KMG Klynveld EDP Audit Services

COMPACT

87/1

Computer en Accountant

Internationaal literatuuronderzoek naar computermisbruik in strafrechtelijk perspectief

door mr. V.A. de Pous

Geïntegreerde gegevensverwerking

door drs. H.C. Kocks

winter 1986/lente 1987

C O M P U T E R E N A C C O U N T A N T

INHOUDSOPGAVE

Nummer 43 **Winter 1986/Lente 1987**
ISSN 0920-1645

Winter 1986/Lente 1987

VAN DE REDACTIE

1. KMG Klynveld Kraayenhof & Co. heeft besloten om de naam van de Automatisering & Controle-groep te wijzigen.

   In de afgelopen jaren heeft de Automatisering & Controle-groep een duidelijke groei doorgemaakt.
   Deze groei heeft een toenemende specialisatie op deelterreinen van EDP auditing mogelijk gemaakt. Als gevolg van de specialisatie die vooral op diepgang in de beoordeling is gericht, zijn in toenemende mate bijzondere opdrachten verkregen, die buiten de bestaande algemene controlepraktijk liggen. Dit neemt niet weg dat een ondersteuning van de algemene accountantspraktijk een groot deel van onze inspanning zal blijven vragen, niet alleen bij betrouwbaarheidsonderzoeken in het kader van de jaarrekeningcontrole, maar eveneens voor het ontwikkelen van geautomatiseerde hulpmiddelen in de vorm van audit software-pakketten.

   Ten einde tot een duidelijker profilering van het gehele werkterrein te komen met aansluiting op de met name in Angelsaksische landen gevestigde beroepsaanduiding van EDP auditor, is gezocht naar een passende naam, waarmee de brede dienstverlening op het gehele gebied van EDP audit kan worden aangeduid.

   Gekozen is voor de naam **KMG Klynveld EDP Audit Services** *)

   Wij verwachten dat onze groep zich onder deze naam nog duidelijker kan profileren dan tot heden reeds het geval was.

2. Wat onwennig maar gesterkt zijn wij uit onze periode van herbezinning gekomen. Wij schreven u hierover in het zomernummer 1986. Dit nummer betekende tevens de afsluiting van 12½ jaar redactioneel werk. Een belangrijk deel van door ons verworven kennis en ervaring uit deze periode hebben wij geactualiseerd. Vervolgens neergelegd in de jubileumbundel "24 over EDP-auditing", die verschenen is in het najaar van 1986.

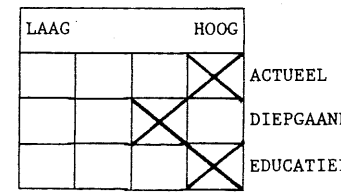
   Het verheugt de redactie zeer dat wij onze interne en externe relaties een exemplaar hebben kunnen aanbieden. Wij hopen dat u hiermee een indruk gekregen hebt van de "State-of-the-art of EDP auditing in the Netherlands".

   Voor een boekbespreking van "24 over EDP-auditing" van de hand van D. Boom, Bibliotheek & Documentatie (BIDOC) verwijzen wij naar blz. 6.

*) afkorting EAS

3. Nu naar het heden. Na de jubileumbundel hier de nieuwe uitgave van Compact. Het is een erg dik nummer, waarin een aantal relatief omvangrijke, maar leerzame artikelen zijn opgenomen.

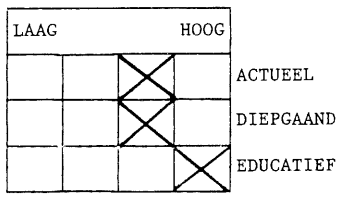
Internationaal literatuuronderzoek
naar computermisbruik
in strafrechtelijk perspectief
door mr. V.A. de Pous



In het voor u liggende nummer van Compact treft u een bijzonder artikel aan. Vestigen wij normaliter de aandacht op de aspecten van het gebied EDP audit, in dit nummer maken wij een uitstapje naar het strafrechtgebeuren. Ten behoeve van de uitvoering van een opdracht tot onderzoek naar de effectiviteit van getroffen en op korte termijn te treffen maatregelen van computerbeveiliging bij bedrijfsleven en overheid in Nederland in opdracht van de Commissie Computercriminaliteit (ook wel de Commissie Franken genoemd, naar haar voorzitter), moest ook een literatuuronderzoek plaatsvinden naar regelgeving in binnen- en buitenland met betrekking tot computerbeveiliging.
Wij hebben de bekende jurist/publicist mr. V.A. de Pous bereid gevonden ons bij de uitvoering van dit onderdeel van de opdracht een handje te helpen. Mr. De Pous heeft op ons verzoek ook een internationaal literatuuronderzoek naar computermisbruik in strafrechtelijk perspectief uitgevoerd.
Zijn tekst blijkt voor de lezers van Compact interessant omdat niet slechts op de strafrechtelijke problemen wordt ingegaan doch omdat ook aandacht wordt besteed aan de verschillende vormen van computercriminaliteit en deze kort worden beschreven. Al met al een zeer lezenswaardig artikel dat weer eens een ander licht werpt op de beheersbaarheidsproblematiek (interne controle en beveiliging) van de geautomatiseerde informatieverwerking.

Waar mr. De Pous wetteksten en uitspraken van rechters interpreteert schiet de kennis van EDP auditors, die de redactie van dit tijdschrift vormen, tekort. De keuze van de uitspraken en daaropvolgende interpretaties komen dan ook geheel voor rekening van mr. De Pous.

Winter 1986/Lente 1987



"Geïntegreerde gegevensverwerking"
door drs. H.C. Kocks

In aansluiting op het artikel
"Accountant en elektronische informatieverwerking"
van prof. D. Steeman, wordt in deze bijdrage nader ingegaan op "geïntegreerde gegevensverwerking".

Het probleem doet zich echter voor dat niet eenvoudig is aan te geven wat nu precies onder geïntegreerde gegevensverwerking moet worden verstaan, omdat dit begrip in de automatisering en controleliteratuur in twee betekenissen voorkomt, namelijk "samengevoegd" en "gemeenschappelijk". In het algemeen is gemeenschappelijk gebruik een gevolg van samenvoeging terwijl gemeenschappelijk gebruik tevens samenvoeging tot gevolg kan hebben.
Integratie, in beide betekenissen, heeft zich op vele gebieden in de organisatie gemanifesteerd als gevolg van (technologische) ontwikkelingen in de automatisering. Terwille van de duidelijkheid is gekozen voor een benaderingswijze van de problematiek waarbij het ontstaan en de (historische) ontwikkeling in de automatisering wordt beschreven en waarbij successievelijk voorkomende "integratie-aspecten" worden behandeld alsmede gevolgen ervan voor de interne controle.

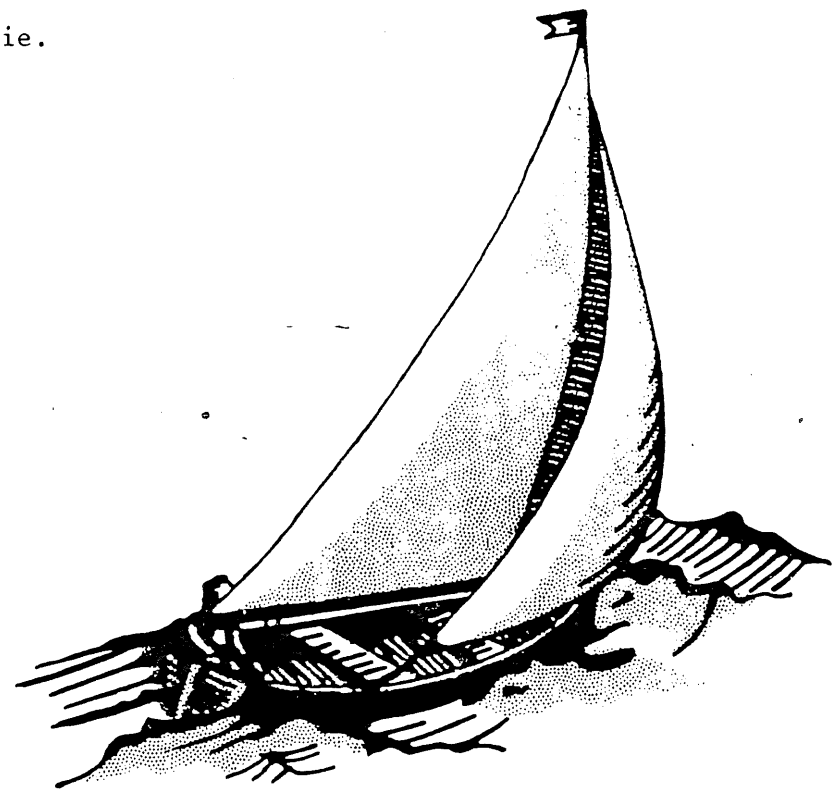
Vanuit een basisconcept zullen de ontwikkelingen en invloeden als gevolg van toenemende geavanceerdheid van de automatisering worden behandeld. Tot uitdrukking zal worden gebracht dat automatisering aangemerkt kan worden als het probleem van onderlinge verschuivingen zoals het verschuiven van (controle)activiteiten van de gebruikers- naar de automatiseringsorganisatie en van de automatiseringsorganisatie naar besturingsprogrammatuur. De daarmee samenhangende delegatie- en integratie-aspecten bepalen de invloed op de interne controle.

Wanneer we een tweetal zinsneden vrijelijk citeren uit het voorwoord en de epiloog van "24 over EDP-auditing" dan bevelen wij de pennevruchten van beide auteurs in uw aandacht aan; bedenk hierbij dat EDP auditing nog in de kinderschoenen staat.

De rubrieken met actuele info vindt u op de gebruikelijke plaats.
Ook op deze wijze pogen wij u ondersteuning te geven.

4. Door uw vragen/kritiek/manuscripten
houdt u ons op goede koers.
Wij beantwoorden gaarne
uw signalen in dit blad of
anderszins gebruikmakend van
onze EAS vakbekwaamheid.
Wees verzekerd
van onze welgemeende belangstelling.

De Redactie.



Winter 1986/Lente 1987

COMPACT (R) is een uitgave van
KMG Klynveld EDP Audit Services

Deze informatie is in de eerste plaats bestemd voor diegenen, die in de algemene controlepraktijk werkzaam zijn. De in dit tijdschrift weergegeven meningen mogen niet altijd gezien worden als officiële zienswijzen van KMG Klynveld Kraayenhof & Co. De in de rubrieken besproken artikelen worden soms geheel opgenomen of verkort aangehaald, tevens als regel voorzien van commentaar.

Redactie:
A.H.C. Koedijk
A.W. Neisingh
Prof. D. Steeman
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.

ISSN 0920-1645

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).

Boekbespreking

24 over EDP-auditing

door D. Boom/Bibliotheek & Documentatie

De Automatisering en Controle-groep van KKC, die sinds kort KMG Klynveld EDP Audit Services heet, verraste de vele toehoorders op de laatstgehouden Najaarsconferentie met de uitreiking van een bundel over EDP Auditing. De uitreiking vormde een apotheose nadat de EDP Audit Services eerder op deze dag een tweetal produkten uit eigen keuken demonstreerde nl. FAT en Palet. In COMPACT, het huisorgaan van EDP Audit Services, worden de ontwikkelingen op automatisering en controle-gebied uiteengezet. De reden voor uitgave van deze fraai vorm gegeven bundel was gelegen in het feit dat COMPACT 12 1/2 jaar bestaat. In de loop van al deze jaren zijn een groot aantal artikelen geschreven door medewerkers van de AC-groep die in een groot aantal gevallen hun actualiteitswaarde hebben behouden. Uit inmiddels 42 afleveringen COMPACT is een selectie gemaakt van 21 artikelen, die voor de jubileumuitgave werden geactualiseerd, terwijl een zestal nieuwe artikelen werd geschreven om de bundel te completeren. Alle artikelen hebben gemeen dat zij op enigerlei wijze het werkgebied aanduiden.

De inhoud

De inhoud van deze bundel laat zich niet zo makkelijk beschrijven. Ieder artikel staat immers op zichzelf en kan dus door de lezer zelfstandig worden gelezen zonder eerst kennis hoeven te nemen van wat voorafgaand is geschreven.
De inhoud van dit boek is gesplitst in een 5-tal hoofdstukken. De indeling maakt het mogelijk snel een selectie te maken van artikelen die voor hem of haar interessant zijn. Makkelijk is dat ieder hoofdstuk wordt voorafgegaan door een samenvatting. Tevens is daarbij aangegeven of het artikel actueel, diepgaand of educatief is. Hoofdstuk 1 is de inleiding en bestaat uit een tweetal overzichtsartikelen die een indruk geven van wat EDP auditing inhoudt.
Hoofdstuk 2 is de romp van de bundel en beslaat liefst 11 artikelen. Het hoofdstuk is getiteld Automatisering en Controle en de lezer treft hier de meest uiteenlopende artikelen aan, zowel beschrijvend als zeer technisch. Hoofdstuk 3, Toepassing van de computer in de accountantscontrole, omvat een 4-tal artikelen over o.a. het gebruik van de micro in de controle.
Hoofdstuk 4, Gegevensbeheer en datacommunicatie, heeft een 7-tal artikelen die op de wat technische aspecten van EDP auditing ingaan, zoals de organisatie van gegevensbeheer, database management systemen en netwerkbeveiliging.
Hoofdstuk 5 tenslotte, gaat in drie artikelen op "nieuwe ontwikkelingen" in, wat tevens de naam van dit hoofdstuk is. Aan de orde komen o.a. 4e generatietalen, de Wet persoonsregistraties en een heldere uiteenzetting over Knowledge Based Systems ofwel kennissystemen.

Algemene indruk

De redactie van de jubileumbundel is er naar mijn mening goed in geslaagd een selectie te maken uit de vele interessante COMPACT-artikelen. De bundel geeft een goed overzicht van wat er op dit moment gaande is in de EDP audit omgeving. Het boek zal dan ook voor velen een interessant naslagwerk zijn en voor 'nieuwkomers' een bruikbaar studieboek.

De Samsom uitgave "24 over EDP-auditing" is in de boekhandel verkrijgbaar tegen f69,--per exemplaar.

ACTUALITEITEN

1. Gegevensbescherming

Onder deze titel is recentelijk een nieuw boek verschenen bij Kluwer (ISBN 90 267 1130 1). De ondertitel luidt: "Een praktisch model voor het opzetten en invoeren van een systeem van gegevensbeschermende maatregelen". Auteurs zijn J.F. Bautz, A. Brouwer en A.J.F.M. Jongenelen.
Over dit praktijkgericht boek volgt in de komende Compact een boekbespreking.

2. (Technische) termen op het gebied van datacommunicatie

Het komt regelmatig voor dat aan BIDOC een (technische) vraag wordt gesteld over nogal bekend klinkende begrippen maar waarvan men de precieze inhoud niet kan verklaren.
Zo'n vraag bijvoorbeeld: Hebben jullie informatie over datacommunicatie-apparatuur die gebruik maakt van echo cancellation op point-to-point 2-draads huurlijnen al dan niet voorzien van hypothetische referentieverbindingen voor gebruik in synchrone openbare netwerken. De apparatuur dient conform CCITT V- en X-serie gekeurd te zijn.

Teneinde dit soort vragen adequaat te kunnen beantwoorden maken wij sinds kort gebruik van een door Philips opgesteld informatiepakket over datacommunicatie waarvan wij de verklarende woordenlijst ter kennisneming aanbevelen.

3. Data Base & Accountant (derde druk) ISBN 90 14 03622 1

De tweede (in 1985 geheel herschreven) druk van het boek raakte in ruim een jaar uitverkocht. De thans verschenen derde druk wijkt inhoudelijk niet of nauwelijks af, maar de toegankelijkheid van het boek is vergroot en de inzichtelijkheid in onderlinge samenhang tussen de delen van het boek verhoogd. Van de "achterflap" citeren wij.....
Het boek beoogt vooral begripsvorming te kweken, niet om technische detailkennis te verschaffen. Waar noodzakelijk, wordt de techniek echter niet geschuwd. De technische uitwerkingen die men in de praktijk ontmoet worden daarbij gerelateerd aan beheersbaarheidsmodellen.
Een algemeen inzicht wordt verschaft in gegevensmodellen en database-technieken, waarbij zowel netwerk- als relationele database-systemen worden behandeld. Onontkoombaar daarbij is de on-line-verwerking (teleprocessing).

