verwerking bij de financiële instellingen, gaat de schrijver in op de opkomst van de nieuwe betaalvormen. Deze betaalvormen, zijnde het verrichten van geldhandelingen door de consument zelf met behulp van elektronische apparatuur, worden ook wel begrepen onder de termen "electronic fund transfer" en omvatten zoal:

- de gelduitgifte-automaat (GUA, cashdispenser);
- de point of sale terminal, waarmee de klant direct het aankoopbedrag kan afrekenen met de leverancier. Het bedrag wordt direct afgeschreven van de rekening van de klant bij een bepaalde financiële instelling;
- de automatische transactiemachine (ATM)\*, waarmee saldogegevens kunnen worden opgevraagd of waarmee opdrachten tot overboeking bij banken kunnen worden gegeven.

In het artikel van Mr. J.M.A. Berkvens is de juridische problematiek van het geautomatiseerde betalingsverkeer als volgt ingedeeld:

1. De juridische aspecten van het betalingsverkeer *sec*, waarbij met name de vaststelling van het tijdstip van een betaling, de bewijsrechtelijke aspecten van met een geautomatiseerd systeem verrichte verwerkingen en de aansprakelijkheid van belang zijn.

\*) In Angelsaksische literatuur Automatic Teller Machine = gelduitgifte-automaat.

2. De juridische aspecten die voortvloeien uit de organisatie van het betalingsverkeer in (omvangrijke) samenwerkingsverbanden. Hier staan op de voorgrond de wederzijdse aansprakelijkheid van financiële instellingen, het verschijnsel gastgebruik\*), het standaardiseren van technische, organisatorische en juridische maatregelen ter bevordering van de integriteit van het betalingsverkeer (key management, blacklist-management, encryption, uniforme protocollen, uniforme berichten-formaten en gelijkgeschakelde administratieve processen) en het mededingingsrecht.
3. De juridische aspecten die samenhangen met de gebruikte communicatie-infrastructuur. In Nederland (evenals in veel andere landen) worden de datacommunicatiemedia beheerd door (Staats)monopolies. Het betalingsverkeer is afhankelijk van de mate waarin en de (juridische) voorwaarden waaronder gewenste automatiseringsvormen in kwantitatieve en kwalitatieve zin worden toegelaten.
4. De strafrechtelijke invalshoek. De Nederlandsche strafwetgeving is niet berekend op nieuwe vormen van criminaliteit die verband houden met automatisering. Door hun kwetsbaarheid vormen computernetwerken en -systemen een doelwit voor diverse vormen van misbruik.
5. De privacyproblematiek. Tot op heden valt de privacyproblematiek in hoofdzaak onder het burgerlijk wetboek: de bepalingen over onrechtmatig (onzorgvuldig) handelen en het nakomen van contractuele verplichtingen. De komende privacywetgeving, geïnitieerd vanwege de oprukkende automatisering van persoonsregistraties zal vergaande gevolgen hebben. De geautomatiseerde betalingsprocessen veroorzaken grotere, soms nieuwe privacyrisico's. De (ontwerp) wetgeving noodzaakt tot het treffen van omvangrijke en kostbare organisatorische en technische maatregelen bij bedrijfsleven en overheid. Verschillende landen onderwerpen grensoverschrijdend gegevensverkeer aan restricties (Transborder Data Flow, TBDF), met name als het persoonsgegevens betreft die naar landen gaan waar geen privacywetgeving bestaat.
6. Auteurs/octrooirechtelijke aspecten van betalingsverkeersystemen. De ontwikkeling van deze systemen vergt omvangrijke investeringen in ontwikkelwerk zowel door leveranciers van apparatuur en/of programmatuur als door de financiële instellingen. Zoals reeds in vorige nummers van Compact is besproken, is met name de programmatuur slecht beschermd tegen diefstal.

De schrijver komt tot de conclusie dat in zijn algemeenheid het Nederlandse recht voldoende is berekend op het verschijnsel elektronisch geld. Op een aantal terreinen is echter bijstelling noodzakelijk.

---

\*) pag. 21 Het ter beschikking stellen door een financiële instelling van apparatuur aan andere dan eigen cliënten voor het doen van betaaltransacties.

## **Review of Distributed Database Systems (DDBS)**

**E.G. Jancura, A.R. Michenzi**

**(The Internal Auditor, augustus 1983)**

In het artikel wordt verslag gedaan van een onderzoek in dertien grote bedrijven waar een vorm van DDBS geïnstalleerd is.

In zes van deze bedrijven werd de Interne Audit-afdeling gevraagd naar de controlebenadering van deze complexe geautomatiseerde informatie-systemen.

Het artikel is gebaseerd op de antwoorden die uit de interviews naar voren kwamen:

"See how the experiences of the internal audit organizations mentioned here, compare with your group's review of distributed data base systems."

### **Definities DDBS:**

Een Distributed Data Base System wordt door de schrijvers als volgt gedefinieerd:

A **distributed** data base system exists when the data elements stored at multiple locations are interrelated, or when an EDP process at one location requires access to data stored at another location.

Deze definitie wordt nader aangescherpt in een categorisering van de aangetroffen systemen in de volgende 2 groepen:

1. Relatively independent distributed data base dispersed throughout the major operating divisions, with communication links between the various distributed data processing centers.
2. A central data processing center which contains the full data base. Each distributed location replicated the portion of the central data base required for its operation. The central data processing system was updated periodically to reflect the changes which occurred in the distributed data base.

Deze definities en de nadere uitwerking ervan komt overeen met wat hier te lande wordt aangehouden.

Aan de internal auditors van de zes grote bedrijven werden met betrekking tot aanpak van de DDBS-systemen de volgende vragen voorgelegd:

- What were the additional review procedures?
- What were the compliance test procedures?
- What were the substantive test procedures?
- Was the audit trail adequate?
- Did internal audit participate in the system development?
- Did the timing, nature, or extent of the audit test change?

De uitwerking van deze vragen is in de bijgaande tabel opgenomen. Daarbij is aangegeven hoe het management van de DP-activiteiten per bedrijf is georganiseerd c.q. "gedistribueerd".