Uit de beschrijving van de beheersbaarheidsaspecten vloeit een opsomming van aandachtsgebieden voort die onderzocht moeten worden bij een systeemgerichte aanpak van accountantscontrole. Data Dictionary Directory Systemen spelen hierbij een steeds belangrijker rol.
Het boek besluit met hoofdstukken over gespreide (distributed) databases, database-machines, gebruikerstalen en microcomputers. In dit laatste hoofdstuk wordt ook de micro als "audit tool" voor de accountant beschreven.

Het boek richt zich primair op de algemene - niet op automatisering gespecialiseerde - accountant; voorts is het boek bestemd voor (aankomend) EDP auditors en gebruikers, in het bijzonder gebruikers die beheersfuncties hebben ten aanzien van gegevens en/of gegevensverwerkende processen.

Het boek is geschreven door een team van specialisten op het gebied van EDP audit van KMG Klynveld Kraayenhof & Co. onder redactie van A.H.C. Koedijk, redacteur Compact.

4. Onderzoek computerbeveiliging

De Commissie Computercriminaliteit (Commissie Franken) bracht op 8 april 1987 haar eindrapport uit aan de Minister van Justitie. Als bijlage bij het rapport van de Commissie zijn gevoegd de resultaten van het door KMG Klynveld EDP Audit Services uitgevoerde onderzoek naar de huidige stand van zaken bij het bedrijfsleven en de overheid in Nederland met betrekking tot de effectiviteit van genomen en op korte termijn te treffen beveiligingsmaatregelen tegen computercriminaliteit.

Het totale beeld van de computerbeveiliging zelfs bij organisaties met grootschalige automatisering is weinig geruststellend.

Een en ander is weergegeven in onderstaand overzicht:

Kwalificatie met betrekking tot de beveiliging

Automatiseringsgraad	Goed		Voldoende		Geen Oordeel		Onvoldoende		Totalen	
	Aantal	%	Aantal	%	Aantal	%	Aantal	%	Aantal	%
Kleinschalig	0		7	11	25	41	29	48	61	100
Middelgroot	0		8	33	4	17	12	50	24	100
Grootschalig	0		42	54	-	-	36	46	78	100
Totalen: aantallen	0		57		29		77		163	
%		0		35		18		47		100

Opvallend is in de eerste plaats, dat het predikaat "goed" aan geen der deelnemers kon worden toegekend, hoewel bij de deelnemers met grootschalige automatisering 8 deelnemers er niet ver vandaan zitten. Naarmate de organisatie grootschaliger wordt, neemt het percentage der deelnemers met voldoende te achten beveiliging toe en dat van "geen oordeel" progressief af. Voorts blijkt, dat de percentages der deelnemers bij wie "onvoldoende" beveiliging werd vastgesteld, voor alle categorieën rond de 50 liggen.
U zij gewaarschuwd!

5. **Aansprakelijkheid en automatisering,** door J. Vossen.
Bijeenkomst Sectie Computerrecht van het Nederlands Genootschap voor Informatica op 19 maart 1987.
Inleiding door mr. R.W. Holzhauer (Erasmus Universiteit) en mr.drs. C. Stuurmans (Vrije Universiteit).

Opgeleverde systemen die niet functioneren volgens afspraak; overschrijding van overeengekomen data; systemen die wel werken maar in de praktijk niet bruikbaar zijn.
Wie draait op voor de gevolgen: opdrachtgever, opdrachtnemer of de eventuele adviseur?
Aansprakelijkheid kan voortvloeien uit wanprestatie of rechtstreeks uit de wet (onrechtmatige daad, produkt aansprakelijkheid). Aansprakelijkheid kan ook voortvloeien uit onderhandelingen tijdens de precontractuele fase.
Aansprakelijkheden kunnen bij contract worden verdeeld of beperkt. Verzekering is een mogelijkheid.

Mr. R.W. Holzhauer
Aansprakelijkheid in de precontractuele fase (vooronderzoek, offerte en onderhandeling)

Rechters zijn steeds meer geneigd om de precontractuele fase bij het contract mee te nemen. De inhoud uit de precontractuele fase wordt bij de overeenkomst meegenomen en leidt tot aansprakelijkheid uit wanprestatie. Dit heeft invloed op het contract. Er bestaat ernstige twijfel of het zgn. vier hoeken beding (alleen wat in het contract staat is bindend) nog gehonoreerd zal worden.
Enkele gevolgen hiervan specifiek voor de precontractuele fase:
- terugtrekken uit onderhandelingen is niet te allen tijde mogelijk. Onzorgvuldig terugtrekken kan tot vergoedingen leiden;
- juridische betekenis van afgelegde verklaringen tijdens de precontractuele fase (bijvoorbeeld responsetijden, compatible). Toezeggingen van deze aard kunnen leiden tot wanprestatie.

Mr.drs. C. Stuurmans
Aansprakelijkheid in de contractuele fase

Basisverplichting die op de adviseur rust: zorgvuldigheid

Hoe is dit in te vullen?
Toetsing aan inspanning van een redelijk handelend vakgenoot.
Het Hof van Den Haag heeft dit voor de automatisering als volgt ingevuld "redelijk handelend en bekwaam automatiseringsdeskundige".
Nadere invulling hiervan geschiedt door gedragscodes van beroepsorganisaties zoals:
- COSSO
- NOVAA
- VRI
- NIVRA
- ROA/OOA

Verplichtingen van de adviseur:
a. Informatieplicht

Doordat bij automatisering vaak sprake is van een ondeskundige cliënt ligt op de informatieplicht meer nadruk dan bij ander aansprakelijkheidsrecht.
Grenzen aan de informatieplicht:
1. cliënt heeft eigen verantwoordelijkheid ten aanzien van de keuze van de adviseur;
2. de adviseur verzamelt informatie in samenwerking met de cliënt. De adviseur is niet verantwoordelijk voor achtergrondinformatie die door de cliënt wordt achter gehouden;
3. de cliënt dient zelf te informeren naar zaken die hij niet begrijpt.

b. Eigen belang

De adviseur mag nooit uitsluitend eigen belang nastreven.

c. Doorverwijzen

De adviseur is verplicht bij gebrek aan kennis door te verwijzen.

d. Eigen verantwoordelijkheid

De adviseur mag zich niet oneindig laten leiden door de wensen van de cliënt. Bij het bereiken van zijn ondergrens (van eigen verantwoordelijkheid) dient hij dit schriftelijk te melden aan de cliënt.

e. Meerpartijenverhouding

In dit geval krijgt de adviseur er een taak bij, namelijk controleplicht.

Bij een overeenkomst gaat een adviseur een inspanningsverplichting aan. Bij wanprestatie dient de opdrachtgever aan te tonen dat er sprake van een fout is. Dit in tegenstelling tot een resultaatverplichting waarbij niet de opdrachtgever maar de tegenpartij moet aantonen dat wel een juist resultaat is geleverd.

Beperking van aansprakelijkheid:

1. exoneratieclausule;
   Deze kan betrekking hebben op:
   - omvang van de vergoeding;
   - ernst van de fout die gemaakt moet zijn alvorens men aansprakelijk is;
   - vrijwaring van aanspraken van derden;
   - garanties die men geeft (maar ook niet meer dan dat);
   - overmacht.

   Dit soort clausules is over het algemeen geoorloofd.
   Onder omstandigheden is een beroep op "in strijd met de goede trouw" mogelijk:
   - passend beding;
   - verhoudingen tussen partijen;
   - indien men ervoor verzekerd is.
2. Verzekeringen.

Overweging

Het aansprakelijkheidsvraagstuk leent zich voor risicobeheersing. Het identificeren van de risico's, inschatten en evalueren van de gevolgen kunnen bijdragen tot het beheersen van het risico (bijvoorbeeld beperken van de risico's).

6. KMG Computer Newsletter — K Memory

march 1987

K Memory wordt uitgegeven door KPMG International Office, Marketing and Communications Unit onder supervisie van H. Roos, als lid van de Computer Audit Sub-Committee (CASC).

Het blad is in eerste aanleg voor intern gebruik binnen KPMG. Voor belangstellenden - ook voor onze cliënten - is een exemplaar van de jongste editie, namelijk die van March 1987 beschikbaar. De uitgave van December 1986 is nog beperkt leverbaar.

De inhoud van March 1987 handelt over de volgende onderwerpen, geschreven door een internationaal gezelschap van auteurs:

- "The costs of computer software" in de rubriek Software Accounting. Research en informatie over dit onderwerp is afkomstig van Michel Léger, Frinault Fiduciaire.
- "Tomorrow's accountant: expert aided?" in de rubriek Software Development.
  Deze samenvatting is gebaseerd op een artikel van Robin Mathieson, Peat Marwick McLintock.
- "The role of accountants" in de rubriek Computer fraud is gebaseerd op een lezing van William List, Peat Marwick McLintock.
- "Automated data entry in WISPR" in de serie Software Integration, geschreven door H.H. van den Brink, KMG Klynveld EDP Audit Services.
- "Dial-IBM" in de rubriek KMG computer services - office by office, bijdrage van D. Boom, BIDOC.
- Onder de rubriek "Bits & Pieces" wordt informatie verschaft over CARS and Culprit Update, Culprit/EDP Auditor training course van 1-5 juni 1987 alsmede praktijkervaringen met WISPR en UFFE.

Voor meer diepgaande informatie verwijzen wij naar het blad met onderliggend studiemateriaal.

COMPACT is een uitgave van
KMG Klynveld EDP Audit Services

Winter 1986/Lente 1987

INTERNATIONAAL LITERATUURONDERZOEK NAAR COMPUTERMISBRUIK IN STRAFRECHTELIJK PERSPECTIEF

door mr. V.A. de Pous

0. Inleiding

De internationale literatuur hanteert geen eenduidig begrip van "computercriminaliteit". Zowel aanduiding (computer crime, computer-related crime, computer abuse, edp crime, information processing crime) als inhoud en omvang van aan te geven (rechts)gebied verschillen.

Daarnaast brengt men computermisbruik in strafrechtelijk perspectief (hierna te noemen: computermisbruik) veelal onder sociale aspecten van geautomatiseerde gegevensverwerking, maar ook onder technische (beveiliging) aspecten van geautomatiseerde gegevensverwerking. In de voornamelijk Engelstalige literatuur lopen afzonderlijke aandachtsgebieden in elkaar over: "computer security", "computer protection", "computer litigation", etc.

Voor wat betreft de juridische wetenschap valt op dat tot op heden niet of nauwelijks enige grondslagendiscussie is gevoerd ten aanzien van het bestaan van "computer law" als afzonderlijk rechtsgebied. "Klassieke" rechtsgeleerden rubriceren computermisbruik als strafrecht, bijvoorbeeld in het kader van "white collar crime" of economische misdrijven. Daarnaast pleegt men in computerrecht-kringen computermisbruik als onderdeel van het informatierecht, informaticarecht of computerrecht te beschouwen.

De OEDCD spreekt van "computer crime" of "computer related crime" als "ieder wederrechtelijk, onethisch of onbevoegd gedrag met betrekking tot automatische gegevensverwerking en/of verzending van gegevens". (Rapportage 1983.)

Twee punten vallen hier op. Allereerst wordt niet gesproken van elektronische gegevensverwerking omdat de elektronische wijze van het verwerken van gegevens niet van belang is. Het feit dat een en ander geautomatiseerd plaatsvindt bepaalt het karakter. Daarnaast kan nog worden aangevoerd dat sommige processen, zoals vastleggen van gegevens magnetisch of optisch geschiedt. Tevens vermijdt men het begrip "informatie".
De ontvanger bepaalt uit een veelheid van gegevens zelf wat informatie is; welke gegevens tot informatie worden. En daarmee wordt informatie een subjectief en derhalve voor juridische normstelling een onhanteerbaar begrip.')

---

1) Zie nieuwe voorstellen van de Commissie Computer Criminaliteit (Commissie Franken) pag. 114 e.v. van genoemd rapport.

Indien computermisbruik wordt bekeken met de computer als invalshoek, kan worden onderscheiden in ontoelaatbare handelingen met betrekking tot: de invoer, verwerking, opslag en uitvoer van gegevens. Tevens kan men computercriminaliteit (traditioneel) strafrechtelijk benaderen door uit te gaan van bestaande indelingen en delicten. Vallen diefstal van computerprogrammatuur of verduistering van "elektronisch" geld onder de bestaande vermogensdelictomschrijvingen? (Zie voor een overzicht in casu IUS 7, Antwerpen 1985.)

Computermisbruik wordt "abuser friendly".
Computersystemen worden steeds meer gebruikersvriendelijk en dus ook "misbruikersvriendelijker". J.J. Buck Bloombecker, directeur van het National Center for Computer Crime (een nonprofit onderzoeksinstituut in Los Angeles) noemt de trend dat computers toegankelijker worden "democratization of computer crime" (Computerworld USA, 27 oktober 1986).

Tevens lijken zich andere lijnen af te tekenen.
Computermisbruik wordt in het ruime kader van "the vulnerability of society" geplaatst. (Zie Computer technology and the vulnerability of society, Norwegian Official report, 1986:12). Een grote verscheidenheid aan gevolgen wordt veroorzaakt door het - grootschalig - gebruik van gegevensverwerkende systemen in de postindustriële samenleving.

Voor het eerst in Nederland zal deze benadering onder de aandacht van een breed publiek worden gebracht op een internationaal congres (NGI, Amsterdam, 28-30 september 1987): "Coping with computer-age vulnerability".

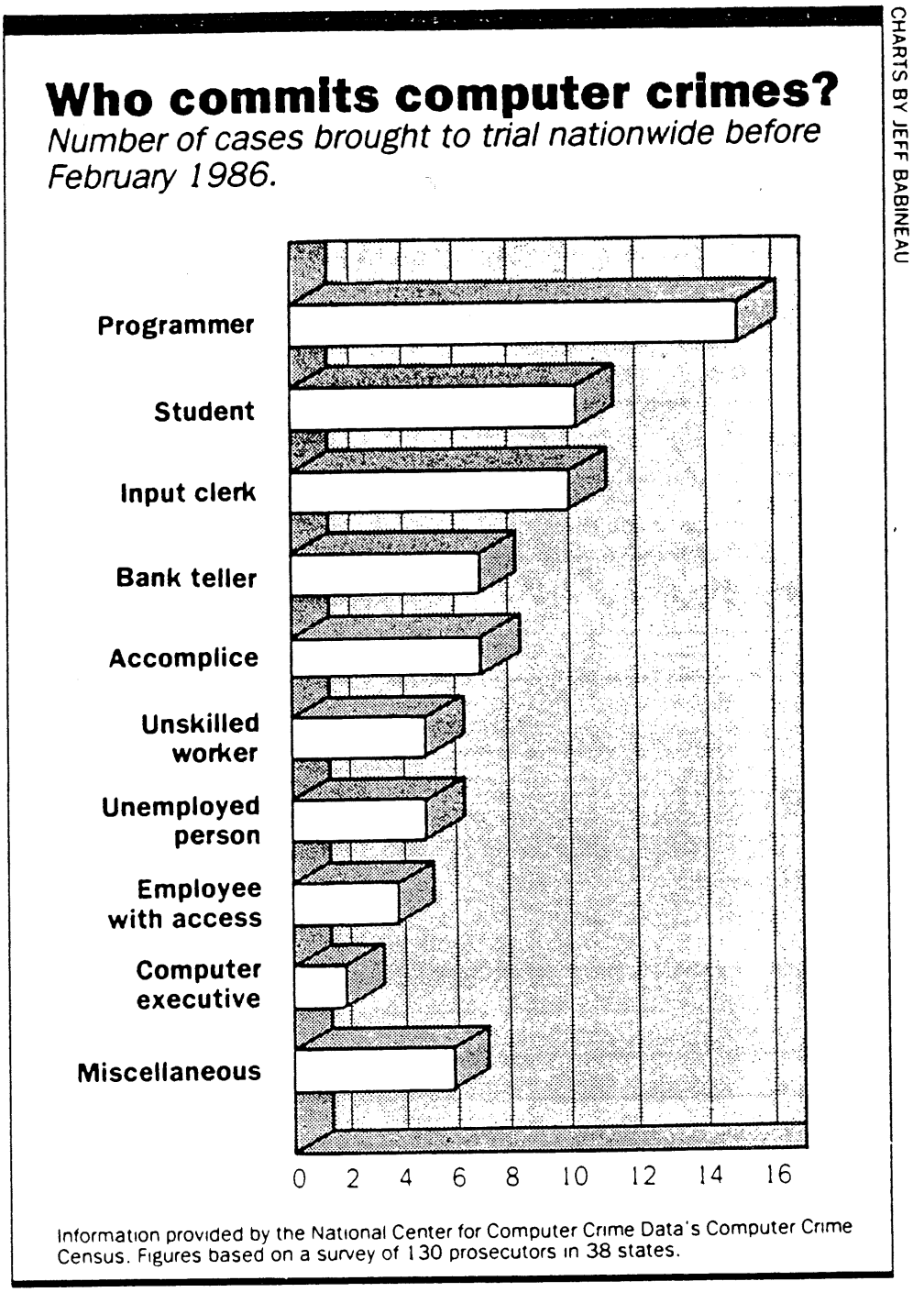
Vast staat dat de bedreigingen nog zullen toenemen, in het bijzonder door het grootschalige kleincomputergebruik met PC of terminal, aangesloten op een centraal computersysteem en het gebruik van nationale en internationale netwerken.

1. Daders

Verschillende mensen maken zich schuldig aan computermisbruik:
- management;
- werknemers;
- derden.

Een type moderne crimineel is de aardige, soms introverte maar vooral gefrustreerde werknemer, die op basis van onvrede met zijn arbeidsomstandigheden overgaat tot computermisbruikhandelingen.
De laatste categorie bestaat uit outsiders. Een outsider is iemand die op afstand werkt, bijvoorbeeld via telefoon- en datanetten en zich met kwade bedoelingen onbevoegd toegang verschaft tot computersystemen.

Figuur 1: Wie pleegt computermisbruik?
(Bron: Computerworld USA, 27 oktober 1986)



2. Motieven

"Ik had persoonlijke problemen omdat ik 20.000 dollar schuld had. Maar ik heb ook keihard gewerkt voor ze, en ze passeerden mij voor promotie. Ik ben goed en verdien een betere behandeling (...). Ik besloot ze terug te pakken."

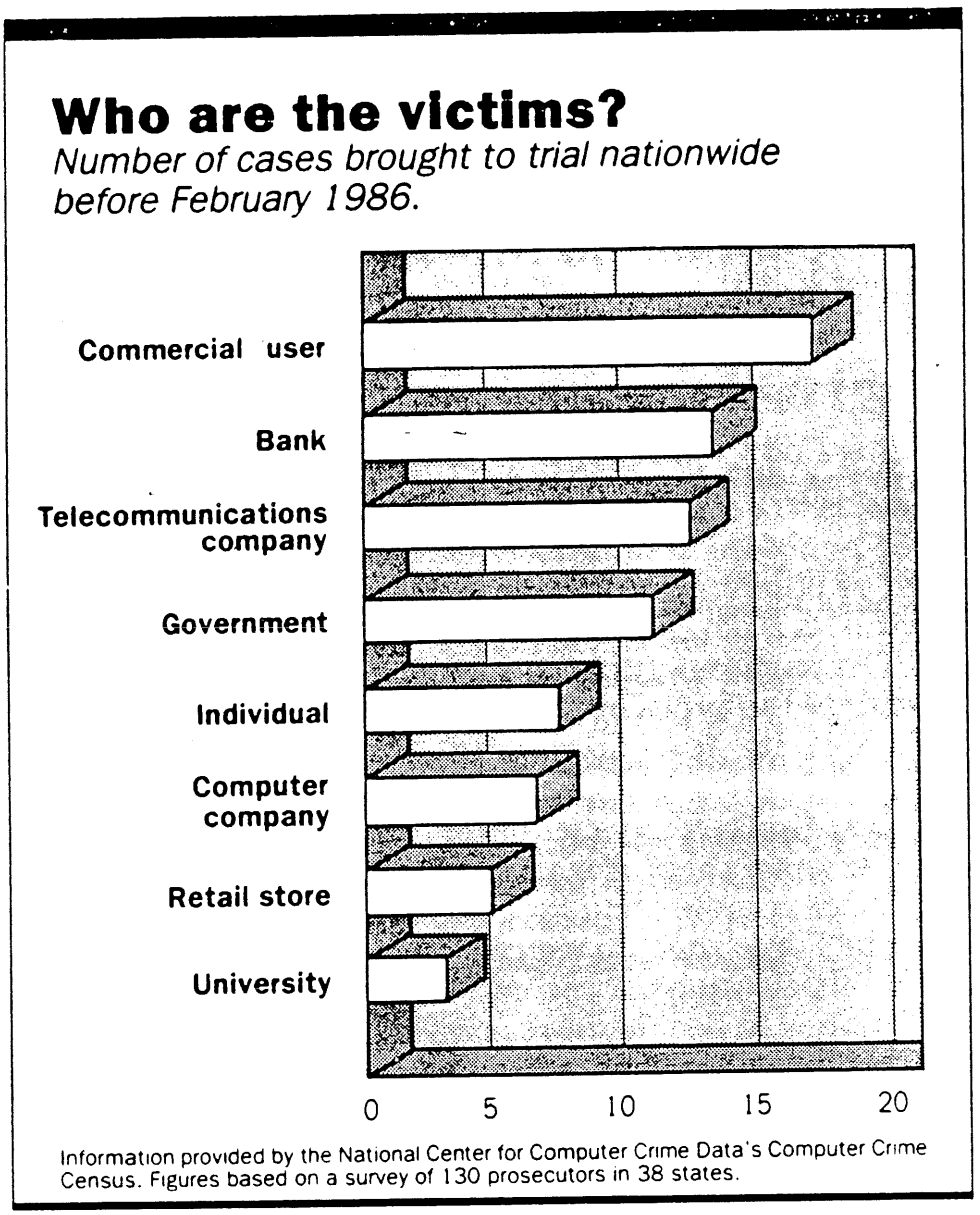
Aldus de Amerikaanse dader van een computermisdrijf. Volgens uit 1985 daterende cijfers van het U.S. Department of Health and Human Service (HHS), dat onderzoek heeft verricht naar de motieven van 46 "computer criminals", vertoont 75 procent van de plegers van misdrijven tegen de Amerikaanse overheid, die verband houden met geautomatiseerde gegevensverwerking, het hierboven geschetste profiel. Men wil vooral geld stelen als reactie op stress en persoonlijke crisis.

Andere motieven voor computerfraude en -misbruik betreffen toevallige ontdekking van mogelijkheden en de kwetsbaarheid van het systeem. Opvallend is dat eveneens factoren als verveling en vrije tijd hierbij een rol spelen.

3. Slachtoffers

Het grootschalig gebruik van systemen voor geautomatiseerde verwerking en transport van gegevens in vrijwel alle onderdelen van de post-industriële samenleving, betekent dat iedereen het slachtoffer van computermisbruik kan worden.

Figuur 2: Wie zijn de slachtoffers?
(Bron: Computerworld 27 oktober 1986)



4. Opsporing en vervolging

Ontdekking van computermisbruik is veelal niet meer dan een kwestie van geluk. En dan begint het pas: het verzamelen van bewijsmateriaal en het opsporen van de dader(s). Vrijwel overal ter wereld heeft men de opsporingstaak in relatie tot strafbare feiten aan politionele organisaties toegewezen. In het algemeen wordt een lage aangiftebereidheid aangenomen, zodat als men al op computermisbruik stuit, het van de betrokkenen afhangt of aangifte wordt gedaan. Bedrijven voelen zich in verlegenheid gebracht door computermisbruik in eigen huis. Er gaan dan ook geen stemmen op om tot een algemene meldingsplicht over te gaan.

Daarentegen is door het Amerikaanse Huis van Afgevaardigden onlangs een wetsvoorstel in behandeling genomen, dat aangifte van fraude en dus ook fraude door middel van EDP, voor accountants verplicht stelt. In ieder geval kan in Nederlands perspectief worden opgemerkt dat de registeraccountant een dergelijke meldingsplicht niet zal steunen, omdat zo'n verplichting hun rechtspositie aantast. Rechtspraak heeft uitgewezen dat deze vrije beroepsgroep geen aanspraak kan maken op een civiel- en strafrechtelijk verschoningsrecht.

In het kader van de justitiële informatievoorziening kan men zich voorstellen dat er een bijzondere meldingsplicht komt voor allerhande opsporingsambtenaren met betrekking tot computermisbruik.

Problemen waarvoor de opsporingsinstanties zich geplaatst zien bij de bestrijding van computermisbruik zijn onder andere de complexiteit van computersystemen, die het onmogelijk maakt dat bij de opsporingsinstanties voldoende kennis aanwezig is over verschillende typen apparatuur - en wat belangrijker is - programmatuur. Veelal zal voor het verkrijgen van relevante gegevens een extern deskundige moeten worden aangetrokken. Daarnaast doet de moeilijkheid van het vinden van bewijsmateriaal zich voor, in het bijzonder bij huiszoeking: welke tape of disk is relevant en hoe ontsluit ik de gegevens of programma's die hierop staan geschreven.

5. Maatregelen

Verschillende maatregelen ter voorkoming, opsporing en vervolging van computermisbruik zijn in de loop der jaren voorgesteld.[1])

Maatregelen met betrekking tot voorkoming van computermisbruik:
- het creëren van een bewustwordingsproces met betrekking tot de kwetsbaarheid van de samenleving door het gebruik van geautomatiseerde gegevensverwerkende systemen, zodat door vrijwillig te nemen maatregelen computermisbruik (en strafwetgeving dan wel toepassing van strafrecht) kan worden voorkomen;
- het activeren van een computermoraal, hetgeen een actief beleid van overheid en bedrijfsleven vraagt dat bepaalde handelingen ten aanzien van geautomatiseerde gegevensverwerking niet door de beugel kunnen. Men

[1]) Zie nieuwe voorstellen van de Commissie Computer Criminaliteit (Commissie Franken)

moet zich bewust worden dat bepaalde handelingen ten aanzien van geautomatiseerde gegevensverwerking niet door de beugel kunnen en dat de persoonlijke levenssfeer van anderen dient te worden gerespecteerd;
- het opzetten van (inter)nationale "Computer Crime Centers".

Maatregelen met betrekking tot opsporing en vervolging van computermisbruik:
- het instellen van een algemene of bijzondere aangifteplicht bij justitie (algemeen: voor iedereen; bijzonder: voor accountants, "security officers", etc.);
- het instellen van een meldingsplicht voor opsporingsambtenaren bij een centrale instantie, zodat onregelmatigheden waarbij computers zijn betrokken, hetzij als hulpmiddel, hetzij als doel aan het licht komen;
- het opzetten van nationale opsporingsteams met bijzondere bevoegdheden, die niet gebonden zijn aan lokale en regionale grenzen;
- het opleiden van bijzondere opsporingsambtenaren met kennis van forensische[1]) informatica (vergl. forensische accountancy);
- het initiëren van een nationaal vervolgingsbeleid in nauw overleg met internationale "law enforcement agencies" (computermisbruik is "grenzeloos");
- openbare aanklagers voorzien van een gedegen juridisch instrumentarium om computermisbruik ook daadwerkelijk te vervolgen, hetgeen aanpassing in de sfeer van strafvordering betekent (één van de meest wezenlijke kenmerken van computermisbruik betreft de snelheid waarmee handelingen worden uitgevoerd);
- het verzorgen van een basiscursus informatica bij openbare aanklagers en rechterlijke macht;
- het instellen van openbare aanklagers ("automatiseringsofficieren") die zich met computermisbruik bezig houden en die zich hebben gespecialiseerd in geautomatiseerde gegevensverwerking, waarbij tevens op de continuïteit van de functie moet worden gelet.

6. Misbruikhandelingen

In het brede kader van computermisbruik staan "computer fraud" of "fraud by computer manipulation" centraal. Daarnaast bestaat veel aandacht voor het zonder toestemming van de rechthebbende, inbreken in computersystemen: "hacking". Ook meldt zich internationaal de software-piraterij als aandachtsterrein en onderdeel van computermisbruik. Tenslotte richten veel ogen zich op het onrechtmatig gebruik van geautomatiseerd verwerkte persoonsgegevens.

Andere misbruikhandelingen in verband met geautomatiseerde verwerking en communicatie van gegevens treden beduidend minder op de voorgrond.
De modus operandi bij computermisbruikers is verschillend.
Vaststaat dat kennis van geautomatiseerde gegevensverwerking voorwaarde is,

[1]) Forentie = strafrechtelijke expertise

echter het niveau van kennis laat zich moeilijk bepalen. Behalve technische kennis zijn toeval en creativiteit ook van invloed.

Een overzichtelijke opsomming van misbruiktechniek geeft "the father of computer crime" Don B. Parker in "White-Collar Crime: Theory and Research", Beverly Hills, 1980).

COMPUTER-RELATED CRIME MODI OPERANDI

As computer-related crime methods become more widely known in the computer field, jargon terms are assigned to them: Trojan horse, salami, superzapping, logic bombs, data leakage, data diddling, piggybacking, and scavenging. These methods have become fascinating to computer technologists because they generally require great skill and detailed knowledge of the system to be attacked. In addition, if they are used with sufficient care, they usually are neither preventable nor detectable even when their use is suspected.

Each of the known technical methods is described below briefly in nontechnical terms.

Data diddling. The unauthorized modification, replacement, insertion, or deletion of data before or during its input to a computer system is called data diddling. This can be done by altering input data forms, punch cards, magnetic tapes or disks, or by direct keying at a terminal or computer console. It is the simplest and usually the safest method of perpetrating a fraud in a computer. All of the data input validation controls in the computer must be known and subverted.

Superzapping. This is the unauthorized use of utility computer programs to modify, destroy, disclose, or use data or computer programs in a computer system. Utility computer programs are for general use. Computers that contain access controls require a means of gaining access that successfully violates all safeguards in case of control and authorization failure. In most IBM computer installations a utility program called "Superzap" is used for this purpose and is the source of the criminal method term.

Impersonation. Taking and using the identity of an authorized computer user to use the computer in his stead is called impersonation. Computer systems usually have authorized user identification data files that are employed automatically to verify the identity and access authorization of computer users. If an individual can obtain the necessary identification of another person he can impersonate that person to the computer.

Piggybacking. Piggybacking is the unauthorized interdiction of a communication circuit to covertly replace an authorized user. This could be done by electrically inserting a computer terminal on the same communication circuit to a computer as an authorized terminal and interacting with the computer when the authorized user is

momentarily not using his activated terminal. This is another form of impersonation.

Wire tapping. This is the commonly understood method of covertly tapping into a communication circuit, but the circuit carries digitized data instead of voice data.

Trojan horse. As its name implies, this is a method of covertly inserting computer instructions into a computer program that is authorized for use in a computer. The secretly altered program will perform properly but the inserted instructions are also executed to perform an unauthorized act in conjunction with the correct functions of the program. A few instructions can be hidden in a typical computer program with 10,000 or 200,000 instructions in ways that defy detection (Parker, 1976).

Asyncronous attack. This is a method of compromising a computer system by taking advantage of weaknesses in its asyncronous functions. A computer system asyncronously processes tasks to be performed by queuing them up and performing them out of sequence as sufficient resources become available. It is sometimes possible to change some of the conditions after the system starts, taking action based on those conditions. Further description of this method would require an understanding of computer technology beyond the scope of this material.

Trap door. A trap door is a weakness or error introduced into or left in a computer program that can be exploited at a later time to compromise a computer system. Occasionally, a computer programmer will inadvertently weaken a program while developing, maintaining, or changing it. The programmer may also place functions in the program that are not needed for its ultimate purposes but aid in testing or maintenance. These weaknesses, functions, or errors that have been introduced may be used later by persons intent on unauthorized acts.

Salami methods. Salami methods are based on transferring small amounts of assets (slices of salami) from a large number of accounts into a favored account which then can be converted to a fraudulent gain. The possibility of discovery is minimized, because no single victim or account custodian has lost enough to notice or complain about it. It may also be successful because assets are not removed from the system of accounts but only transferred within the system; therefore, the total sum of assets is not changed. The classical salami is the "round down" fraud, in which fractions of pennies remaining from interest calculations for savings accounts are collected in one account rather than being distributed among all accounts. The salami methods require placing changes or additional instructions into the computer program that performs the processing of accounts (Trojan

horse method) or developing a program that can be run in a computer with access to a large file of accounts (Parker, 1976).

Logic bomb. A logic bomb is a computer program or part of a program that is automatically repeatedly executed to test the state and contents of a computer system. When all prescribed conditions are met, the program triggers an unauthorized act in the computer system. A logic bomb could examine the day of year and time of day clock in a computer (a time bomb) to select an optimum time for a fraud to take place providing the greatest safety to the perpetrator (Parker, 1976).