Herfst 1983

## Exhibit 2. Summary of Internal Auditor DDBS Interview

Internal Auditor	DP Review Procedures	Additional Procedures for DDBS Review	Compliance Test Procedures	Substantive Test Procedures	Analysis Results of Audit Trail's Adequacy	Personal Participation in DDBS Development
I	<ul style="list-style-type: none"> <li>Internal control questionnaires.</li> <li>Audit software package and programs.</li> <li>Applications reviewed in cycle.</li> </ul>	<ul style="list-style-type: none"> <li>Review and reconciliation of numerous transactions.</li> <li>Verification of data within the data base.</li> </ul>	<ul style="list-style-type: none"> <li>Extensive manual reconciliation.</li> <li>Test data and transaction tagging.</li> <li>Audit software programs analyze audit trail supporting application results.</li> </ul>	<ul style="list-style-type: none"> <li>Support ending account balances by computer audit programs and examining source documents.</li> <li>Computer audit programs analyze audit log to support the account balances.</li> </ul>	<ul style="list-style-type: none"> <li>Data base language provides adequate and comprehensive audit trail.</li> <li>Audit trail key to audit procedures.</li> </ul>	<ul style="list-style-type: none"> <li>Involvement commenced after the system was field tested.</li> </ul>
II	<ul style="list-style-type: none"> <li>Internal control questionnaire.</li> <li>Manual review processing.</li> <li>Applications reviewed in cycle.</li> <li>Computer audit programs reconcile transactions and review application results.</li> </ul>	<ul style="list-style-type: none"> <li>Computer audit programs reconcile data at central and distributed locations.</li> <li>Review and reconciliation of numerous transactions.</li> <li>Backup and recovery review.</li> <li>Review access security.</li> </ul>	<ul style="list-style-type: none"> <li>Transaction tagging.</li> <li>Audit software programs analyze audit trail supporting application result.</li> <li>Analyze console log to locate unauthorized activity.</li> <li>Concurrent auditing of all transactions is expected in the future.</li> </ul>	<ul style="list-style-type: none"> <li>Computer audit program analyzes audit log to support the account balance.</li> </ul>	<ul style="list-style-type: none"> <li>Data base language provides adequate and comprehensive audit trail.</li> <li>Audit trail is expected to be key in the concurrent audit package.</li> </ul>	<ul style="list-style-type: none"> <li>Reviewed initial system after management and users agreed upon a design.</li> <li>As project progressed, suggestions were made to improve auditability.</li> </ul>
III	<ul style="list-style-type: none"> <li>Internal control questionnaire.</li> <li>Manual review procedures.</li> <li>Key controls isolated and tested.</li> <li>Applications reviewed in cycle.</li> <li>Application flowcharts developed.</li> <li>Computer audit programs reconcile transactions and review application results.</li> </ul>	<ul style="list-style-type: none"> <li>Detail review of parallel run results.</li> <li>Computer audit programs reconcile data at central and distributed locations.</li> <li>Review of teleprocessing and telecommunication functions and security.</li> </ul>	<ul style="list-style-type: none"> <li>Computer audit programs analyze audit trail for unusual transactions.</li> <li>Computer audit software programs perform application tests.</li> <li>Analysis of console log activity to locate unauthorized access.</li> <li>Transaction tagging.</li> </ul>	<ul style="list-style-type: none"> <li>Computer audit programs analyze audit log to support the account balance.</li> <li>Computer audit programs review account activity for unusual transactions.</li> </ul>	<ul style="list-style-type: none"> <li>Data base language provides adequate and comprehensive audit trail.</li> <li>Audit trail key to audit activity.</li> </ul>	<ul style="list-style-type: none"> <li>Reviewed system after development work commenced.</li> <li>As project progressed, additional analyses made.</li> </ul>
IV	<ul style="list-style-type: none"> <li>Internal control questionnaire.</li> <li>Flowchart of application.</li> <li>Key controls isolated and tested.</li> </ul>	<ul style="list-style-type: none"> <li>Review and reconciliation of numerous transactions.</li> <li>Review of access security.</li> </ul>	<ul style="list-style-type: none"> <li>Test data validates the application.</li> <li>Detailed review of parallel run results.</li> <li>Computer audit programs analyze audit trail for unusual transactions.</li> </ul>	<ul style="list-style-type: none"> <li>Computer audit programs analyze audit log to support the account balance.</li> <li>Computer audit programs review account activity for unusual transactions.</li> </ul>	<ul style="list-style-type: none"> <li>Audit trail key to audit procedures.</li> </ul>	<ul style="list-style-type: none"> <li>Reviewed pilot system and made recommendations.</li> </ul>
V	<ul style="list-style-type: none"> <li>Key applications reviewed.</li> <li>General controls reviewed.</li> <li>Application flowcharts prepared.</li> <li>Key application controls reviewed.</li> </ul>	<ul style="list-style-type: none"> <li>Extensive flowcharts prepared.</li> <li>Review of access security.</li> <li>Key application controls tested.</li> <li>Backup and recovery review.</li> </ul>	<ul style="list-style-type: none"> <li>Documentation review.</li> <li>Transaction tagging.</li> <li>Computer audit programs analyze audit trail and data base for unusual activity or results.</li> <li>Simulation of application programs and comparison of results.</li> </ul>	<ul style="list-style-type: none"> <li>Computer audit programs analyze account balance for unusual activities.</li> <li>Support the account balance by referencing the source documents.</li> </ul>	<ul style="list-style-type: none"> <li>Data base language provides adequate and comprehensive audit trail.</li> <li>Audit trail key to audit procedures.</li> </ul>	<ul style="list-style-type: none"> <li>Reviewed system during and after system design.</li> </ul>
VI	<ul style="list-style-type: none"> <li>System security reviewed.</li> <li>General controls reviewed.</li> <li>Applications reviewed on a cycle basis.</li> <li>Manual review procedures.</li> <li>Computer audit programs reconcile and review application results.</li> </ul>	<ul style="list-style-type: none"> <li>Security review of the shared data base.</li> <li>Backup and recovery review.</li> </ul>	<ul style="list-style-type: none"> <li>Detailed review of code of key application programs.</li> <li>Test data validates applications.</li> <li>Computer audit software programs to analyze the data base.</li> <li>Analyze console log for unauthorized access.</li> </ul>	<ul style="list-style-type: none"> <li>Support the account balance by referencing the source documents.</li> <li>Computer audit programs analyze account balance for unusual activities.</li> </ul>	<ul style="list-style-type: none"> <li>Data base language provides adequate and comprehensive audit trail.</li> <li>Audit trail key to audit procedures.</li> </ul>	<ul style="list-style-type: none"> <li>Reviewed system after development of system design.</li> </ul>

## Exhibit 1. Research Objectives and Sources

The goal of this extensive research project\* was to identify, through a careful study of companies using distributed data base systems (DDBSs), those control and auditing techniques currently in use. We studied 13 systems from 1979-81 through a series of interviews with the data processing personnel, accounting personnel responsible for internal control, internal auditors, and the external auditors of these systems. The systems met one of the three basic patterns for DDBSs:

1. Centralized data storage with distributed processing facilities.
2. Partitioned data bases.
3. Replicated data bases.

Six of the participating companies had internal audit staffs which we interviewed. Their responses form the basis of this article. The six companies included:

Company No. 1 has some 40,000 employees and sales of approximately \$3 billion. It is a major manufacturer that also participates in joint-venture operations.

Company No. 2 is a large manufacturing operation with retail outlets. It employs over 18,000 people with approximately \$2.4 billion in sales. EDP standards are established at the corporate level, but DP centers are under control of division management.

Company No. 3 is a large manufacturing firm with retail outlets. The company organizes DP activities with a combination of regional centers with reporting responsibility to corporate DP staff.

Company No. 4 employs over 19,000 people with sales in excess of \$1 billion. EDP activity is centrally located and controlled by corporate staff although the company has three major divisions with basically independent management.

Company No. 5 is a diversified manufacturing and service organization employing over 44,000 people. Sales exceed \$2.2 billion. Divisional DP personnel report to divisional management with a "dotted line" responsibility to corporate EDP executive. There is also a large corporate EDP function.

Company No. 6 has about \$900 million in sales. The company is basically decentralized. DP activity is also decentralized; the corporate DP staff is small and acts as a service function to the groups' DP organizations.

\*Funded by a grant from Peat, Marwick, Mitchell & Co.

Bronmelding:  
Beide schema's zijn ontleend aan  
**The Internal Auditor**  
August 1983, pag. 51, 52 uit de  
rubriek Information Systems  
door Frederick B Palmer CIA  
waarin dit artikel werd opgenomen.

## Enkele conclusies van de auteurs

While the internal auditors had not changed their review procedures for DDBS, they had increased the detailed transaction testing required once the system was generally the only distributed data base in their corporation and the internal auditors had not yet developed complete confidence in their DDBS expertise. Although no significant changes in procedures due to DDBS were noted, this could be because of the internal auditor's unfamiliarity with the distributed systems. In two cases, auditors expressed significant concern over the field auditor's ability to audit the remote location's activities.

At the time of the interview, all auditors were contemplating some additional compliance procedures. These were not yet well-defined. The substantive test seemed to have less significance to the auditors than the current and contemplated compliance test. They said the DDBS would provide accurate and valid data because the user was closer to the data input and error correction functions of the application. They said that the higher incidence of formalized verification procedures (particularly the programmed checks) occurring at the time of data entry should produce more reliable data. Once these procedures have been verified by successful compliance tests, the extent of substantive testing should decline.

The audit trail was thought to have generally improved because the data base languages handle the recording of the transaction and are able to automatically generate logs. The source documents will still be located at the user's location and manual retrieval is available. Since the data base language had a copy of all transactions, audit procedures could be performed by specialized EDP-audit programs.

The internal auditor's participation in the feasibility study, systems design, and systems approval was unaffected by the DDBS. The auditors as a group anticipated little change in the future. The internal auditors responded to the impact of DDBS in a very consistent manner. All accepted the challenge to perform the required review, each selecting familiar techniques.

With a wait-and-see attitude about whether their techniques were the best, they planned to make adjustments based upon their findings. They felt that neither the nature nor the timing of their audit tests changed significantly. However, they increased the number of the audit tests since this was their first encounter with DDBS. As their confidence and knowledge of DDBS grows, they anticipate that no new major development of test techniques will occur in the next several years.

## Conclusie

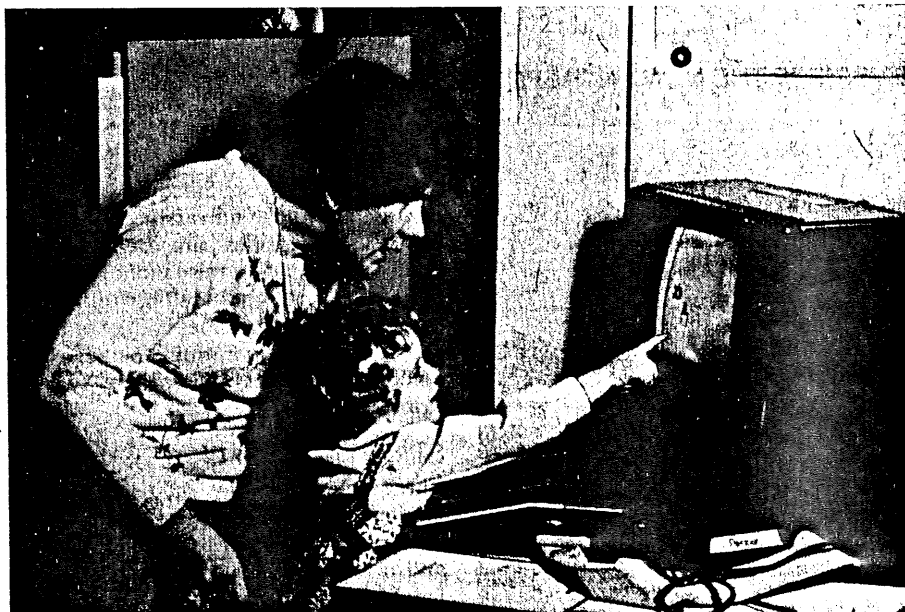
Distributed Data Base Systems beginnen in toenemende mate de aandacht te trekken van interne en externe accountants. Uit het hiervoor geciteerde artikel lijkt naar voren te komen dat de ondervraagde internal auditors nog geen afgerond beeld hebben van de aanpak van de controle van deze systemen in combinatie met de algemene controle enerzijds en de operationele aspecten anderzijds.

Het verdubbelen van de inspanning en uitbreiding van de substantive testprocedure leidt niet vanzelfsprekend tot een betere, effectieve greep op dit type systemen.

Aanzetten tot een meer "in-depth"-benadering van deze systemen zijn in het artikel genoemd, zoals bijvoorbeeld de "concurrent auditing". Hierbij signaleert een "ingebouwde" auditor tijdens het normale werkingsproces afwijkingen van gangbare patronen en legt de daarbij behorende transacties vast in een apart bestand dat voor analyse door de auditor beschikbaar is.

De laatste opmerking die door de auteurs wordt doorgegeven is die waaruit blijkt dat de ondervraagden er niet vanuit gaan dat nieuwe testtechnieken voor de controle van DDBS in de komende jaren beschikbaar zullen komen.

Hier ligt voor accountants een geweldige uitdaging.



How many times must I explain this to you, Mum?

Bron: The Economist

## **Geautomatiseerde audit-technieken**

door drs. J. Achterberg R.A. en drs. G.L. Sijsma.  
Maandblad Informatie, september 1983.

Geavanceerde toepassingen van geautomatiseerde informatiesystemen en databases leiden er steeds meer toe dat de controleerbaarheid van deze systemen afhankelijk wordt van eveneens geautomatiseerde audit-technieken. De behoefte aan kennis van deze technieken en aan specialisten die deze technieken kunnen hanteren neemt dan ook toe.

In het kader van een onderzoek naar deze geautomatiseerde audit-technieken is een literatuurstudie aan de Vrije Universiteit gedaan. Daarin zijn alle in de literatuur voorkomende technieken opgenomen, ook die technieken die niet in de praktijk worden toegepast.

Nadat een beschouwing is gegeven over het begrip controleerbaarheid wordt ingegaan op de verschillende geautomatiseerde audit-technieken die bij de voornoemde literatuurstudie naar voren zijn gekomen.

De schrijvers hanteren hierbij het volgende onderscheid:

- A. Speciale audit-programmatuur georiënteerde technieken.
- B. Testdatatechnieken.
- C. Overige audit-technieken.

### ad A.

Speciale audit-programmatuur georiënteerde technieken.

Bij deze technieken wordt speciale programmatuur geschreven, die wordt toegepast in een bestaand operationeel systeem.

De volgende technieken worden hierbij door de schrijvers onderscheiden:

#### **Parallel Operations:**

Hierbij wordt door het audit-team applicatieprogrammatuur geschreven die operationele programmatuur nabootst. Er wordt gebruik gemaakt van testdata.

#### **Parallel Simulation:**

Hierbij worden geen testdata maar data afkomstig uit werkelijke transacties gebruikt bij het nabootsen van de applicatieprogrammatuur.

#### **Job Accounting Data Analysis:**

Deze techniek bestaat uit het analyseren van de job accounting file waarop de toegang tot een gevoelig bestand wordt vastgelegd.

#### **Embedded Audit Routines:**

Dit zijn bepaalde audit-subroutines die in de applicatieprogrammatuur ingebouwd worden om de intern gegenereerde berichten tussen bepaalde logische modules te analyseren en vast te leggen op een audit-file.

#### **Systems Performance Monitoring and Analysis:**

De apparatuur wordt hierbij getest met behulp van monitoring systemen, zodat de performance gemeten kan worden.



Enkele algemene voordelen van deze technieken zijn:

- mogelijkheid om een systeem te testen terwijl het operationeel is;
- het meerdere malen kunnen gebruiken van eenmalig ontwikkelde programmatuur.

Algemene nadelen:

- audit-team moet speciale kennis en training bezitten;
- ontwikkelen programmatuur is tijdrovend;
- hoge verwerkingskosten;
- moeilijk te beoordelen of de nieuw ontwikkelde programmatuur geen invloed heeft op het systeem.

ad B.

Testdatatechnieken.

Hieronder vallen alle technieken die gebruik maken van testdata. Door middel van het invoeren van testdata kan de werking van processen gecontroleerd worden.

De volgende audit-technieken worden hiertoe gerekend:

**Base Case System Evaluation.**

Bij deze techniek wordt de applicatieprogrammatuur getest met behulp van testtransacties die via een aparte "test mode" terminal worden ingebracht.

**Integrated Test Facility (ITF).**

Testdata worden hier ingevoerd via een in het systeem opgenomen terminal, terwijl het systeem operationeel is.

Enige algemene voordelen:

- minder automatiseringskennis vereist dan bij ad a;
- de waarschijnlijkheids- en validiteitscontroles die getest zijn met behulp van testdata kunnen als module gebruikt worden in elk proces waarbij sprake is van invoer;
- relatief goedkoop.

Enkele algemene nadelen:

- niet altijd mogelijk om testdata samen te stellen die alle omstandigheden dekken;
- het neutraliseren van de gevolgen van testtransacties kan ingewikkeld zijn.

ad C.

Overige audit technieken.

**Transaction selection.**

Door middel van steekproeven worden bepaalde transacties uit de verwerkte transacties gelicht. Verificatie vindt plaats buiten het eigenlijke computerproces.

## **Audit trail.**

Hierbij worden bepaalde transacties vanaf het basisdocument tot de logging files, andere bestanden en uitvoerdocumenten gevolgd.

## **Tagged Transactions.**

Met behulp van bepaalde in de toepassingsprogrammatuur opgenomen routines worden "live-transacties", die aan bepaalde condities voldoen (bepaald door de auditor), geselecteerd.

Hetzelfde kan gelden indien bepaalde gebeurtenissen zich voordoen.

## **Snapshot and trace.**

Een bepaalde transactie wordt volledig gevolgd terwijl deze door het systeem loopt. Het is een soort debug-techniek.