Data leakage. A method for covertly obtaining data from a computer system by leaking it out in small amounts is called data leakage. This might be done by coding the data in a computer in the form of different lengths of printed lines on the output printer. The resulting printed output listing would contain innocuous information, but the length of each printed line could represent a letter of the alphabet or digit. Many other methods could be devised.

Simulation. Simulation of processes or systems is a common computer application that can be used to simulate a fraud for planning purposes or as an aid in regulating, monitoring, or accounting in the perpetration of an ongoing complex fraud. Any one or combination of these technical methods represent only one part of a crime. Other actions could include studying the computer system and application, computer programming, entering the computer system, neutralizing or avoiding controls, suppressing evidence, and converting results of acts to removable gain.

6.1 Computerfraude

Fraude is een algemeen begrip. Iemand die fraude pleegt brengt een ander financieel nadeel toe (zie over fraude-omschrijving in Nederland: A.B. Frielink in "Fraude, automatisering en accountant", Amsterdam, april 1981). Meestal wordt computerfraude omschreven als vermogensdelict, waarbij geautomatiseerde gegevensverwerking sine qua non is.

In de financiële sfeer zijn het accountants die de controlefunctie uitoefenen en veelal als eerste met fraude en computerfraude in aanraking komen. Daarbij staat vast dat banken en verzekeringsmaatschappijen fraudegevoeliger organisaties zijn dan de meeste andere ondernemingen.

Een van de problemen ten aanzien van computerfraude is de ongelukkige situatie dat in de strafwetgeving van verschillende landen in de delictsomschrijving van fraude staat opgenomen dat het slachtoffer wordt bedrogen. Wanneer louter de computer wordt "bedrogen" zou dus niet kunnen worden vervolgd.
Toch zijn er mogelijkheden op grond van andere strafbepalingen, hetgeen onder andere blijkt uit de zaak Slavenburg II.

Veel aandacht wordt vervolgens besteed aan strafrechtelijke aspecten van het geautomatiseerde betalingsverkeer: "electronic funds transfer" (EFT). De verwachting is dat problemen in deze richting zullen toenemen door het gebruik op grote schaal van geld- en betaalautomaten.

6.2 Inbreken in computersystemen

In een databank met gegevens over tropische ziekten zijn de volgende gegevens opgenomen: naam, symptomen en behandelingswijze(n). Na inbraak in deze medische databank zocht de Amerikaanse universiteit, die de gegevensbank heeft opgebouwd en beheerd, contact met de hackers die het systeem zonder toestemming waren binnengekomen. Naar eigen zeggen hadden de hackers alleen wat rondgekeken. De gegevens zouden niet veranderd of vernietigd zijn. Het universiteitsbestuur vond desalniettemin het risico dat veranderingen waren aangebracht te groot. De medische gegevens werden opnieuw ingebracht.

De voorbeelden zijn talloos. Over "hacking" is veel te doen.
Verdeeldheid blijkt troef over deze bijwerking van de automatisering van de gegevensverwerking. Sommigen plaatsen hackers in de sfeer van een moderne Robin Hood, terwijl anderen hun handelen ten sterkste afkeuren.

Vermeldenswaard is het Noorse wetsvoorstel dat het inbreken in computersystemen strafrechtelijk aanpakt, op de wijze van schending van het briefgeheim.

"Bulletin boards" (elektronische prikborden in computersystemen, onder meer via telefoonlijnen te raadplegen) zijn in de Verenigde Staten onderwerp van wetsvoorstellen.
Zware verantwoordelijkheden zouden moeten worden gelegd op de schouders van systeembeheerders van deze prikborden om het bestand "schoon" te houden. Mededelingen over telefoonnummers, toegangswoorden en -cijfers van computersystemen zijn uit den boze.

6.3 Software-piraterij

Juridische bescherming van computerprogrammatuur blijft in veel landen de aandacht van betrokkenen vasthouden. De eerste generatie rechterlijke uitspraken die betrekking hadden op de vraag of een computerprogramma (in bron- of objectcode; als software of firmware) op grond van het (reeds bestaande) auteursrecht kan worden beschermd laat zien dat dit veelal mogelijk is.

Vervolgens kwam in de tweede generatie software-beschermingszaken de vraag aan de orde wat dan de omvang van deze intellectueelrechtelijke bescherming is. Deze procedures doen zich nog steeds voor. Auteursrecht kan volgens de Amerikaanse rechter ook op microcodering worden toegepast, terwijl daarnaast - eveneens in de Verenigde Staten - discussies zijn losgebarsten over geestelijk eigendom op de "look and feel" van een programma.

Enerzijds wordt aangenomen dat software-piraterij groeit en bloeit dankzij het feit dat er geen sluitende (internationale) wetgeving bestaat en dat de programmatuur zelf technisch onvoldoende tegen onrechtmatige handelingen kan worden afgeschermd.

Anderzijds kan men het "Borland"-verschijnsel signaleren: standaardprogrammatuur ("package software") voor microcomputers wordt voor een lage prijs en zonder enige vorm van technische antikopieerbeveiliging op de markt gebracht. Overigens gaan steeds meer (Amerikaanse) software-leveranciers hun produkten (ook "dure" software) zonder beveiliging aanbieden. Technisch beveiligen betekent meer investeren, terwijl de techniek gebruikers op den duur - en soms zelf op zeer korte termijn - niet tegenhoudt de beveiligde programmatuur te "kraken". Daarbij komt dat bij beveiligde software zich problemen kunnen voordoen met het maken van een "back-up copy", indien het standaardpakket reeds op een harde schijf is gezet.

Wat heeft juridische normering voor zin als de techniek schending van rechtsnormen eenvoudig maakt, sterker nog stimuleert en deze handelswijzen in grote delen van de samenleving aanvaardbaar worden geacht. Hierbij kan bijvoorbeeld worden gedacht aan het kopieerapparaat, de audiorecorder, de videorecorder en de computer.

Ook probeert de software-industrie illegale verveelvoudiging en gebruik bij grootgebruikers tegen te gaan door "site license agreements" af te sluiten, waarbij voor een (onderhandelbaar) bedrag een ongelimiteerd aantal kopieën in eigen huis kunnen worden gemaakt en worden gebruikt. Wel is het zo dat netwerken roet in het eten kunnen gooien. De "site" kan in theorie wereldwijd zijn.

Voor wat betreft de chips - om precies te zijn topographieën van halfgeleider produkten - hebben de Verenigde Staten het voortouw genomen en een nieuwe vorm van intellectuele eigendom gecreëerd: de "Semiconductor Chip Protection Act 1984". Westerse landen zijn geneigd, mede onder druk van de gevolgen de Amerikaanse wetgeving (slaafs) na te bootsen.

6.4 Privacy-inbreuken

De eerste generatie privacy-wetten zijn vrijwel allemaal vervangen door de volgende generatie. Nederland neemt in dit kader een uitzonderingspositie in. Vrijwel iedere wet die betrekking heeft op de bescherming van de persoonlijke levenssfeer bevat tevens strafbepalingen.

Wel gaan verschillende stemmen op voor het tot stand brengen van wettelijke bescherming van privacy voor rechtspersonen. Een van deze stemmen betreft de Internationale Kamer van Koophandel (ICC).

Is het niet voldoen aan voorschriften die in privacy-wetten zijn opgenomen een vorm van computermisbruik?

Een voorbeeld: De huidige Engelse privacy-wetgeving, de "Data Protection Act of 1984", verplicht organisaties maar ook individuen die persoonsgegevens hebben opgeslagen zich te laten registreren. Veelal voldoet men hier niet aan en nu de inschrijvingstermijn voor bestaande persoonsregistraties is verstreken, heeft de Data Registrar Eric Howe laten weten tot vervolging over te zullen gaan.

6.5 Computerchantage

Een van de eerste keren dat computer-related crime in de Nederlandse pers aandacht kreeg betrof de XYZ-zaak (1972). De verleiding is blijkbaar te groot geweest voor het hoofd van de Automatiseringsafdeling. De man verduisterde (alle) honderden magnetische tapes en zo'n 50 magnetische schijven en bood deze de directie voor 1.25 miljoen gulden aan. Door internationale samenwerking werd de dader twee dagen na het plegen van de strafbare feiten aangehouden en ook het verduisterde goed werd teruggevonden. De kwetsbaarheid van een onderneming door automatisering van de gegevensverwerking stond onomstreden vast.

Recentelijk speelt in België een soortgelijke zaak. Ditmaal werden cruciale onderdelen van een computersysteem gestolen.

Aangenomen wordt dat het meer dan eens gebeurt dat een werknemer technische en/of administratieve know-how verduistert, nadat hij deze al dan niet heeft gekopieerd. Indien de werkgever niet bereid is het materiaal terug te kopen (chantage), wordt het veelal aan de concurrent aangeboden (bedrijfsspionage).

6.6 Tempest

Met het afluisteren van informatie is vergelijkbaar het verschijnsel "tempest". Computers zenden, wanneer zij zijn ingeschakeld, continu radiogolven uit, die met behulp van een ontvangeenheid binnen een straal van 150 meter kunnen worden opgevangen en gedecodeerd. Anti-tempest computerruimtes en tempest proof computers zijn hiervoor oplossingen.

6.7 Telecommunicatiemisbruik

Het Noorse voorstel dat het inbreken in computersystemen strafrechtelijk aanpakt, overeenkomstig de schending van het briefgeheim, sluit aan bij bestaande rechtsnormen. Teksten opgenomen in een krant zijn voor iedereen toegankelijk. Wordt een artikel uitgeknipt en per brief verstuurd, dan is de inhoud van de brief - het artikel - beschermd. Met andere woorden, ongeacht de (gegevens)inhoud van de brief hebben de meeste formele wetgevers het briefgeheim, veelal als (klassiek) grondrecht, erkend en schending ervan strafbaar gesteld. Hetzelfde kan worden genoteerd ten aanzien van het telefoon- en telegraafgeheim. Langs deze weg kan een "datageheim" juridisch worden geconstrueerd.

De passieve kant van telecommunicatiemisbruik - het "afluisteren" in welke vorm dan ook - is meestal wel duidelijk. Op gevolgen van actieve misbruik van communicatiemedia wordt minder de aandacht gericht.

Neem nu het zonder vergunning uitzenden op frequenties geschikt voor radiogolven. Dit zenden is meestal strafbaar gesteld, maar het merendeel van de samenleving blijkt zich niet druk te maken, terwijl gerichte opsporingsactiviteiten om verschillende redenen spaak lopen. Het "wegdrukken" van legale zenders door illegale zenders is vrijwel geaccepteerd, echter wanneer een "piraat" een krantenpagina vervangt door eigen tekst, is het meer dan waarschijnlijk dat over aantasting van de democratie wordt gesproken. (Ether-)piraterij kan in relatie tot gedigitaliseerde netwerken en geautomatiseerde databanken extreme gevolgen voor de samenleving hebben.

6.8 Computervirus

Volgens sommige Amerikanen zou in het bijzonder voor "sophisticated European terrorists" het tot leven brengen van computervirussen een volgende stap zijn. Bij het virus gaat het om een programma dat voornamelijk in een financieel of militair computersysteem wordt gebracht "that would come alive at a given date and time and jump around through the system, destroying it", aldus Robert Kupperman (Computer Crime Digest, augustus 1986).

6.9 Dood door schuld in verband met automatisering

Het begrip "computerfouten" is niet eenduidig. Het betreft het niet of slecht functioneren van geautomatiseerde gegevensverwerkende systemen. Dit impliceert "Malfunction" van apparatuur, programmatuur, (tele)communicatie-faciliteiten, ongeacht de oorzaak. Niet functioneren betekent het "down gaan" van de computer, terwijl slecht werkende systemen bijvoorbeeld voor een onjuiste gegevensverwerking zorgen. In de Nederlandse rechtspraak komt men het begrip voornamelijk tegen in relatie tot onjuiste uitbetalingen van loon of pensioen.

In ruime zin zijn computerfouten een handelen of nalaten, dat dood of lichamelijk letsel tot gevolg kan hebben, waarbij het in casu gaat om strafrechtelijke aansprakelijkheid voor ernstige, vermijdbare verwijtbaarheid in relatie tot geautomatiseerde gegevensverwerking.

Bekend is ook dat met betrekking tot Challenger-ramp ten minste drie boordcomputers de lekkende brandstoftank zouden hebben moeten constateren, terwijl naar redelijke waarschijnlijkheid het tot tweemaal toe uit de koers raken van het neergeschoten Zuidkoreaanse verkeersvliegtuig aan een onjuiste programmering van de twee navigatiecomputers te wijten is.

In de zaak James A. Cummings Inc. versus Lotus Development Corp. (Verenigde Staten) werd de software-producent (civielrechtelijk) aansprakelijk gesteld voor schade, die volgens eiser is ontstaan door bugs in het rekenprogramma Symphony. Wat nu als de resultaten van het rekenwerk niet werden gebruikt voor het opstellen van een offerte, maar bij de bouw van een brug of stuwdam?

Ook worden instortende bouwkundige werken in een andere context illustratief in de literatuur gebruikt, namelijk om aan te geven dat juridische aansprakelijkheid - echter voornamelijk civielrechtelijk - kan ontstaan door het nalaten om geautomatiseerde gegevensverwerking toe te passen. Een enkeling wijst op een mogelijke strafrechtelijke aansprakelijkheid voor gedragingen die dood of zwaar lichamelijk letsel tot gevolg hebben.

6.10 Misbruikhandelingen in computerfaillissementen

Het gebeurt dat ondernemers hun zaak laten failleren, nadat de ontwikkelde programmatuur, in het bijzonder source code-versie, listings en documentatie aan het faillissement worden onttrokken.
Voor openbare aanklagers is het vrijwel onmogelijk om te bewijzen dat de programmatuur is verveelvoudigd. Hetzelfde geldt voor de curator. Dit materiaal vormt dan het bedrijfskapitaal voor een nieuw op te richten besloten vennootschap. Om eventuele herkenbaarheid van de aan het faillissement onttrokken software te bemoeilijken, worden kleine veranderingen in de sources aangebracht.

in de gang of in de werking van zodanig werk veroorzaakt of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft, ...". Naast strafbare feiten waar opzet voorwaarde is, pleit de Commissie Franken ook voor opname van schulddelicten. Sabotage van computersystemen moet worden bestraft als daardoor schade aan het functioneren van de openbare infrastructuur wordt toegebracht, en/of gevaar voor goederen of levering van diensten te duchten is, en/of levensgevaar voor anderen te duchten is.

In het kader van het onbevoegd inbreken in systemen ("hacking", of volgens de commissie "computervredebreuk") heeft men gekozen voor beveiliging als voorwaarde voor strafbaarstelling:

> "Hij die wederrechtelijk binnendringt in een daartegen beveiligd geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een daartegen beveiligd deel daarvan, wordt gestraft met een gevangenisstraf van ten hoogste zes maanden of een geldboete van de derde categorie."

Centraal in deze strafbepaling staat het "binnendringen" in een computersysteem. Volgens de Commissie Franken moet daaraan de volgende wettelijke omschrijving worden gegeven: "Hij die zich de toegang heeft verschaft door middel van het aannemen van een valse hoedanigheid, listige kunstgrepen of een valse sleutel, wordt geacht te zijn binnengedrongen."
Door strafbaarstelling, onder de nodige beperkingen, van computervredebreuk worden volgens het rapport gegevens in gegevensverwerkende systemen op een indirecte wijze beschermd.

In al haar wetsvoorstellen heeft de Commissie Franken het woord "informatie" vermeden. In de letterlijke tekst treft men "gegevens" aan, bijvoorbeeld "telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk" en "een geautomatiseerd werk voor de opslag of verwerking van gegevens".

De staatscommissie komt tot het uiteindelijke resultaat na het uitvoeren van een scala aan onderzoeksactiviteiten. Haar werkwijze bevatte naast literatuurstudies open oproepen en werkbezoeken. Ook werden deskundigen gehoord, gebruikers enquêteerd en onderzoeken uitbesteed, onder andere naar de stand van computerbeveiliging in Nederland. Deze opdracht werd uitgevoerd door KMG Klynveld Kraayenhof & Co. accountants. Zo'n 851 organisaties (overheid en grote, middelgrote en kleine ondernemingen) werden naar de beveiliging van hun geautomatiseerde gegevensverwerking gevraagd. Van de geënquêteerden hebben 163 voor de sluitingsdatum een bruikbare vragenlijst ingeleverd (19%). Op basis hiervan blijkt dat het slecht is gesteld met de beveiliging van onze geautomatiseerde systemen. De meest verregaande beveiligingsmaatregelen treft men aan bij de grootschalige organisaties.

De rapportage van de Commissie Franken draagt vooral een technisch-juridisch karakter. Er worden er geen uitspraken gedaan over de politieke kant van zaken, zoals de mate van handhaafbaarheid van de voorgestelde veranderingen in het strafrecht. De minister van justitie gaat het rapport nu bestuderen.

2. Basisconcept

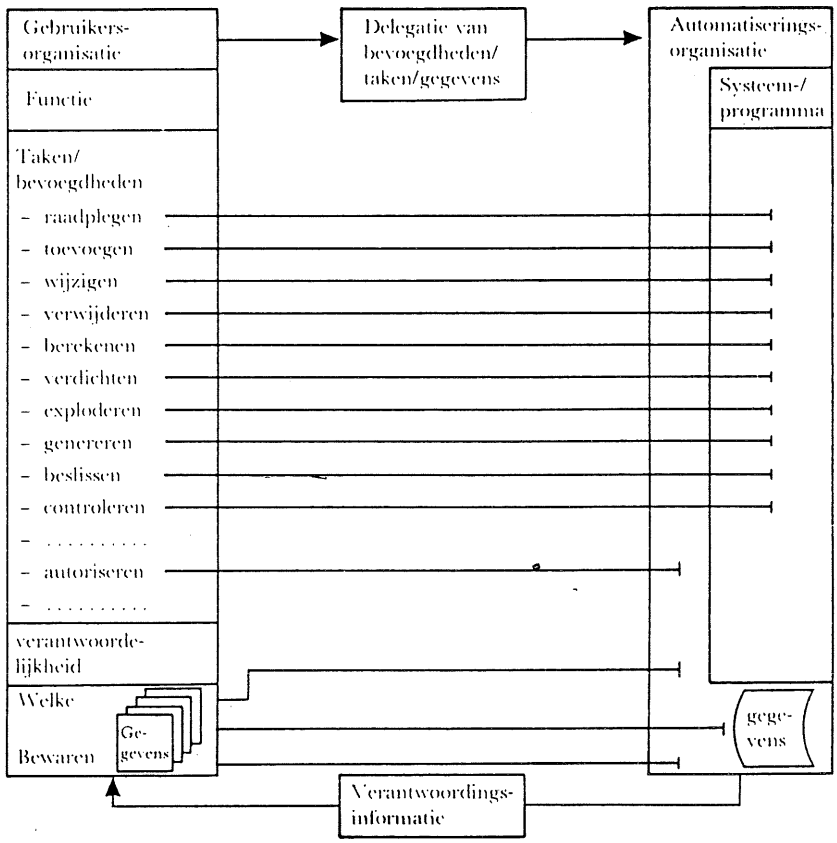
Bij de introductie van automatisering in een organisatie voltrekt zich het volgende proces. De taken van de diverse bedrijfsfuncties worden vertaald naar systemen c.q. programmatuur en ondergebracht bij de automatiseringsfunctie.
Bovendien verhuizen de bij die activiteiten behorende gegevens(verzamelingen) eveneens naar die functie. Deze (gedelegeerde) uitvoering van taken alsmede de bewaring van gegevens geschiedt dan door die automatiseringsfunctie. Dit is derhalve geen "nieuwe" functie maar een uit doelmatigheids- c.q. betrouwbaarheidsoogpunt verbijzonderde functie samengesteld uit reeds bestaande taken met een eigen verantwoordelijkheid al dan niet ondergebracht in een aparte afdeling (automatiseringsorganisatie).

De gebruiker heeft taken gedelegeerd maar blijft uiteindelijk (inhoudelijk) verantwoordelijk voor het gedelegeerde. De primair verantwoordelijke zal derhalve verantwoordingsinformatie dienen te ontvangen om vast te kunnen stellen dat het gedelegeerde volgens gestelde randvoorwaarden is c.q. wordt uitgevoerd.
In controletermen geredeneerd, de primair verantwoordelijke gebruiker moet verantwoordingsinformatie krijgen van de automatiseringsfunctie om vast te kunnen stellen dat:

- de ter verwerking aangeboden mutaties volledig en juist zijn verwerkt (met de juiste programmatuur en de daarbij behorende gegevensverzamelingen);
- de gegevensverzamelingen volledig en juist zijn gebleven (en niet ongeautoriseerd zijn gewijzigd);
- de bewaring van programmatuur en bestanden aan de gestelde eisen voldoet;
- alleen door de gebruikersfunctie aangeboden gegevens/mutaties worden verwerkt.

Dit gehele proces zal zodanig moeten worden opgezet dat de functiescheiding in de gebruikersorganisatie naar de automatisering toe wordt vertaald (en blijft gehandhaafd) en de verwerking alsmede bewaring op eenzelfde betrouwbaarheidsniveau plaatsvinden als zonder automatisering het geval geweest zou zijn.
Het beschreven verschuivingsproces is schematisch weergegeven in figuur 1.

Figuur 1: Ontstaan automatiseringsfunctie



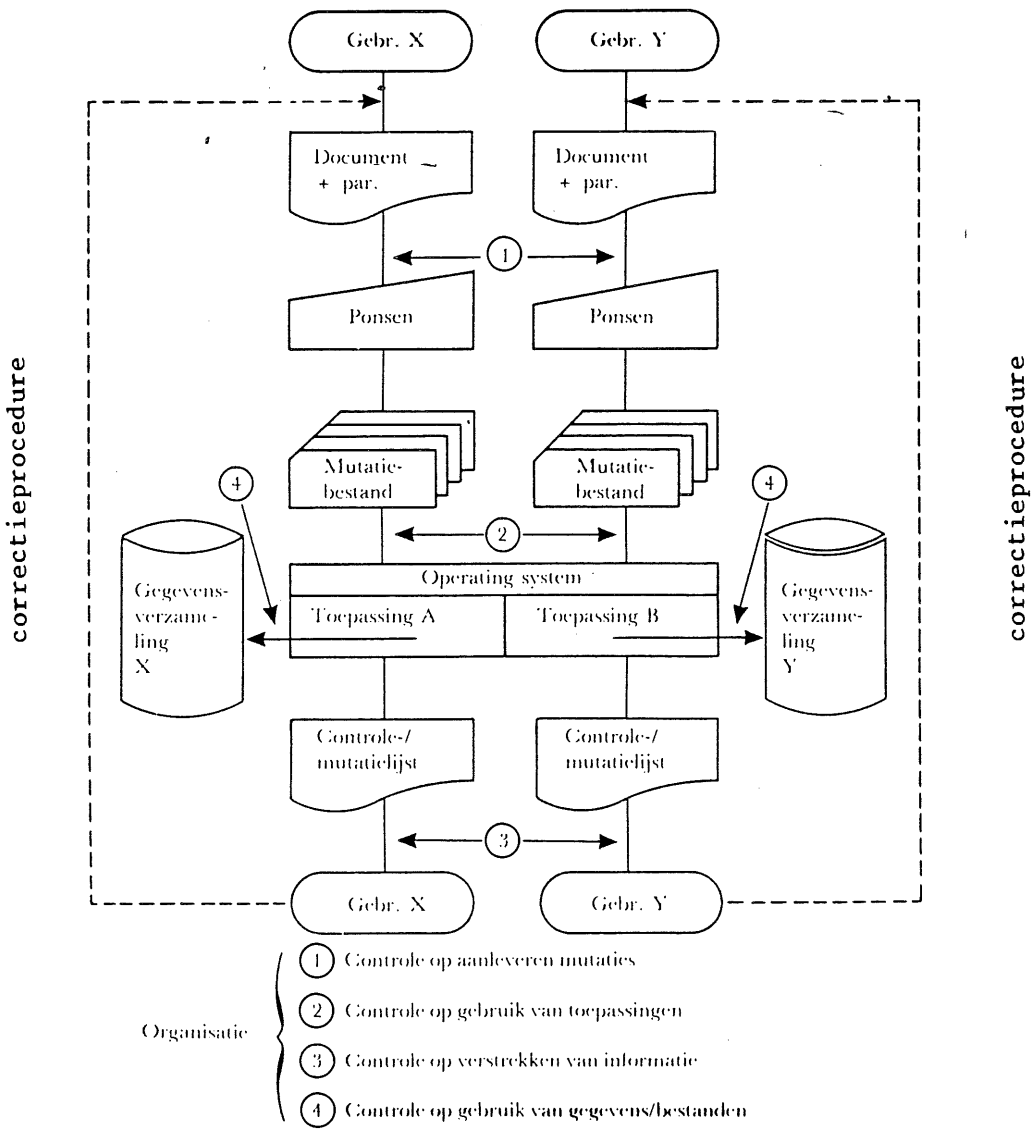
Onder de gebruikersorganisatie is een - niet limitatieve - opsomming van taken opgenomen waaruit een functie kan bestaan. Deze taken kunnen worden geautomatiseerd. Het weergegeven proces geeft te zien dat die taken kunnen verschuiven naar systemen/programmatuur en/of de automatiseringsorganisatie. Hoewel algemeen van karakter, blijkt uit nadere bestudering dat dit schema het proces van batch-verwerking weergeeft. Dit batch-proces wordt tot uitdrukking gebracht door de "taak" autoriseren (nog) niet te laten verschuiven naar de toepassingsprogrammatuur maar wel naar de automatiseringsorganisatie. Met dit "autoriseren" wordt bedoeld wie (welke gebruiker) mag wat met welke gegevens doen.

Bij batch-verwerking is derhalve wel sprake van verschuiving maar waarbij de volgende (controle)taken nog zijn gedelegeerd aan de automatiserings-organisatie:

- controle op aanbieding van door gebruikers ter verwerking aangeboden gegevens/mutaties (input);
- controle op het gebruik van de programmatuur;
- controle op de afgifte van verwerkte gegevens/mutaties (output);
- controle op het gebruik van gegevens (bestanden);
- controle op bewaring van gegevens en programmatuur.

Dit proces is schematisch weergegeven in figuur 2.

Figuur 2: Organisatorische controles bij batch-verwerking



Integratie-aspecten

De integratie-aspecten, als gevolg van het verschuivingsproces, kunnen zich zowel in de gebruikers- als de automatiseringsorganisatie manifesteren. De invloed van de automatisering op de gebruikersorganisatie kan tweeledig zijn.

Enerzijds kan de verschuiving van taken zodanig ver gaan dat gebruikersfuncties worden "uitgehold" (in de meest vergaande vorm blijft alleen de "verantwoordelijkheid" over). Uit doelmatigheidsoverwegingen kan dan samenvoeging (integratie) van functies plaatsvinden. Het gevolg hiervan kan weer zijn dat de controletechnische functiescheidingen in de gebruikersorganisatie worden bedreigd c.q. teniet gaan. Dit probleem zal zich eerder voordoen in een organisatie van beperkte omvang.

Anderzijds bestaat de mogelijkheid dat voorheen zichtbare controlepunten verdwijnen door het/de:
- samenvoegen van voorheen gescheiden stromen (procedures etc.);
- wegvallen van tussenverzamelingen (registraties);
- integratie van functies in de gebruikersorganisatie;
- delegeren van taken en gegevens aan de automatiseringsorganisatie.

Het delegatie- en verantwoordingspatroon dient derhalve aan de gewijzigde situatie te worden aangepast.

Resource sharing

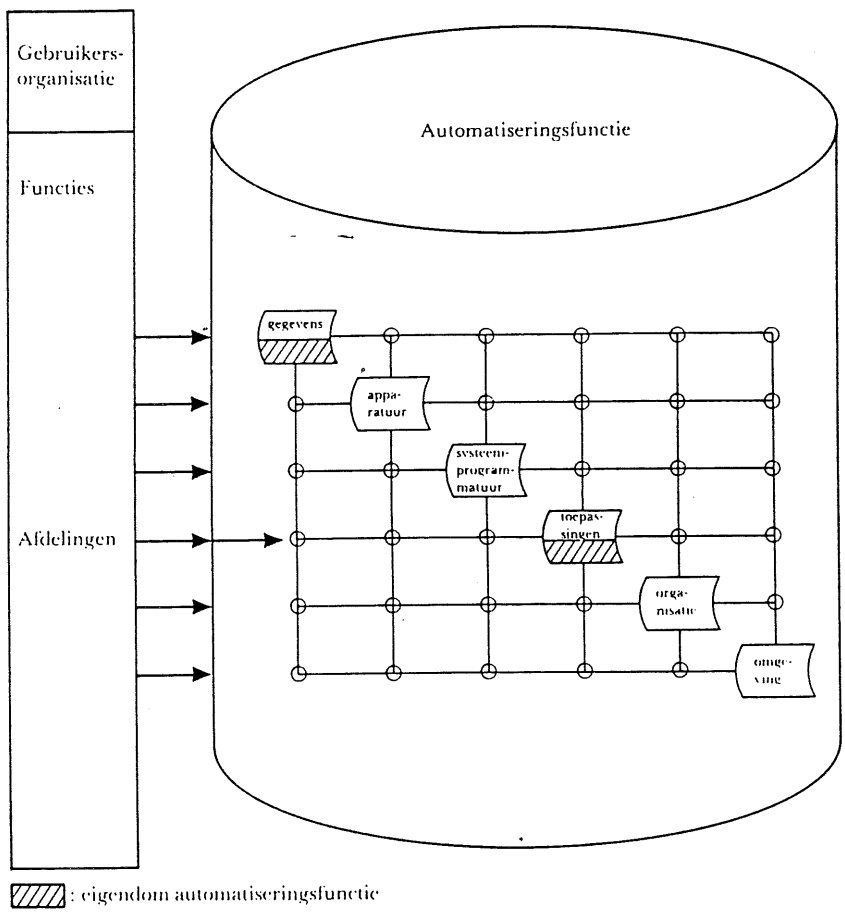
Uit het beschreven proces komt naar voren dat de gebruikersorganisatie gemeenschappelijk gebruik maakt van de componenten (resources) waaruit de automatiseringsfunctie is opgebouwd. Dit kan "resource sharing" worden genoemd. Gemeenschappelijk wordt gebruik gemaakt van de:
- apparatuur en informatiedragers;
- besturingsprogrammatuur;
- organisatie (mensen, functies, procedures en voorschriften);
- omgeving (fysieke locatie: gebouwen/terreinen/technische installaties).

Het gebruik van gegevens (data sharing) en toepassingsprogrammatuur (program sharing) vindt nog niet gemeenschappelijk plaats. Zowel de gebruikers als de automatiseringsfunctie beschikken (nog) over hun eigen gegevens en programmatuur die echter van dezelfde resources gebruik maken. In een dergelijke situatie gaat het erom dat de controletechnische functiescheidingen zowel in de gebruikersorganisatie als in de "automatisering" niet worden aangetast door de "resource sharing". De betrouwbaarheid van de verantwoor-

dingsinformatie is in belangrijke mate afhankelijk van de wijze waarop de componenten van de automatiseringsfunctie zijn georganiseerd.

In figuur 3 is resource sharing schematisch weergegeven.

Figuur 3: Resource sharing



Op basis van het voorgaande is de uitspraak gerechtvaardigd dat in geval van automatisering altijd sprake is van geïntegreerde verwerking. De invloed op de interne controle kan wisselen per situatie. De invloed van resource sharing is voor de gebruiker in geval van zuivere batch-verwerking van beperkte omvang. In geval van het verstrekken van bestands(tellingen) en/of verwerkingsinformatie (mutatie-overzichten) heeft de gebruiker de mogelijkheid zelfstandig vast te stellen of naar programmatuur gedelegeerde taken juist zijn uitgevoerd (en/of functiescheiding in de gebruikersorganisatie niet is doorbroken).

De juiste en volledige uitvoering van gedelegeerde controletaken gericht op het autorisatie-aspect zijn eveneens zelfstandig door de gebruiker vast te stellen. Blijft over de verantwoording over de gedelegeerde bewaring van gegevens (die nogal eens ontbreekt). Hierover zou de gebruiker eveneens periodiek moeten worden geïnformeerd om vast te kunnen stellen of blijvend aan zijn bewaringsnormen wordt voldaan.