## **Code Comparison.**

Hieronder wordt verstaan het doen vergelijken van twee programma's door een derde programma. Hierdoor kan worden vastgesteld of er verschillen zijn tussen versies van operationele programmatuur.

## **Program Code Review.**

Hierbij wordt de gebruikte programmatuur grondig bestudeerd, bijvoorbeeld in de vorm van desk-checking of door manueel ontwikkelde stroom-schema's.

## **Audit Sampling and Testing.**

Statistische toepassingen om bepaalde processen, bestanden, e.d. te controleren.

Algemene voor- en nadelen van deze technieken zijn, gezien de diversiteit, moeilijk te geven.

In nevenstaande figuur is een indicatie gegeven van het nut en de kosten van hiervoor besproken technieken. Door middel van een \* is aangegeven welke criteria hierbij bepalend zijn geweest. Aan deze criteria is eenzelfde gewicht toegekend.

Herfst 1983

Audit-technieken	Criteria nut			
	belang exclusiviteit	controle-bereik van de techniek	toepasbaarheid van de techniek	diepgang van de techniek
Parallel Operations	*	*		*
Parallel Simulation	*	*		*
Job Accounting Data Analysis	*		*	
Embedded Audit Routines	*	*	*	*
Systems Perf. Mon. and Anal.')	*		*	*
Base Case System Evaluation		*		*
Integrated Test Facility		*		*
Transaction Selection		*		*
Audit-trail		*		*
Tagged Transactions		*		
Snapshot and Trace	*	*	*	*
Code Comparison		*		*
Program Code Review		*		*
Audit Sampling & Testing	*	*	*	

Audit-technieken	Criteria kosten				Nut	Kosten
	start-kosten	verwerkingskosten	deskundigheidskosten			
Parallel Operations		*	*		++	--
Parallel Simulation		*	*		++	--
Job Accounting Data Analysis		*			+	-
Embedded Audit Routines	*	*	*		++	--
Systems Perf. Mon. and Anal.')	*	*			++	--
Base Case System Evaluation			*		+	-
Integrated Test Facility			*		+	-
Transaction Selection	*				+	-
Audit-trail					+	-
Tagged Transactions	*		*		+	-
Snapshot and Trace	*	*	*		++	--
Code Comparison			*		+	-
Program Code Review			*		+	-
Audit Sampling & Testing			*		++	-

- ++ = zeer nuttig
- + = nuttig
- = relatief duur
- = relatief goedkoop

')

Systems Performance monitoring and analysis.

Voordat de schrijvers overgaan tot het trekken van conclusies geven zij schematisch weer, waarbij de geïnterpreteerde audit technieken kunnen worden toegepast. Hierbij onderscheiden zij:

- brongebied van de transacties;
- invoer van de transacties;
- datacommunicatie;
- gegevensverwerking;
- opslaan en opvragen van de gegevens;
- verwerking van de uitvoergegevens.

De schrijvers komen tot de volgende conclusies:

1. Er is gebleken dat er betrekkelijk weinig onderzoek is gedaan naar het verband tussen de toegepaste technieken en de omgeving waarin zij worden toegepast.
2. Geautomatiseerde audit-technieken onderscheiden zich van handmatige technieken doordat eenmaal ontwikkelde programmatuur tegen relatief geringe meerkosten herhaald kan worden toegepast.
3. Geautomatiseerde audit-technieken dienen in elk systeemontwikkelingsproces vanaf de aanvang van dat proces aandacht te krijgen.
4. Het doel van audits kan niet met één bepaalde techniek alleen worden verwezenlijkt. Door zorgvuldige keuze van audit-technieken die elkaar kunnen aanvullen en/of versterken, moeten de controledoelstellingen worden bereikt.

#### Naschrift redactie

Wij verwijzen naar de in het Handboek Accountancy opgenomen publikaties\*) van de hand van A.H.C. Koedijk en A.W. Neisingh, waarin naast een uitputtende beschrijving van de mogelijkheden van het gebruik van de computer in de accountantscontrole aandacht wordt besteed aan de onafhankelijkheid van de accountant bij gebruik van de verschillende technieken (3660 t/m 3664).

\*) Handboek Accountancy:

"Het gebruik van de computer in de accountantscontrole"

Deel I Het onderzoek van gegevensverzamelingen (3651 e.v.)  
december 1979.

Deel II Technieken ten behoeve van beoordeling organisatorische maatregelen (3669 e.v.) november 1981.



COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.

Herfst 1983

## **N** Automatisering Beveiliging Controle **NIEUWS**

door J.F.C. van Epen, H.C. Kocks en M.C. Duym

### **Automatisering**

#### **NIEUWE SOFTWARE-PRODUKTEN**

##### Nieuwe IBM-produkten voor MVS/370 en MVS/XA-systemen

De produkten zijn:

1. Database 2 (DB2). Een relationeel data management MVS-subsysteem dat interactief kan werken met TSO, IMS/DC en CICS.
2. Query Management Facility (QMF). Voor het opvragen van gegevens uit en het maken van rapporten op basis van gegevens in DB2. QMF is ook beschikbaar voor SQL/DS onder VM/SP.
3. Data Extract (DXT). Om gegevens uit IMS/VS-, SAM- en VSAM-bestanden te verzamelen en onder te brengen in DB2 en SQL/DS-tabellen.

##### IBM System/34 RPG (II) software kan draaien op IBM PC

Baby/34 allows the IBM Personal Computer to run software written for the System/34 series of computers. The product creates a software environment for the P.C., allowing complete RPG II application systems and programs developed for the S/34 to be transported "as is" to the P.C. Performance will be degraded since the P.C.'s engine is not as powerful, however.

Ter verduidelijking:

The Baby/34 package includes an IBM System/34 Operations Control Language processor; an S/34 compatible RPG II compiler; a Runtime Execution package; source entry utility; screen format generator; basic data exchange conversion; and a data file utility.

Baby/34 runs under PC/DOS and requires a minimum of 128Kb of RAM and a 5 1/4- or 8-inch diskette drive.

Het pakket kost \$ 2,500 en wordt geleverd door California Software Products, Inc., Santa Ana, California.

Datamation, June 1983 (gewijzigd).

Herfst 1983

## HP 3000 Cobol source code dictionary

The Robot/3000 Dictionary System is a self-generating and self-maintaining COBOL source code dictionary for the HP 3000 minicomputer. The product cross-references copy libraries and source code automatically and provides eight different crt display screens for instant access to its IMAGE database. The system consists of 22 programs that keep track of all changes and enhancements made to COBOL applications to provide application system integrity and quality assurance; e.g., when a new software package is brought on-line that affects a certain item in the database. Robot/3000 lists all COBOL-programs that access that item and that therefore need to be updated.

The program is intended to be able to run immediately, without training. If all of the data items/fields, data sets/files, and databases are defined in one or more copy-libs, Robot/3000 loads itself automatically, the vendor says. It first scans all the copy-libs, and then the remainder of the source code library, without manual assistance.

The program maintains itself daily, taking a few minutes of cpu time to update itself and providing a hardcopy log of all the changes. If it finds a copy statement in a program without a corresponding copy-book in the copylib, it will report the inconsistency.

Datamation, August 1983

## **JURISPRUDENTIE**

### Commentaar

Het afgelopen kwartaal is de schaarse jurisprudentie op automatiseringsgebied verrijkt door twee uitspraken. De eerste uitspraak is het resultaat van een kort geding over de afgifte van source code door een software house. De andere uitspraak komt voort uit een strafzaak voor het Gerechtshof en betreft het kopiëren van gegevens door een (ex-)werknemer.

Over het kort geding is uitvoerig bericht in Computable van 7 oktober 1983. Aan de strafzaak is door diverse dagbladen aandacht geschonken. Wij geven hier een samenvatting van de berichtgeving over beide zaken.

### Afgifte source code door software house

Met het kort geding wilde een dealer in apparatuur en programmatuur bereiken, dat zij kon beschikken over de source code van de door haar, in combinatie met bepaalde apparatuur, geleverde programmatuur. De dealer was van mening, dat de klachten die zij van haar afnemers ontving terug te voeren waren op de programmatuur. Zij zou deze daarom willen aanpassen.