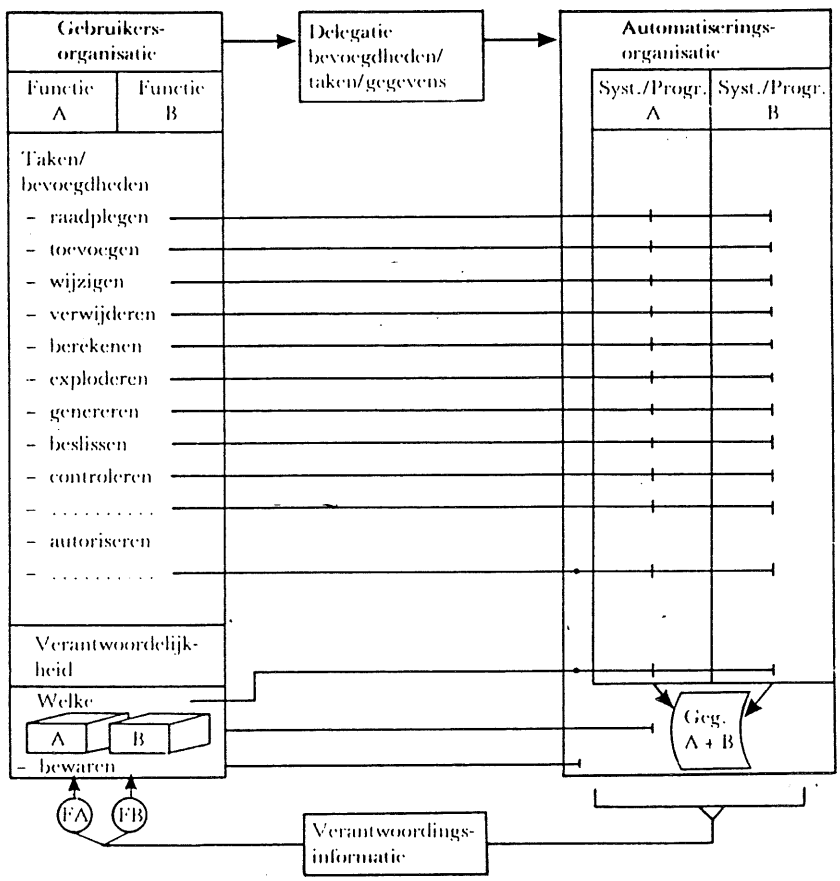
3. Gemeenschappelijk gegevensgebruik (data sharing)

De automatisering staat echter niet stil. De technische mogelijkheden alsmede de ontwikkelingen op het gebied van (besturings)programmatuur maken het mogelijk de voorheen per functie gescheiden gegevensverzamelingen samen te voegen en gemeenschappelijk te gebruiken. Dit wordt "data sharing" genoemd. Eenmalige gegevensvastlegging krijgt de overhand (elimineren van redundantie) waardoor enerzijds de consistentie (betrouwbaarheidsaspect) wordt verhoogd maar anderzijds het risico van verlies van gegevens groter wordt tenzij aanvullende maatregelen (back-up, recovery en restart) zijn getroffen.

Het uit oogpunt van interne controle voornaamste gevolg van deze ontwikkeling (data sharing) is dat extra voorzieningen moeten worden getroffen om te bewerkstelligen dat de functiescheiding in de gebruikersorganisatie niet door de "automatisering" wordt doorbroken. Uitgaande van de vraag "wie wat met welke gegevens" mag doen krijgt nu welke een extra dimensie. In het toepassingsprogramma zal nu geregeld moeten worden met welke gegevens het programma mag werken. Een geïntegreerd bestand wordt immers voor de verwerking beschikbaar gesteld waarvan het programma slechts een gedeelte mag gebruiken, namelijk dat gedeelte dat bij een bepaalde gebruikersfunctie behoort.

Uit het voorgaande blijkt dat ook hier van verschuiving sprake is.
Een voorheen zichtbare organisatorische controle wordt overgenomen door de automatisering. Het gaat hier om een controle die eerst is verschoven van de gebruikers- naar de automatiseringsorganisatie, en nu verschuift van de automatiseringsorganisatie naar de toepassingsprogrammatuur. Dit verschuivingsproces is weergegeven in figuur 4.

Figuur 4: Data sharing zonder database-management-systeem



Gevolgen data sharing

Data sharing heeft zowel voor de gebruikers- als automatiseringsorganisatie gevolgen. In de gebruikersorganisatie vraagt onder andere het aspect gegevensbeheer meer aandacht.
Onder gegevensbeheer wordt grofweg het volgende verstaan:

1. het zorg dragen voor eenduidige (niet strijdige) gegevensdefinities;
2. het geven van algemene richtlijnen voor het gegevensgebruik (in casu met nadruk op handhaving van controletechnische functiescheiding);
3. het (doen) uitvoeren van controle op naleving van hetgeen onder punt 1. en 2. is opgenomen.

De onder gegevensbeheer vermelde activiteiten werden voorheen in een min of meer geïsoleerde omgeving per organisatorische functie uitgeoefend. Door het samenvoegen en gebruik van functioneel gescheiden registraties vraagt gegevensbeheer uit oogpunt van betrouwbaarheid (tevens uit doelmatigheidsoverwegingen) om verbijzondering. Er vindt verschuiving van taken - en in dit geval tevens van verantwoordelijkheden - plaats van de desbetreffende functies naar de verbijzonderde functie gegevensbeheer. Deze functie is nu verantwoordelijk voor een juist gegevensgebruik (waarbij handhaving van functiescheiding voorop staat).

Gegevensbeheer is, zoals uit het voorgaande blijkt, een verantwoordelijkheid van de gebruiker. In geval van automatisering wordt de uitvoering van de door gegevensbeheer opgestelde richtlijnen gedelegeerd aan de automatiseringsorganisatie. In controletermen vertaald zal de automatiseringsorganisatie zorg dienen te dragen voor een adequate uitvoering van door of namens de gebruikers uitgevaardigde richtlijnen. In een situatie waar nog geen sprake is van data sharing speelt dat hele proces zich af tijdens de systeembouw binnen één (geïsoleerde) functie. In geval van data sharing wordt de zaak complexer. Het wordt moeilijker vast te stellen of de functiescheiding in de gebruikersorganisatie adequaat naar de "automatisering" wordt doorgetrokken. In dat geval kan een verbijzonderde functie worden gecreëerd die database administration (dba)[1]) wordt genoemd.
Deze functie heeft als taak de richtlijnen, gegeven door de data administration functie (da)[2]) op het gebied van controle en beveiliging te realiseren.

Hieruit valt op te maken dat wederom (bij de dba) van verschuiving sprake is, nu geheel binnen de automatiseringsorganisatie. De genoemde taken werden voorheen uitgevoerd door de functies systeemontwikkeling, systeemprogrammering en produktie.

---

1) Database administration functie (dba-functie)
Een functie verantwoordelijk voor het/de:
- ontwerp, definiëren en technisch beheer van de database;
- definiëren van de feitelijke opslagwijze;
- te treffen beveiligingsmaatregelen van de opgeslagen gegevens;
- periodieke reorganisatie van de feitelijk opgeslagen gegevens;
- de uitgifte, volgens richtlijnen verstrekt door de da-functie, van deelbeschrijvingen (subschema).

2) Data administration functie (da-functie)
Een functie die verantwoordelijk is voor het:
- vaststellen en beheren van eenduidige en onderling niet strijdige definities van gegevens van de onderneming;
- geven van algemene richtlijnen inzake het gebruik, de beveiliging en de betrouwbaarheid van gegevens;
- toezien op gebruik en naleving van de richtlijnen.

Terugkerend naar het "wie mag wat met welke gegevens" zal in geval van data sharing het wat met welke gegevens opgenomen moeten worden in de toepassingsprogrammatuur. Indien dit niet juist geschiedt kan dat - zoals eerder gesteld - consequenties hebben voor de functiescheiding in de gebruikersorganisatie. Daarom is het noodzakelijk dat - in casu - bij de ontwikkeling van systemen de testactiviteiten worden uitgebreid. Het testen mag niet beperkt blijven tot het wat maar tevens moet worden getest of de programmatuur slechts met de juiste gegevens kan en zal werken.
Dit geldt eveneens bij het onderhoud van systemen c.q. programmatuur. De aangepaste programmatuur moet niet alleen worden getest op de aanpassingen in het wat maar tevens in het welke.
In geval van data sharing is het derhalve aan te bevelen onderhoud te beschouwen als nieuwbouw en "compleet" te testen om vast te stellen of (nog) aan de gestelde gebruikerseisen wordt voldaan.

Verantwoordingsinformatie

De verantwoordingsinformatie dient zich aan de gewijzigde situatie (structuren) aan te passen. Het verschil met de basissituatie ligt in het feit dat de "autorisatie" is verschoven. Ten aanzien van de betrouwbaarheid (volledigheid en juistheid van de verwerking alsmede volledig en juist blijven van bestanden) zal de gebruiker dat zelfstandig (moeten) kunnen vaststellen door middel van verstrekte informatie. Het autorisatie-aspect wordt hiermee eveneens grotendeels afgedekt. Uit die informatie moet namelijk kunnen worden afgeleid of "ongeautoriseerd" gemuteerd is. Daarenboven heeft de gebruiker bij het testen van nieuwe c.q. gewijzigde systemen/programmatuur de mogelijkheid om zelfstandig vast te stellen of de gedelegeerde autorisatie juist is opgenomen in de programmatuur.
De gebruiker dient verantwoordingsinformatie te ontvangen over het feit of eenmaal geteste, geaccepteerde en overgedragen programmatuur niet ongeautoriseerd wordt c.q. is gewijzigd. Hierbij wordt de gebruiker - zoals de literatuur aangeeft - afhankelijk van de "algemene maatregelen" (general controls) die op dit punt zijn getroffen binnen de automatiseringsorganisatie. Over de toereikendheid van de algemene maatregelen dient de gebruiker rechtstreeks of via een derde (deskundige) informatie te ontvangen of ze in continuïteit hebben gewerkt. De vraag is of deze verantwoordingsinformatie over de algemene maatregelen in de automatiseringsorganisatie voor de gebruiker voldoende is en of dit - uit controle-oogpunt - de zelfstandige vaststelling (door middel van output) kan vervangen.

Met betrekking tot de gedelegeerde bewaarfunctie is er geen verschil ten opzichte van de beschreven basissituatie. Wel zullen vanwege de toenemende eenmalige vastlegging van gegevens aanvullende maatregelen moeten worden

getroffen om het risico van verlies van gegevens te beperken tot een door de gebruiker aangegeven niveau. Over het feit of hieraan blijvend wordt voldaan zal de verantwoordelijke gebruiker eveneens periodiek moeten worden geïnformeerd.

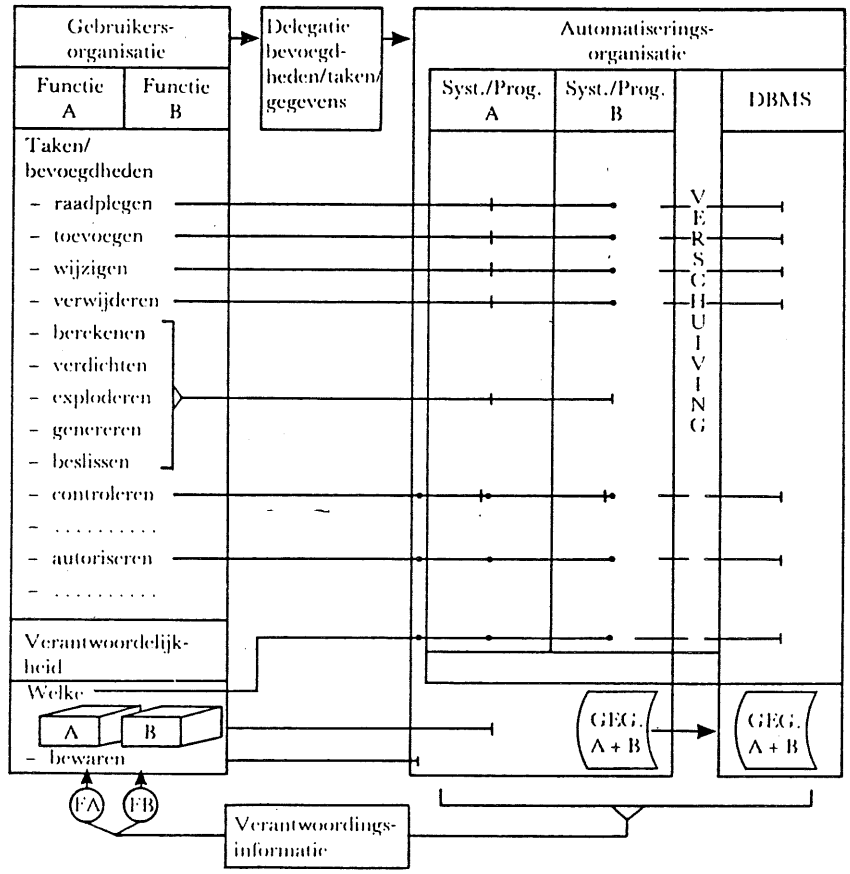
Gezien het feit dat alleen het wat met welke gegevens in de programmatuur is opgenomen, is er nog sprake van een zuivere batch-verwerking. De controle op "wie" geschiedt nog geheel door middel van organisatorische (door de gebruiker direct waarneembare) maatregelen. Uit het voorgaande is de conclusie gerechtvaardigd dat data sharing in een zuivere batch-omgeving nog van beperkte invloed is op de interne controle. De situatie wordt enigszins complexer door de mogelijk toenemende verbijzondering van functies waardoor de delegatie- en verantwoordingsstructuur er anders uit gaat zien. Daartegenover staat dat in batch-programmatuur de te verrichten activiteiten (het wat) nagenoeg vastliggen in een vaste vooraf bepaalde volgorde.
De test-, acceptatie- en overdrachtsprocedures krijgen een extra dimensie door het "welke". Overeind blijft dat de gebruiker, om zijn inhoudelijke verantwoordelijkheid te kunnen blijven dragen, door middel van verantwoordingsinformatie de mogelijkheid moet hebben - zelfstandig of indirect - vast te kunnen stellen of het gedelegeerde volgens afspraak is uitgevoerd.

4. Overkoepelende besturingsprogrammatuur

Nagenoeg gelijktijdig met de introductie van data sharing kwam overkoepelende besturingsprogrammatuur (database management systemen) beschikbaar voor het "gecentraliseerd beheer" van gegevens. Centraal kan met deze programmatuur worden bepaald wat (gedeeltelijk) met welke gegevens mag worden gedaan. Met andere woorden, alle toepassingen onder deze besturingsprogrammatuur uitgevoerd zijn aan de controles onderhevig die in de overkoepelende programmatuur zijn gedefinieerd. Controles c.q. activiteiten die voorheen in toepassingsprogrammatuur waren opgenomen - en per toepassing moesten worden geregeld - verschuiven naar een hoger liggende laag: de besturingsprogrammatuur.

Het effect van het gebruik van overkoepelende programmatuur is weergegeven in figuur 5.

Figuur 5: Data sharing met database management systeem



Gevolgen gebruik dbms[3])

Uit figuur 5 blijkt dat de verschuiving van het wat slechts gedeeltelijk is en zich beperkt tot het raadplegen, toevoegen, wijzigen en verwijderen. Daarnaast kunnen een aantal controles verschuiven. Het welke verschuift geheel naar de besturingsprogrammatuur. Centraal kan worden gedefinieerd en gecontroleerd wat (gedeeltelijk) een programma met een gegeven kan en mag doen.

3) Database management systeem (dbms).
Een geheel van (besturings)programma's nodig voor het gecentraliseerd beheer van een database.

Het definiëren kan geschieden door het uitgeven van deelbeschrijvingen (subschema's) door de database administration functie op grond van richtlijnen van de gegevensbeheerfunctie (data administration). Per deelbeschrijving kan per gegevens(element) worden bepaald welke bewerkingen (raadplegen, toevoegen, wijzigen, verwijderen) mogen worden verricht. Elk programma wordt voor uitvoering gekoppeld aan een deelbeschrijving. De overkoepelende besturingsprogrammatuur controleert nu of dat programma slechts gebruik maakt van de in de deelbeschrijving opgenomen gegevens(elementen) en of de bewerkwijze met die gegevens(elementen) beperkt blijven tot de in de deelbeschrijving gedefinieerde. Indien een dbms in deze te weinig mogelijkheden biedt of als van de (controle)mogelijkheden van een dbms geen of te weinig gebruik wordt gemaakt zal het wat met welke gegevens weer door middel van toepassingsprogrammatuur moeten worden geregeld met alle - controle - consequenties van dien.

Een database management systeem kan, mits juist gebruikt, een positieve invloed hebben op de interne controle. Op centraal niveau (wel binnen de automatiseringsorganisatie) kan onder controle worden gehouden of bij data sharing de functiescheiding in de gebruikersorganisatie wordt gehandhaafd. Daarnaast kan het een positieve bijdrage leveren aan de beheersbaarheid van het onderhoud van systemen.
Het onderhoud wordt zogenaamd gegevensonafhankelijk. Alleen de activiteiten die niet verschoven zijn naar de overkoepelende besturingsprogrammatuur, zoals bijvoorbeeld berekenen, verdichten, etc., zijn aan wijziging onderhevig. Indien bij gepleegd onderhoud activiteiten aan de toepassingsprogrammatuur zijn toegevoegd op en met gegevens(elementen) die de deelbeschrijving niet toestaat c.q. kent, worden deze niet uitgevoerd. Het dbms staat dat niet toe. Immers bij onderhoud ondergaat de deelbeschrijving in principe geen wijziging. Indien dat wel het geval is zullen de richtlijnen voor het gegevensgebruik blijven gelden en zal de dba een aangepaste deelbeschrijving moeten verstrekken.
Dit gaat slechts op als de functievervulling van de database administrator adequaat is. Indien uitgegeven deelbeschrijvingen te ruime mogelijkheden bieden (met andere woorden ze bevatten te veel gegevens en/of er zijn onvoldoende beperkingen in het gebruik ervan aangebracht) is er met betrekking tot de onderhoudsproblematiek geen verschil ten opzichte van de situatie zonder database management systeem.
Het voorgaande stellend tegenover de verwerkingstypologieën (batch; online) is de conclusie gerechtvaardigd, dat bij een zuivere batch-verwerking er in principe geen verschil is of er gewerkt wordt met of zonder een dbms. Immers, een batch-programma bestaat uit een groot aantal in min of meer vaste volgorde liggende acties die alle gebruik maken van één en dezelfde deelbeschrijving.
Deze deelbeschrijving, identiek aan het totale bestand, zal dan weinig uit controle-oogpunt gewenste beperkingen omvatten. Het toepassingsprogramma zal wederom de specificatie van het volledige wat met welke gegevens dienen te bevatten.

On-line-verwerking

Naast het wat en het welke blijft het wie nog over. Ten aanzien van de controle op het wie (controle op aanleveren mutaties, gebruik programmatuur en bestanden, verstrekte output) is de verschuiving weergegeven van de gebruikers- naar automatiseringsorganisatie. De volgende stap is de verschuiving van de automatiseringsorganisatie naar de (besturings)programmatuur. In dat geval spreken we van on-line-verwerking. Op dit verschuivingsproces wordt hierna ingegaan na een korte beschrijving van de drie vormen van on-line-verwerking die in de praktijk wordt aangetroffen.

a. On-line data entry met (uitgestelde) batch-verwerking

Hieronder wordt verstaan dat mutaties via een terminal (al dan niet voorzien van een beeldbuis) worden ingevoerd en opgeslagen in een mutatiebestand. In latere batch-verwerking (meestal 's avonds) worden de mutaties pas verwerkt in het stambestand. Tijdens de invoerfase is de achterliggende programmatuur meestal zodanig van geprogrammeerde controles voorzien, dat schone invoer voor de latere batch-verwerking wordt verkregen. Foutlijsten, en derhalve uitgebreide correctieprocedures, verdwijnen hierdoor. Voor het overige biedt deze werkwijze identieke controlemogelijkheden als bij batch-verwerking (bestandstellingen, mutatieverslagen, batch-totalen).

b. On-line pseudo real time

Een verwerkingswijze die suggereert dat ingevoerde mutaties direct in het bestand worden verwerkt. Dit is echter niet het geval. Mutaties worden evenals onder het vorige punt op een mutatiebestand (kladbestand) opgeslagen. Ook hier kan de data entry programmatuur voorzien zijn van controles om schone invoer te bewerkstelligen.
Wordt bijvoorbeeld na het aanbrengen van een mutatie op een voorraadbestand de voorraad van dat gemuteerde artikel opgevraagd, dan is door aanvullende programmatuur bewerkstelligd dat de werkelijke voorraad wordt getoond (inclusief de mutatie).
In de latere batch-verwerking worden de mutaties echt op het bestand aangebracht. Deze manier van verwerken biedt geen wezenlijke verschillen ten opzichte van die onder het vorige punt. Bestandstellingen, mutatieverslagen etc. blijven tot de mogelijkheden behoren.

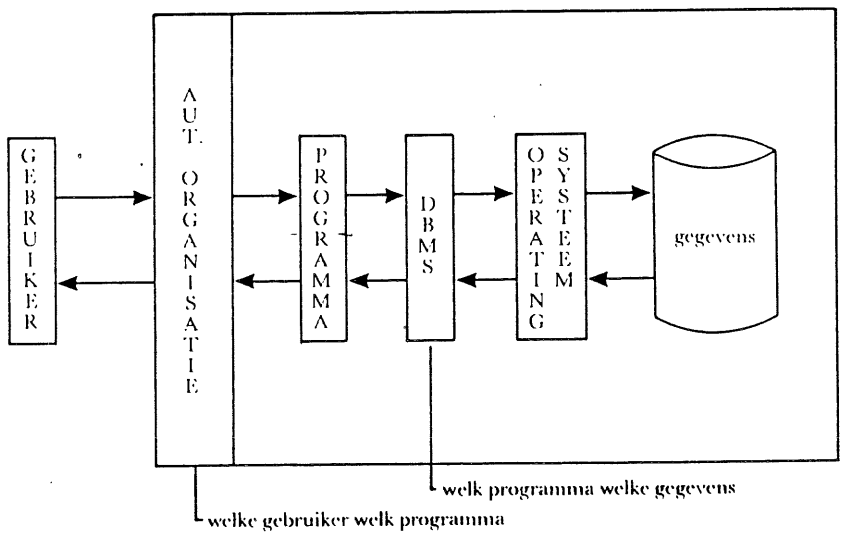
c. On-line real time

Dit is de meest geavanceerde wijze van gegevensverwerking. De mutaties worden rechtstreeks aangebracht op het bestand en zijn direct effectief. Het is eenmalige vastlegging in optima forma.
Vanwege het feit dat een bestand continu postgewijs wordt gemuteerd zal het moeilijker zijn periodieke bestandstellingen en mutatieverslagen te realiseren. Bovendien zullen aanvullende maatregelen (en andere technieken) nodig zijn om te verzekeren dat geen gegevens verloren gaan.

Controle-aspecten on-line-verwerking

On-line-verwerking geeft een aantal uit controle-oogpunt zeer belangrijke verschuivingen te zien. Om dat aan te geven nog even terug naar de basisgedachte dat het gaat om wie wat mag met welke gegevens. De automatisering (batch-verwerking) in ogenschouw nemende loopt het proces (relatie gebruiker-gegevens) als in figuur 6 weergegeven (situatie met database management systeem).

Figuur 6: Relatie gebruiker-gegevens bij batch-verwerking met dbms



De volgorde is derhalve:
- gebruiker;
- programma;
- database management system;
- operating system;
- gegevens.

De controle-activiteiten tussen de gebruiker en de overige componenten worden verricht door de automatiseringsorganisatie.

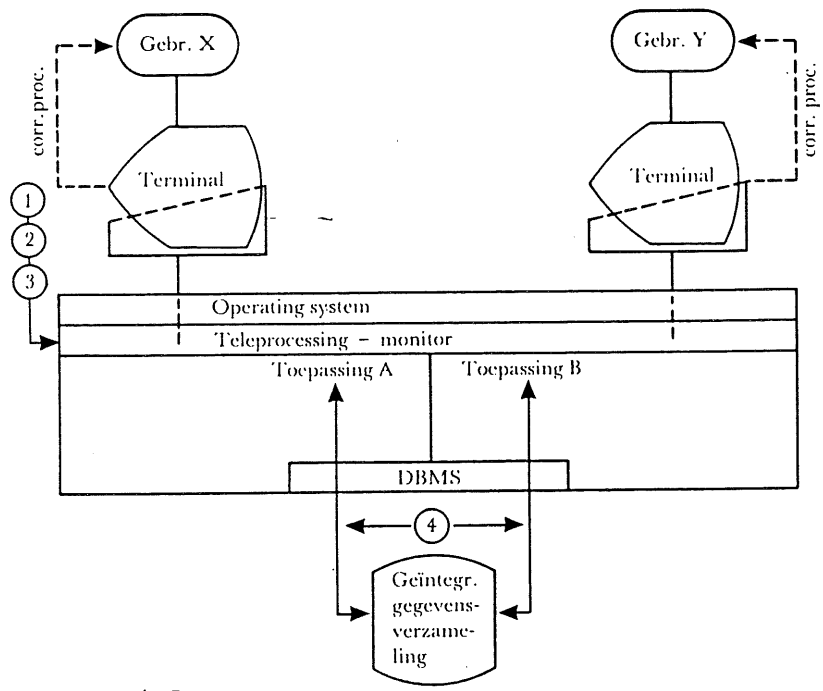
In een on-line-omgeving wordt tussen gebruiker en programma besturingsprogrammatuur gelegd (teleprocessing monitor)[4]) die in feite bepaalt welke gebruiker welke programmatuur mag gebruiken (en daarmee welke gegevens).

4) Teleprocessing monitor (TP-monitor).
Besturingsprogrammatuur die in een on-line gegevensverwerkingssituatie de toegang tot toepassingsprogrammatuur regelt.

Hieruit valt te concluderen dat de volgende controle-activiteiten zijn verschoven van de automatiseringsorganisatie naar de teleprocessing monitor (TP-monitor):
- wie mag welke gegevens ter verwerking aanbieden;
- wie mag welke programmatuur gebruiken (en daarmee bepaalde gegevens benaderen);
- wie mag welke (verwerkte) informatie ontvangen.

Dit is schematisch weergegeven in figuur 7, (situatie met database management systeem).

Figuur 7: On-line-verwerking



Het proces verloopt als volgt. Een gebruiker identificeert zich door middel van een password om toegang te krijgen tot het systeem (authentication). Aan dat password is een identificatie gekoppeld. Slechts door middel van password + identificatie kan de gebruiker toegang tot programmatuur verkrijgen.

De TP-monitor bevat een tabel waarin de te gebruiken programmatuur is opgenomen en elk programma is voorzien van een code. Indien de gebruikerscode overeenstemt met die van een bepaald programma in de tabel is de gebruiker gerechtigd dat programma te gebruiken.

Het vullen, alsmede wijzigen van die programmatabel wordt meestal overgelaten (gedelegeerd) aan de automatiseringsorganisatie. Na het vullen c.q. wijzigen zal de inhoud van de tabel de situatie qua functiescheiding in de gebruikersorganisatie (blijvend) moeten weergeven.
De gebruiker dient derhalve verantwoordingsinformatie te ontvangen of de inhoud van de programmatabel inclusief codes juist is aangebracht en niet ongeautoriseerd kan worden gewijzigd.

Door het verschuiven van voornoemde controles van de automatiseringsorganisatie naar besturingsprogrammatuur verdwijnen ze nog verder uit het gezichtsveld van de gebruiker. Zichtbare controles worden vervangen door onzichtbare waarvan de blijvende goede werking zichtbaar gemaakt moet worden.

Voor die blijvende goede werking is de gebruiker ook hier afhankelijk van het "niveau" van de automatiseringsorganisatie. Over het feit of de algemene maatregelen voldoende zijn en in continuïteit adequaat hebben gefunctioneerd zal de gebruiker direct of indirect verantwoordingsinformatie dienen te ontvangen. Het zal de lezer duidelijk zijn dat in een on-line-omgeving de aandacht niet beperkt moet blijven tot het password-systeem. Het password-systeem heeft slechts beperkte betekenis en is in hoofdzaak een instrument voor de gebruiker om de onder zijn/haar verantwoordelijkheid vallende gebruikersorganisatie te regelen. Een password-systeem moet derhalve niet geïsoleerd doch in samenhang met alle aspecten rondom de TP-monitor worden gezien.

Verantwoordingsinformatie

Als meest vergaande vorm van eenmalige vastlegging is genoemd de on-line real time-verwerking. Naast het feit dat bij on-line real time-verwerking meestal sprake is van data sharing valt tevens waar te nemen dat gestreefd wordt naar optimale redundantieverwijdering. Dit kan zover gaan dat voorheen uit controle-oogpunt gescheiden (opgebouwde) registraties worden samengevoegd waardoor controles moeten worden aangepast of controlemogelijkheden ontbreken.
Het is bij gebruik van steeds geavanceerder technieken voor de gebruiker niet meer eenvoudig of in het geheel niet meer mogelijk vast te stellen of de gedelegeerde taken naar behoren worden uitgevoerd.
Gesteld is dat de gebruiker (als verzamelnaam) inhoudelijk verantwoordelijk is en blijft.
Dit blijft in een on-line real time-omgeving onverkort van kracht, alleen de informatie uit het geautomatiseerde proces ondergaat wijziging waardoor het blijvend kunnen dragen van die verantwoordelijkheid steeds moeilijker wordt. Bijvoorbeeld bestands- en mutatietellingen worden vervangen door de

introductie van een "netwerk van controletotalen" waarbij meestal onvoldoende aandacht is voor het feit:
- dat de controles deel uitmaken van het geautomatiseerde proces;
- dat bij het niet sluiten van het "netwerk" localisering van de fout mogelijk moet zijn.

Het zal de lezer duidelijk zijn dat een netwerk van controletotalen verantwoordingsinformatie dient op te leveren over zowel de volledigheid als juistheid van de mutatieverwerking alsmede het volledig en juist blijven van gegevensverzamelingen. Zoals reeds gesteld is het voor de gebruiker moeilijk op grond van alleen dergelijke informatie dat vast te kunnen stellen. In dit soort situaties wordt er min of meer van uitgegaan dat de algemene maatregelen in de automatiseringsorganisatie voldoende waarborgen bieden dat alleen met door de gebruiker geautoriseerde gegevens alsmede getes-te en geaccepteerde apparatuur wordt gewerkt.

In het voorgaande is de aandacht erop gevestigd dat in een on-line-omgeving het autorisatie-aspect (wie) meer aandacht dient te krijgen. Dit geldt zeker voor een on-line real time-omgeving. De gebruiker dient verantwoordingsinformatie te ontvangen waaruit blijkt dat de functiescheiding in de "automatisering" is geëffectueerd en als zodanig in continuïteit wordt gehandhaafd.
Bovendien is gememoreerd dat bij eenmalige vastlegging het risico van verlies van gegevens wordt vergroot en aanvullende maatregelen nodig zijn. Over het feit of die maatregelen voldoende zijn dient de gebruiker te worden geïnformeerd. Bij de test-, acceptatie- en overdrachtsprocedures dienen deze aanvullende maatregelen te worden getoetst. Over de continue werking van de maatregelen dient de gebruiker periodiek te worden geïnformeerd.

5. Gemeenschappelijk programmagebruik (program sharing)

Het derde aandachtsgebied - naast resource en data sharing - van geïntegreerde gegevensverwerking is het gemeenschappelijk gebruik van programmatuur. Dit houdt in dat uit controle-oogpunt gescheiden (gebruikers)functies gebruik maken van dezelfde programmatuur.
Program sharing kan zich voordoen zowel in een batch als in een on-line-omgeving. Bij batch-verwerking wordt gemeenschappelijk gebruik gemaakt van het hele batch-programma waarin de volgorde van activiteiten vrijwel vastligt. In een on-line-omgeving kan deze situatie wijzigen. Immers bij on-line-verwerking kan de verwerkingsgang bestaan uit in programmatuur opgenomen acties die niet altijd in vaste volgorde hoeven te worden gebruikt. Elke actie toevoegen, wijzigen of verwijderen is als het ware een programma op zich dat in verschillende verwerkingsgangen kan voorkomen. De volgorde van de acties (programma's) kan steeds wijzigen (gewijzigde programmastring).

In hoeverre program sharing invloed heeft op de interne controle is in belangrijke mate afhankelijk van wat het gemeenschappelijk gebruikte program-

ma in welke situatie met welke gegevens kan (en mag) doen en in hoeverre de gebruiker verantwoordingsinformatie ontvangt.
Daarnaast speelt nog mee of er sprake is van data sharing, al dan niet met gebruikmaking van een dbms. Met opzet is de relatie weer gelegd naar het gegevensgebruik. Indien dat uit interne controle-oogpunt voldoet, is daarmee tevens program sharing onder controle. Het programma is immers een hulpmiddel en intermediair tussen gebruiker en gegevens.