Herfst 1983

Door het software house werd aangevoerd dat:

1. de klachten terug te voeren waren tot het gebrek aan administratieve en technische kennis bij de dealer;
2. er geen contractuele verplichting bestond tot afgifte van de source code;
3. in de branche het vaste gebruik bestaat de source code niet aan anderen ter beschikking te stellen;
4. zij nooit had geweigerd om behoorlijke service te verlenen.

De vice-president van de rechtbank te Amsterdam waarvoor het kort geding diende deed de volgende uitspraak:

"Voor een onderzoek naar alle omstreden feitelijkheden is in dit kort geding geen plaats. Aangezien het er thans bepaald niet naar uitziet dat eiseres in een eventuele bodemprocedure de juistheid van het van haar kant gestelde zal kunnen aantonen, is er geen goede grond om - met welke voorlopige voorziening dan ook - op de uitslag van zodanige procedure vooruit te lopen."

Op argument 3 van het software house werd in het Computable-artikel nader ingegaan omdat dit - bij het ontbreken van een contractuele afspraak (zie argument 2) - ook voor andere soortgelijke zaken zal worden aangevoerd. Hiertoe werden de standaardleveringsvoorwaarden van de drie belangenorganisaties van leveranciers in de branche als volgt becommentarieerd:

- "Volgens de Vifka software-voorwaarden behoudt de leverancier alle rechten.
- De NSV-voorwaarden bepalen terecht dat opgeleverde maatwerkprogrammatuur volledig eigendom van de klant wordt, waaruit impliciet afgeleid zou kunnen worden dat ook de broncode wordt overgedragen. Ter informatie vermeld ik nog dat de Amsterdamse Rechtbank in 1981 heeft bepaald dat in geval van een contractueel bepaalde overdracht van eigendom ook de broncode dient te worden overgegeven.
- De Cosso-voorwaarden gaan uit van hetzelfde principe als de NSV-voorwaarden, maar formuleren dit juridisch juist als een overdracht van auteursrechten op de ontwikkelde programmatuur."

### Kopiëren gegevens (ex-)werkgever

Het gerechtshof in Arnhem veroordeelde eind oktober in hoger beroep een systeemanalist/programmeur tot een boete van duizend gulden. Hij had een aantal gegevens die op schijf-eenheden waren opgeslagen gekopieerd op eigen computerbanden bij het beëindigen van zijn dienstverband teneinde deze ten eigen nutte aan te wenden.

Herfst 1983

Door het bedrijf werd onmiddellijk na het ontslag van de programmeur aangifte van verduistering gedaan. De rechtbank van Zwolle waarvoor het proces in eerste instantie diende, sprak de systeemanalist/programmeur vrij.

In de NRC van 1 november 1983 beschrijft mr. F. Kuitenbrouwer de beslissing van het gerechtshof als volgt:

De rechtbank motiveerde dit onder meer met de overweging dat het kopiëren er weliswaar toe strekte de computergegevens onder de heerschappij van de verdachte te brengen, maar niet aan de heerschappij van de werkgever te onttrekken.

Daartoe lenen computergegevens zich trouwens ook niet, "omdat het geen lichamelijke zaken zijn en zij geen zelfstandig bestaan hebben", aldus de rechtbank.

Het gerechtshof in Arnhem koos een andere benadering.

Computergegevens hebben het karakter van "overdraagbaarheid, reproduceerbaarheid en beschikbaarheid, terwijl zij bovendien economisch waardeerbaar zijn".

Dat laatste kenmerk bleek ook verder van belang voor de strafbaarheid: het overnemen van computergegevens heeft geleid tot "vermogensvermeerdering" van de verdachte ten laste van zijn voormalige werkgever.

Deze benadering heeft een zeker precedent. In 1921 deed de Hoge Raad uitspraak over de vraag of het aftappen van een elektriciteitsmeter "diefstal" van energie kon opleveren. Dit werd betwist met het argument dat elektriciteit niet "enig goed" vormt - zoals de strafwet het noemt - terwijl men ook kan betwijfelen of het in de woorden van de strafwet geheel of gedeeltelijk aan een ander toebehoort.

Voor de Hoge Raad gaf de doorslag dat elektriciteit via de meter economisch waardeerbaar is. Als vermogensbestanddeel was het wel degelijk vatbaar voor diefstal of verduistering. Een dergelijke redenering klonk door in het vonnis van het Arnhemse Gerechtshof.

De berichtgevers hopen dat de veroordeelde in cassatie gaat. Een uitspraak van de Hoge Raad over het al dan niet vermogensbestanddeel zijn van computergegevens, die vatbaar zijn voor diefstal, kan van grote betekenis zijn.

In zijn artikel in de NRC legt mr. F. Kuitenbrouwer tevens een relatie met de mogelijke heffingsgrondslag voor import en export van gegevens. Deze is nu nog alleen het opslagmedium.



## Beveiliging

### RESULTATEN VAN EEN ONDERZOEK NAAR COMPUTERBEVEILIGING

#### Inleiding

In het Journal of Systems Management van juni 1983 zijn onder de titel "Computer Security Practice" de resultaten weergegeven van een onderzoek naar de computerbeveiligingsplannen en -procedures.

Voor het onderzoek werden 43 bedrijven in een, volgens de onderzoekers, representatief gebied van de USA geïnterviewd. De geïnterviewde nationale en internationale bedrijven varieerden in grootte:

1. qua budget voor gegevensverwerking van \$ 350.000 tot \$ 10.000.000 en
2. qua personeelssterkte van 8 tot 200 man/vrouw.

84% gebruikte IBM hardware en software.

Meer dan de helft betrok hardware en/of software van meer dan één leverancier.

De beveiligingsplannen en -procedures werden voor 6 deelgebieden onderzocht. Deze waren:

1. Physical and environmental security.
2. Personnel security.
3. Processing and operations security.
4. Software documentation and security.
5. Data security.
6. Security of teleprocessing and communications systems.

#### Onderzoeksresultaten

Het artikel vermeldt vele percentages die de response op bepaalde vragen weergegeven. Wij volstaan hier met, op een enkele uitzondering na, per onderzocht deelgebied de conclusie(s) van de onderzoekers weer te geven. De onderstreping is van ons.

#### Physical and environment security

"Up to eighty percent (80%) of the firms are not properly prepared to shift operations to an alternative site in case of an emergency."

"Management is sensitive to the danger of fire. However, the number of companies (47%) allowing smoking in the computer room is surprising."

"The findings show a lack of protection against the accumulation of water in the computer room."

Herfst 1983

"Most companies maintain secured access to the computer system and have security procedures for protection of the system, but these procedures are not tested."

## Personnel security

"Most companies investigate personnel before hiring but not after hiring. Personnel need to be rotated and vacations required to protect sensitive data and the computer system."

"There is adequate protection of sensitive tasks. Breaches are handled in the best interest of security, but the protection against the activities of disgruntled employees need improvement."

## Processing operations and security

"Improvements could be made in the area of the separation of the development and maintenance functions."

"Procedures for protecting documentation and sensitive data are adequate. However, the controls for erasing information from scratch storage media need to be improved."

## Software documentation and security

"A need for improvement in evaluating the benefits from an application versus the costs to be incurred."

"Adequate documentation of procedures for each activity related to the running of computer jobs."

"Improvements are needed in the areas of program testing and security". (Deze conclusie betreft het testen van programma's na onderhoud en het regelmatig controleren van programma's op ongeautoriseerde wijzigingen.)

## Data security

"Indication of the use of responsible personnel by most firms and the concerns of companies for the loss of data."

"Only seventy-five percent (75%) can determine when and by whom a change was made."

"Proper procedures are being used to clear rejections from the system error reports and files."

"There is a definite need to update or determine the value of a firms data for insurance purposes."

## Security of teleprocessing and communications systems

"Limited access to terminals should be increased by firms in order to secure the computer system."

"Only forty-seven percent (47%) change keys, combinations and passwords frequently."

"Statistical data on the use and type of use of specified files are maintained by seventy-nine percent (79%) of the computer systems."

"Encryption of data is utilized by only twenty percent (20%) of the firms interviewed."

"Fifty-three percent (53%) of the companies are capable of monitoring unauthorized attempts to read or change records in a file. Only fifty-five percent (55%) of these companies can identify all attempted violations of the system."

"Only thirty-nine percent (39%) of the companies disconnect a user when an attempted violation occurs."

### **Commentaar**

- Voor de interpretatie van deze cijfers dient te worden bedacht dat het onderzoek in de Verenigde Staten is verricht, waar de situatie niet noodzakelijkerwijs hoeft overeen te komen met de Europese respectievelijk Nederlandse situatie.
- Niet vermeld wordt hoe de 43 geïnterviewde bedrijven zich verhouden tot alle in het onderzochte gebied aanwezige bedrijven.
- Ook uit deze resultaten blijkt weer eens dat, alhoewel er plannen en procedures zijn, deze niet worden getest en/of indirect weer teniet worden gedaan.

### **GEGEVENSBEVEILIGING DOOR MIDDEL VAN ENCRYPTION**

In het tijdschrift EDPACS (februari 1983) vonden wij de vermelding van een interessante methode voor het beveiligen van gegevens in bestanden. Deze zogenaamde "Seal-methode" bepaalt een op encryption gebaseerd controlegetal van 18 cijfers. Wij citeren verder de desbetreffende mededeling:

Starting with a 35-digit secret key, the Seal-algorithm is applied to the data to be protected. The algorithm calculates a Seal which is stored at the end of the data file to be protected. Text data remains in plaintext; i.e., it is not encrypted.

When a Seal-protected file is processed, a new Seal is calculated. If the new Seal is equal to the one stored at the end of the file, it is safe to conclude the information on the file has remained unchanged since it was created.

The Seal-algorithm is implemented via software. It can be installed on any computer. About 350,000 characters of data can be processed by Seal in one CPU second on an IBM 3033. This represents a fairly low processing overhead.

Herfst 1983

The Swedish Military Cryptological Unit has evaluated the cryptological aspects of the Seal-algorithm. Based on these tests, the unit has officially approved Seal for use in financial applications.

For further information, contact:

SAKdata AB, Ingenjorscentrum, S-191 78 Sollentuna, Sweden.

Vooral in een kleinere organisatie, waar door het ontbreken van voldoende functiescheiding grotere risico's voor ongeautoriseerd lezen of aanvullen, wijzigen of weglaten bestaan, lijkt ons een dergelijke beveiliging het overwegen waard!

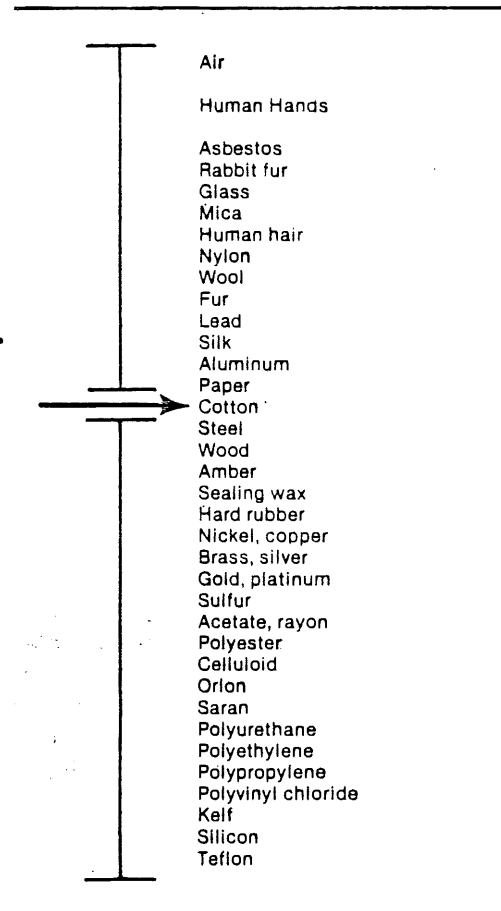
## STATISCHE ELEKTRICITEIT

Statische elektriciteit en vooral de ontlading daarvan via elektronische apparatuur (computers e.d.) kan leiden tot storingen en een heel enkele keer tot schade. Voorbeelden zijn: "bevroren" cursor, vastlopen van papier in een printer, schade aan elektronische onderdelen, chips, e.d. en soms schade in de vorm van vermindering van gegevens of programmafuncties. Dit laatste vereist echter een bepaalde samenloop van omstandigheden, die zich zelden voordoet.

Het is dus aan te bevelen het ontstaan van statische elektriciteit te vermijden. In het tijdschrift MINI-MICRO SYSTEMS van augustus 1983, lazen wij een artikel over dit onderwerp, waarvan wij graag enkele passages willen citeren. Met name waar het gaat om de materialen die de statische lading veroorzaken en de spanningen die onder bepaalde omstandigheden kunnen optreden.

Static results from the interaction of materials or people, combined with movement. Wherever movement occurs, static can be generated by rubbing or separating two materials (table 1).

**Table 1. Interaction of any two materials can produce a charge. In this triboelectric series, cotton is identified as a reference material. Cotton tends to absorb moisture, thereby rendering it somewhat conductive; however, it can still produce a static charge. Materials listed above cotton tend to surrender electrons when friction is produced, thus becoming positively charged. Materials listed below cotton tend to become negatively charged. For example, if nylon and polyethylene are rubbed together, the nylon will become positively charged, and the polyethylene will become negatively charged. The farther apart two materials are, the greater amount of static electricity they will generate together.**



Herfst 1983

A data-processing environment contains many potential sources of static generation, including furniture, tape-storage canisters, disk covers and plastic sleeves. An acrylic dress over a nylon slip, a polyester or cotton shirt under a wool or nylon suit and other combinations of fabrics can develop a static charge from body movement. The charge generated by walking varies with the floor covering and shoe.

Low humidity also increases static charge. When relative humidity falls below 50 percent, higher static charges are likely to be generated (table 2). Considering that indoor relative humidity can drop to less than 10 percent when the outdoor temperature is near freezing, the risk of static discharge and resulting equipment problems is extremely high.

Common static-producing situations in the EDP environment	Electrostatic voltages	
	65% to 90% relative humidity	10% to 20% relative humidity
Walking across carpet	1500	35,000
Walking across vinyl floor	250	12,000
Touching work-bench materials	100	6000
Removing papers from vinyl envelopes	600	7000
Picking up common plastic bag from work bench	1200	20,000
Touching chair padded with polyurethane foam	1500	18,000

Table 2. Electrostatic voltages vary with materials and increase as relative humidity drops.

Het artikel geeft dan als oplossing een antistatische spray te gebruiken op vloeren, zittingen van stoelen en dergelijke. Bij het kiezen van een dergelijke spray dient men zich enkele vragen te stellen, zoals

- does it meet the static decay criteria of military and medical specification?
- is it effective on all materials?
- does it function at relative humidities lower than 15 percent?
- is it non-odor-producing, nonstaining and completely bio-degradable?
- does it leave a residue?
- how long does it last?
- how large an area does it cover?

Bij de op één na laatste vraag wordt nog opgemerkt dat de periode gedurende welke de spray "werkt" kan variëren van 2 maanden tot 1 jaar, afhankelijk van de gekozen spray en de omgeving.

Herfst 1983

## GRENDOERSCHRIJDEND GEGEVENSVERKEER

uit Transnational Data Report 1983, nr. 6, citeren wij de volgende bladzijde:

*This comprehensive international declaration of general principles relating to the regulation of transborder data flows was prepared by Paul Sieghart at the request of the OECD Directorate for Science, Technology and Industry. It was considered by the Expert Party on TDF meeting held in Paris on 28-29 June 1983.*

### The Government of OECD Member Countries,

*Recalling* the principles and objectives contained in the OECD Convention;

*Recognizing* that the unrestricted flow of information of all kinds across national boundaries is an essential condition for international peace, security, mutual respect and understanding, friendly relations and cooperation between nations, fruitful trade, and the mutual enrichment of cultures;

*Noting* that continuing improvements in the technology of computers and telecommunications can facilitate greatly increased flows of information of all kinds across national boundaries;

*Recognizing* the value of information of all kinds for the social, economic, cultural and political development of individuals and peoples, and the harmonious progress of social, economic and cultural groups, nations and the international community;

*Recalling* that the right to freedom of expression, which includes the freedom to seek, receive and impart information and ideas, through any media and regardless of frontiers, and without distinction of any kind, was proclaimed in the Universal Declaration of Human Rights as a common standard of achievement for all peoples and all nations;

*Noting* that this freedom, and its boundaries, have been more precisely defined by the International Covenant on Civil and Political Rights, the European Convention on Human Rights and Fundamental Freedoms, and the American Convention on Human Rights, by one or more of which treaties many of the world's developed and developing nations are now bound;

*Recalling* that many of the other rights and freedoms protected by these and other treaties, as well as emerging new concepts such as the right to communicate and the right to development, cannot be adequately protected or enjoyed in the absence of this central freedom;

*Aware* that information cannot be assembled, stored, processed, retrieved or communicated unless those who carry out these activities are adequately rewarded for their work, and that the unrestricted flow of information therefore requires a régime of free trade in information and information services, across national boundaries, between private individuals and private and public associations and enterprises;

*Aware* also that such a régime requires a framework of coherent and internationally harmonized laws relating to information, information services and information flows of all kinds;

*Recalling* the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as one component of such a framework, and concerned to contribute to its further development;

*Reaffirm* their unqualified adherence to the principle of the unrestricted flow of information across national boundaries under a régime of free trade in information and information services,

*Declare* it to be their policy objectives:

1 to respect the right to freedom of expression by individuals and associations, without discrimination of any kind, as recognized in international law;

2 to impose no prior censorship or any arbitrary controls or constraints on participants in legitimate flows of information;

3 while recognizing that the right to freedom of expression carries with it special duties and responsibilities, to confine any restrictions on it strictly to those authorized by international law where that is necessary to protect national security, public order, public health or morals, or respect for the rights and reputations of others, including their right not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, nor to unlawful attacks on their honor or reputation, and their right to benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which they are the authors;

4 to encourage the development and establishment of a wide variety of independent and autonomous providers of information, information services and communication channels, in order to allow the widest possible freedom choice for those seeking to communicate or receive information;

5 to provide fair and equitable access on reasonable terms to such information, information services and communication channels, and opportunities to participate in them and in the formulation, application, monitoring and review of information and communication policies, at all relevant levels and at all stages;

6 to make available such access to those who wish to exercise any others of their rights and freedoms protected by international law, including the rights to health, education, assembly and association, to take part in public affairs and cultural life, to enjoy the benefits of scientific progress and its applications, and the freedom indispensable for scientific research and creative activity;

7 to make available an adequate right of reply and correction to anyone who has been injured by inaccurate and offensive statements disseminated to the public;

8 to ensure that all improvements in information and communication technology are used to support and extend, and not to restrict or narrow, the rights to freedom of expression and the principle of the unrestricted flow of information;

9 to respect the cultures of different nations and peoples while encouraging their mutual enrichment,

And accordingly *resolve*:

1 to consult and cooperate with each other, and with other nations, in all relevant fora in order to further the achievement of these objectives, especially by harmonizing domestic laws and technical standards;

2 to take all necessary steps in their domestic legislation and policies which will facilitate and encourage that achievement;

3 to refrain from any measures which would impede or delay that achievement. ■

## Controle

### MOORE PARAGON RUST FORMULIEREN UIT MET ANTI-FOUTNUMMER

Onder deze kop (uit *Computable* van 19 augustus jl.) wordt medegedeeld dat er nu voorgenummerde formulieren in de handel zijn gebracht met zelf-controlerende nummering. Dit 'zelf-controleren' dient dan door de computer te geschieden die op deze wijze, met behulp van de 'meegeleverde' algoritme, kan vaststellen of een formuliernummer correct is ingebracht. We citeren nu een gedeelte van het desbetreffende artikel.

De papierleverancier stelt dat bij de invoer van gegevens nogal wat fouten worden gemaakt. Deze fouten beginnen in de meeste gevallen al met het inbrengen van onjuiste ordernummers, rekening- of formuliernummers. De mogelijke gevolgen zijn niet altijd te overzien: foutief uitgevoerde orders, niet geboekte of fout gerubriceerde gegevens of zelfs gevaarlijke vergissingen zoals in de ziekenzorg. Normaliter kost het terugvinden en achteraf corrigeren van foutief ingevoerde informatie veel tijd en geld.

Dit ongemak kan worden voorkomen als het foutief invoeren van nummers onmogelijk is. Het systeem van zelfcorrigerend nummeren van Moore Paragon is speciaal voor dit doel ontwikkeld.

Deze vinding houdt echter in dat slechts van een doorlopende nummering sprake is als men het laatste cijfer, de 'check-digit', buiten beschouwing laat. Aangezien een controle op doorlopende nummering nogal eens wordt gehanteerd ter vaststelling van de volledige verwerking van aangeboden gegevens, dient de controleur bedacht te zijn op het genoemde verschijnsel.

### STRUCTURED COBOL

In *Datamation* van oktober 1983 lazen wij de introductie van een programmapakket dat (oudere) ongestructureerde Cobol-programma's 'herschrijft' in gestructureerd Cobol. Dit pakket, **Superstructure** genaamd, kan van nut zijn voor onderhoud of onderzoek naar werking van programmatuur in ongestructureerde vorm, waarvan geen of slechte documentatie aanwezig is.

De volgende passages geven een indruk van dit pakket.

Superstructure is designed to rewrite users' Cobol applications into structured Cobol programs that are easy to understand and maintain. Programs created by Superstructure execute all paragraphs under the control of a Perform statement; all **alter**, **goto depending on**, **fall thru**, and interparagraph **goto** statements are eliminated.

The structured Cobol programs are written so that each is divided neatly into independent modules of procedure division code.

Each module has a single entry point and a single exit point, and can be invoked only by Perform statements linked hierarchically to the main-line routine.

Herfst 1983

The only **gotos** that are allowed are those that loop back to the paragraph in which they reside. All dead code, within and between modules, is converted into comments. Output from the program includes a listing of the unstructured Cobol program input (if desired), a listing of the structured Cobol program, a structured Cobol program output file, and a scorecard that lists a comparison of key statistics for each version.

The product also comes with a static analyzer that automatically documents structured programs throughout their maintenance live cycles for quality assurance. It can also be used to evaluate existing programs to determine candidates for structuring. Superstructure runs on all IBM and compatible operating systems.

## AUDITING THE TECHNICAL SERVICES DEPARTMENT

In mei 1983 troffen wij in Edpacs een artikel aan dat handelt over de audit van de afdeling Systeemprogrammering.

Acteur: Dave Dunmore

Omdat dit een terrein van EDP-auditing is dat in veel organisaties wordt verwaarloosd bij gebrek aan kennis hoe een dergelijke audit aan te pakken, geeft de schrijver van het desbetreffende artikel een aantal tips gebaseerd op eigen ervaringen opgedaan bij diens eerste audit.

Een aantal van deze tips achten wij zo relevant dat we ze hier (verkort) weergeven.

1. Understand your system software environment.  
Zonder een passende cursus is het nauwelijks mogelijk die specifieke zaken uit uw operating system of andere 'harde' software te halen die u voor een adequaat uit te voeren audit nodig hebt. Het artikel noemt in dit verband de MIS-cursussen MVS, IMS, DOS en CICS. Daarnaast is een goede kennis van de JCL en de in gebruik zijnde utilities een vereiste.
2. Ontwikkel een goed doordacht controleprogramma gebaseerd op een gestructureerde controle-aanpak. Geef daarbij aan welke printouts nodig zijn. Doet u dit niet, dan wordt u door een groot aantal niet ter zake doende lijsten overspoeld.
3. Voer een dergelijke audit aan één stuk uit. De materie is dermate gecompliceerd dat u er niet steeds tussenuit kunt voor andere werkzaamheden, zonder het overzicht te verliezen.
4. Maak gebruik van de hulpmiddelen die aanwezig zijn, zoals TSO of SPF.

Het artikel geeft in totaal negen tips. Wij verwijzen geïnteresseerden naar het desbetreffende artikel maar willen u de laatste niet onthouden:

"Finally, realize that you cannot do it all the first time. Your first audit will not be as good as subsequent audits. The first audit provides experience for better future audits."



COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.



## ONDERWIJS

### Inleiding

Sinds enkele maanden worden bij KKC Amsterdam iedere week een aantal personeelsleden en externe cursisten opgeleid in het gebruik van het toepassingspakket Multiplan.

Iedere deelnemer aan de cursus Multiplan beschikt over een eigen computerconfiguratie welke is opgebouwd uit de volgende delen:

- IBM PC met 128 Kb intern geheugen en 2 diskette drives;
- IBM 80 koloms matrix printer.

Dit artikel besteedt aandacht aan de volgende punten:

- a. de functie van Multiplan en de toepassingsmogelijkheden in algemene zin;
- b. de toepassingsmogelijkheden in de accountantspraktijk;
- c. de inhoud van de cursus;
- d. nazorg.

### De functie van Multiplan en de toepassingsmogelijkheden in algemene zin

Multiplan is een programmapakket dat kan worden gebruikt voor:

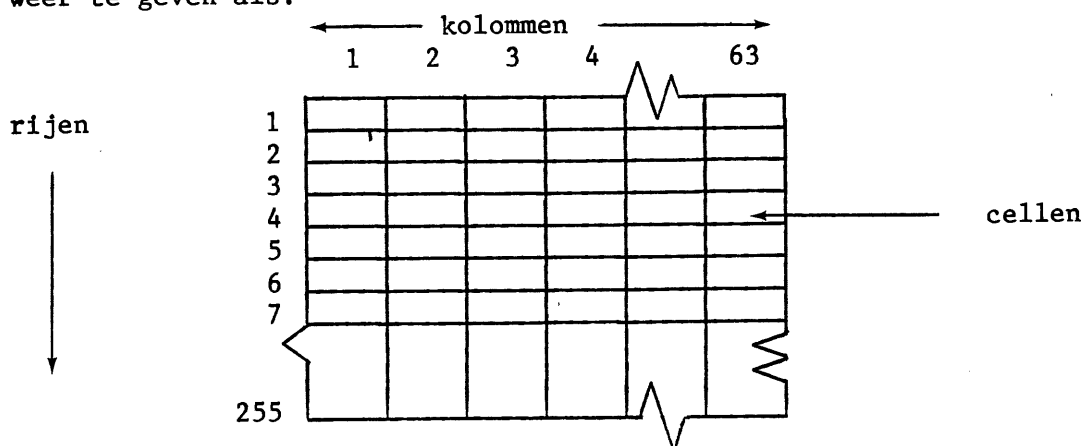
1. Het maken van eenvoudige modellen.  
Een model is een beschrijving van een systeem, dat dient om het gedrag van dat systeem te bestuderen (zo geeft een verlies en winstrekening een bepaalde beschrijving van een bedrijf).
2. Het plannen van activiteiten.

Om bovengenoemde activiteiten te kunnen uitvoeren moeten door de gebruiker de volgende gegevens worden ingevoerd:

- getallen;
- formules; dit zijn rekenregels die op basis van een bewerking op een of meer getallen of andere formules, een nieuw getal opleveren;
- tekst; dit dient voornamelijk als omschrijving.

De wijze waarop de ingevoerde informatie door Multiplan wordt vastgelegd is de matrixvorm.

Het is zodoende te zien als een elektronisch kolommenvel. Schematisch weer te geven als:



Multiplan is een pakket dat tot een familie van gelijksoortige pakketten behoort. Zij worden aangeduid met termen als: spread sheets, electronic work sheets, etc.

Een erg bekend pakket uit deze familie van een andere fabrikant is VisiCalc.

Het gebruik van een dergelijk elektronisch kolommenvel gaat ten opzichte van het klassieke 14-kolommenvel veel voordelen opleveren als met bijna identieke basisgegevens verschillende resultaten moeten worden verkregen. Bij modellen zal men de vraag stellen "als ik nu gegeven X verander, hoe verandert dan het totaalresultaat". Bij plannen zal men vragen stellen in de trend van "als ik activiteit X in deze week plan, hoeveel beschikbare uren heb ik dan nog over?". Beide vragen zijn voorbeelden van "What if" vragen.

Heeft men van een bepaald getallenoverzicht alleen maar vierkantstellingen nodig, dan kunnen de volgende overwegingen een rol spelen om het elektronisch kolommenvel in plaats van het 14-kolommenvel te gebruiken:

- a. Het getallenoverzicht moet periodiek in dezelfde vorm worden gemaakt. Er wordt dan eenmaal een elektronisch kolommenvel gemaakt met de kolom- en rij-omschrijvingen en de formules voor de kolommenrijtellingen.  
Door periodiek dit elektronisch formulier te kopiëren en te vullen met de getallen worden automatisch de gewenste tellingen verkregen.
- b. Er is een getypte versie van het 14-kolommenvel nodig. Van het elektronisch kolommenvel is eenvoudig een afdruk te maken. Het typewerk kan dan worden uitgespaard.
- c. De kans is aanwezig dat een andere representatie van de getallen of de totalen wordt verlangd. Op het elektronisch kolommenvel kunnen met enkele handelingen de getallen worden veranderd in percentages van totalen of kunnen totalen worden vervangen of uitgebreid met gemiddelden.
- d. Er is al direct een behoefte een bepaalde waarde zowel absoluut als relatief weer te geven.
- e. Er bestaat naast totalen behoefte aan gemiddelde en/of standaardafwijking.

#### Toepassingsmogelijkheden in de accountantspraktijk

Zoals uit het bovenstaande valt af te leiden zijn er in de accountantspraktijk diverse situaties denkbaar waarbij het gebruik van een elektronisch kolommenvel de doelmatigheid van de werkzaamheden kan verbeteren. Te denken valt aan:

- consolidaties;
- afschrijvingsstaten;
- kolommenbalansen;
- het berekenen van kengetallen aan de hand van ingevoerde gegevens;

- begrotingen waarbij gebruik wordt gemaakt van de mogelijkheid tot "what if" vragen;
- kostprijsberekeningen;
- investeringsmodellen;
- maken van vergelijkbare cijfers; bijvoorbeeld door het laten omrekenen van absolute resultaten in procenten van de omzet.

## Inhoud van de cursus

De cursus duurt twee dagen en vindt plaats op de maandag en dinsdag. Op de eerste dag wordt na een zeer korte inleiding overgegaan tot het klassikaal uitwerken van een budgetprobleem met Multiplan.

In de inleiding worden zaken aan de orde gesteld als:

- wat is Multiplan;
- de onderdelen met hun functies van de IBM PC;
- wat is een diskette;
- enkele besturingscommando's voor de IBM PC.

De tweede dag wordt ingegaan op de toepassingsmogelijkheden alsmede de mogelijke fouten die gemaakt kunnen worden bij het gebruik van Multiplan met de controles die deze aan het licht kunnen brengen. Vervolgens krijgt iedere deelnemer opdracht om de volgende elektronische kolommenvellen te maken:

- specificaties van machines, gebouwen en auto's van bedrijven A en B;
- een toelichting van A en B met eliminatie- en consolidatiekolom;
- een balans van A en B met eliminatie- en consolidatiekolom;
- een verlies en winstrekening van A en B met eliminatie- en consolidatiekolom.

Men moet bij deze opdracht gebruik maken van de mogelijkheid die Multiplan biedt om gegevens die in één kolommenvel zijn verkregen, bijvoorbeeld de totalen van de specificaties, over te nemen in een ander vel.

Bij het uitvoeren van de opdracht is de cursusleider continu beschikbaar. De cursisten wordt echter aanbevolen zo veel mogelijk gebruik te maken van het handboek, de quick reference guide en de Help-toets. Gedurende de resterende drie dagen van de week is de apparatuur bij voorrang beschikbaar voor eigen oefening van de cursisten van die week.

## Nazorg

Wanneer diegenen die de cursus hebben gevolgd bij het maken van elektronische kolommenvellen ten behoeve van hun praktijk ondersteuning nodig hebben, dan kunnen zij de hulp inroepen van de cursusleider die, in de betreffende week dat het probleem zich voordoet, de cursus geeft of van het AC-kernlid, dat in die week als begeleider/ster fungeert.