Toch heeft on-line-verwerking een aantal aspecten die uit oogpunt van controle nadere aandacht verdienen en een extra dimensie krijgen in geval van program sharing:
a. het autorisatie-aspect ten aanzien van het programmagebruik;
b. de invloed van on-line-programmatuur op het testen;
c. functieverbijzondering in de gebruikersorganisatie.

Ad a.

On-line-programmatuur is te beschouwen als verknipte batch-programmatuur waarbij per "actie" (of deel ervan) een programma is ontwikkeld. Bij (gemeenschappelijk) gebruik ervan in een on-line-omgeving kan het voorkomen dat de volgorde van uit te voeren acties variabel is (programmastring is variabel).
Deze volgorde is afhankelijk van de door de terminal-bediende uit te voeren bewerkingen.
Toch moet er bij gebruik van on-line-toepassingen rekening worden gehouden met het feit dat slechts die programmatuur aan de gebruiker beschikbaar wordt gesteld - ongeacht de volgorde - waartoe hij/zij gerechtigd is. Dit kan op twee manieren:
- de programmatuur wordt ontwikkeld als een batch-programma waarbij elke voorkomende verwerkingsvolgorde (string) zodanig wordt opgebouwd dat geen problemen met de autorisatie-aspecten ontstaan. De volgorde moet een afnemende autorisatie bevatten. In dit geval wordt de autorisatie geregeld via de toepassingsprogrammatuur. Deze vorm kan (en zal) een goede beheersing van de autorisatie in de weg staan. Immers bij programma-onderhoud zal nauwlettend in de gaten moeten worden gehouden of niet van de in eerste instantie gekozen volgorde wordt afgeweken;
- elk programma of essentieel deel ervan wordt in de programmatabel van de TP-monitor voorzien van een code. Bij het aanroepen van dit programma voor gebruik zal de overkoepelende besturingsprogrammatuur controleren of gebruik geoorloofd is. Zo niet dan wordt de verwerking afgebroken. Op deze manier is er centrale controle op het geoorloofd gebruik van programmatuur mogelijk.

Ad b.

Het testen van batch-programmatuur is - afgezien van het bedenken van testgevallen - relatief eenvoudig.
Bij on-line-programmatuur is dat veel moeilijker gezien:
- het grote aantal programma's;
- de mogelijk wisselende volgorde van de programma's (string).

Bij het testen zullen per programma de functies moeten worden getest alsmede de autorisatie-aspecten van de totale string. Daarbij komt nog het probleem dat testen teruggebracht is tot beeldschermactiviteiten.

Het verkrijgen van "test-evidence" wordt daardoor bemoeilijkt omdat vastlegging van de testresultaten in sterke mate vermindert. Alhoewel er programmatuur is om een batch-situatie te simuleren is het gebruik van die programmatuur in de praktijk van beperkte aard. De basis voor acceptatie van programmatuur, alsmede voor controle achteraf op de testactiviteiten, vervalt hierdoor grotendeels.

Eerder is gesteld dat het testen van programmatuur - dus ook on-line-programmatuur - in bepaalde gevallen beperkt kan blijven tot het functionele (het wat). Dit geldt in situaties waar geen sprake is van data sharing of waar adequaat gebruik wordt gemaakt van de controlefaciliteiten van een database management systeem en de dba-functie per programma een aangepaste deelbeschrijving (subschema) bepaalt en implementeert.
Hier wringt de schoen. Het aantal on-line-programma's is meestal dermate groot dat geen verhouding programma-subschema = 1:1 wordt toegepast of mogelijk is. In een dergelijke situatie zal bij onderhoud en testen van programmatuur ook weer aandacht moeten worden geschonken aan het wat met welke gegevens. De subschema's zullen over het algemeen te ruime mogelijkheden bieden waardoor het opnemen van ongeoorloofde activiteiten in programmatuur tot de mogelijkheden blijft behoren.

Ad c.

In geval van program sharing geven de argumenten onder a. en b. grond aan de verbijzondering van een systeembeheersfunctie (ook wel applicatiebeheer genoemd) in de gebruikersorganisatie. Als bovendien sprake is van program sharing zullen, indien aanpassingen in programmatuur moeten worden geëffectueerd, meerdere gebruikersfuncties erbij moeten worden betrokken.
Dit vereist coördinatie-activiteiten. Dit is effectief op te lossen door een verbijzonderde systeembeheersfunctie in te stellen. Hiervoor ontbreken nogal eens de mogelijkheden. Een alternatief kan dan worden gevonden in een overlegstructuur.

6. Het gebruikersprobleem

Het zal de lezer duidelijk zijn dat naast data sharing en program sharing, resource sharing steeds meer invloed krijgt op de interne controle, zowel in de gebruikers- als in de automatiseringsorganisatie. De gebruikers "sharen" een organisatie met zeer complexe hulpmiddelen.
Die complexiteit wordt niet alleen veroorzaakt door de hulpmiddelen zelf maar tevens door steeds verdergaande integratie van die hulpmiddelen.
Bovendien maakt die automatiseringsorganisatie gebruik van diezelfde hulp-

middelen. In deze complexiteit dient de nodige functiescheiding in de gebruikersorganisatie te worden gewaarborgd.
Voorwaar geen eenvoudige zaak.
In beide organisaties wordt de delegatie- en verantwoordingsstructuur steeds complexer waarbij één ding voorop staat. De van oorsprong bestaande taken zijn niet nieuw maar zijn steeds verschoven en al dan niet in een verbijzonderde functie ondergebracht. De kunst (en het vakmanschap) is te onderkennen welke verschuivingen zijn opgetreden, welk delegatieproces daarbij hoort en of de daarbij behorende verantwoordingsinformatie voldoende is.

Gezien de huidigde status (complexiteit) van automatisering dringt de vraag zich op of de "gebruiker" nog voldoende in staat is (deskundigheidsprobleem) om zijn oorspronkelijk toebedeelde verantwoordelijkheid nog te kunnen dragen.
Kernbegrippen in deze zijn verantwoordelijkheid en deskundigheid. Onmiskenbaar heeft het ene met het andere te maken.
In de praktijk wordt de oplossing van het deskundigheidsprobleem nogal eens gezocht in het stationeren van een "deskundige" tussen de gebruiker en de automatiseringsorganisatie, die beider talen spreekt. Hiertegen kan geen bezwaar bestaan mits de verantwoordelijkheden maar duidelijk zijn. Halfslachtigheid is in deze situaties maar al te vaak troef. In situaties waar het mis loopt wordt de beschuldigende vinger toch naar de gebruiker gewezen en de tussenpersoon wast zijn/haar handen in onschuld. In tegenstelling tot wat tot nu toe in dit artikel is gesteld is het verleggen van verantwoordelijkheden wel degelijk acceptabel, vaak zelfs aan te bevelen. Het moet dan echter wel bewust en expliciet worden gedaan.

Het is derhalve noodzaak dat bij wijziging in de (complexiteit van) geautomatiseerde gegevensverwerking wordt nagegaan welke invloed die wijziging zal hebben op de bestaande verantwoordings- en delegatiestructuur (aanpassing functie en taakbeschrijvingen).

7. Verbijzondering van functies (data administration, database administration)

Een aantal keren is gesproken over de verbijzonderde functies gegevensbeheer (data administration) in de gebruikersorganisatie en de database administration in de automatiseringsorganisatie. In vele organisaties (waar sprake is van data sharing) blijft de verbijzondering afwezig of komt slechts gedeeltelijk van de grond. Een van de belangrijke taken van de data-administration is het geven van richtlijnen met betrekking tot het gegevensgebruik (zodanig dat functiescheiding in de gebruikersorganisatie niet wordt aangetast) die dan door de database administrator moeten worden uitgevoerd.
Bovendien moet data administration zorgen voor controle op naleving van de voorschriften. Het gevolg van het ontbreken van een verbijzonderde data administration functie (in geval van data sharing) is, dat verschuiving van

die taken naar de automatiseringsorganisatie plaatsvindt. Verschuiving vindt dan plaats naar een verbijzonderde database administration-functie, systeemontwikkelings- en/of systeemprogrammeringsfunctie.
Door deze verschuiving wordt dan wel veroorzaakt dat het gegevensgebruik in geval van automatisering (in casu functiescheiding in de gebruikersorganisatie) wordt bepaald door de automatiseringsfunctie (wat altijd met kracht is bestreden).

8. Geïntegreerde versus database-omgeving

Het moge duidelijk zijn dat in een geïntegreerde (data sharing) situatie niet altijd gebruik hoeft te worden gemaakt van een database management systeem (dus database) en er in een database management systeemomgeving niet altijd sprake hoeft te zijn van data sharing.
Data sharing met gebruik van een database management systeem biedt meer beheersingsmogelijkheden mits het database management systeem - uit controle-oogpunt - juist wordt gebruikt en de organisatorische verbijzonderingen adequaat worden ingevuld (data administration c.q. database administration).

9. Geïntegreerde gegevensverwerking

Deze verwerking is gekoppeld aan de drie begrippen data sharing, program sharing en resource sharing.
In dit artikel zijn vanuit een basissituatie de ontwikkelingen aangegeven die automatisering heeft gebracht tot wat het nu is. De situaties zijn sec weergegeven. Het grote probleem om in de praktijk de complexiteit aan te kunnen, is het feit dat alle geschetste situaties thans in één en dezelfde organisatie kunnen voorkomen en feitelijk ook voorkomen. Bij het overgaan naar een nieuwe situatie is de voorgaande niet weg. De erfenis uit het verleden wordt meegedragen en kan niet snel worden omgebogen. De complexiteit in combinaties met data sharing, program sharing en resource sharing zal per situatie verschillen. Handhaving c.q. verbetering van inzicht in een daarbij behorende gebruikers- en automatiseringsorganisatie die voldoet aan gestelde interne controle-eisen (delegatieverantwoording) is een uitdaging voor de toekomst en vereist de nodige kennis. Ook de huidige accountant dient deze kennis te bezitten.

10. De accountant en geïntegreerde gegevensverwerking

Voor de controle van de jaarrekening maakt de accountant zoveel mogelijk gebruik van de interne controle die bij de cliënt wordt aangetroffen. Het gaat hierbij in eerste instantie om de aanwezige controlemaatregelen in de gebruikersorganisatie alsmede - indien nodig - in de automatiseringsorgani-

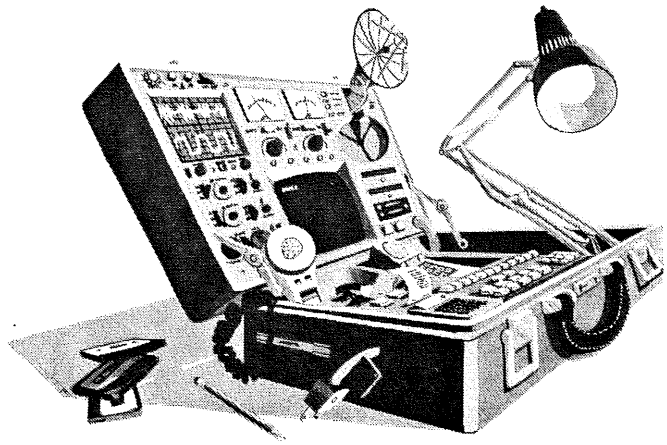
satie. Gericht op de gebruikersorganisatie zal de accountant onderzoeken of de minimaal vereiste functiescheiding aanwezig is en niet door de automatisering wordt aangetast. Daarnaast wordt onderzocht in hoeverre de gebruiker de geautomatiseerde gegevensverwerking onder controle heeft. Dit alles gebeurt door na te gaan welke verantwoordingsinformatie de gebruiker van de automatiseringsorganisatie ontvangt om vast te kunnen stellen of de gedelegeerde taken juist zijn uitgevoerd. In tweede instantie wordt nagegaan wat de gebruiker met die informatie doet (gebruikerscontroles).

In een omgeving waar sprake is van een grote complexiteit (data, program en resource sharing) zal de accountant in toenemende mate problemen ondervinden in het bepalen van de controlewaarde die aan de informatie die de gebruiker ontvangt kan worden toegekend.
Gezien de toenemende complexiteit en de daarmee samenhangende verschuivingen is dit geen eenvoudige zaak. Indien de (automatiserings)kennis van de accountant op dit punt tekort schiet kan dit grote gevolgen hebben voor een door hem/haar uit te voeren controle van de jaarrekening.
De accountant dient zich van het volgende dan ook zeer bewust te zijn.

> Automatisering van de informatieverwerking kan gekenschetst worden als het probleem van de verschuivingen waardoor een steeds wisselend delegatie- en verantwoordingspatroon ontstaat als gevolg van technologische ontwikkelingen en een toenemende tendens tot samenvoegen, gemeenschappelijk gebruik en verbijzondering waardoor het voor de gebruiker en de accountant steeds moeilijker wordt de juiste waarde te kunnen toekennen aan de verantwoordingsinformatie uit het geautomatiseerde proces.

COMPACT is een uitgave van
KMG Klynveld EDP Audit Services

Winter 1986/Lente 1987



DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE

door H. Veenman

In deze rubriek aandacht voor twee artikelen, te weten:
- Introduction to the File Analysis Product Line, door H. Veenman en ing. J.C. van Winkel (pag. 54);
- File Analysis Tool in de praktijk, door J.A. van Rooden (pag. 69).

Het eerste artikel is als "paper" ingezonden aan de EDP Auditors Association als voorbereiding op een presentatie aangaande dit onderwerp op de eerste Europese EDPAA-conferentie in september 1986.
Terwijl in dit artikel wordt ingegaan op de achtergronden en de opzet van de produkten in de File Analysis Product Line, wordt in het tweede artikel, dat is overgenomen uit het blad "Oogmerk" van kantoor Rotterdam, juist het gebruik van de pakketten belicht.

Introduction to the File Analysis Product Line

by KMG Klynveld EDP Audit Services, september 1986
door H. Veenman en ing. J.C. van Winkel

Introduction

Automation of the audit process made its entrance about 15 years ago at KMG Klynveld Kraayenhof & Co.
The first micros were the HP85 computers that were merely used to run mathematical samples on clients figures.

In addition to the use of micro computers, the use KMG KKC's mainframe for the purpose of running audit tests was increasing in the 1970s.
Each year more audit applications were developed and maintained in CA-Earl, Culprit and COBOL. Most of these applications concerned the production of Balance Sheets, Sampling Reports, Selections and Aging Reports.

HP85 is a product of Hewlett-Packard.
CA-Earl is a trademark of Computer Associates International Inc.
Culprit is a trademark of Cullinet Software Inc.

With the great micro boom which manifested itself internationally in the early 80s both KMG KKC and the worldwide KMG organization realized that the micro computer could be of enormous value when applied during the audit process. KMG founded the Computer Audit Sub Committee (CASC). Their mission was to investigate how the audit process could be automated. Eight "Micro projects" were distinguished with subjects like:

- the interface between the auditor and the micro computer;
- the interface between the micro computer and client data;
- automated sampling methods and routines; and
- overall automation of the audit process.

In 1982 a group of KMG Klynveld Kraayenhof & Co. staff, consisting of software engineers and computer science trainees, started to investigate how to realize the two major interfaces that were determined by the CASC, being the interface between auditor and computer, and between computer and client data.
During this phase two very important issues were raised:

- when software is to be used by auditors it should be user-friendly and full-proof, because we cannot assume that the user of this software is a computer expert; and
- when software is to be developed in-house, high standards must be observed to maintain quality and continuity. Continuity can only be achieved by documenting properly and by choosing a development environment that can be easily migrated to wherever the future will take us.

The result of this research was a first design for a User Interface, and a report on the problems to be addressed when client data must be made available to the Auditors' Micro.
In chapters 2 and 3 these topics are discussed in more detail, and chapter 4 addresses KMG's portability considerations.
The components of the KMG File Analysis Product Line are subsequently exposed in chapter 5.

2. The interface between the auditor and his micro

When a product is to be used by people who do not want to understand the product but only to achieve the ends to which the product is the means, this product must be developed with the user in mind.
For using a product like KMG's File Analysis Tool for instance, an auditor wants to produce reports or other material that he can efficiently use during his audit.
One of the major items that can be distilled from the report is that audit software on a micro should be menu-driven.
Menu-driven software guides its user through a sequence of screens (menus) until it has sufficient information to fulfil the mission that is requested. This way a clear distinction can be made between the user interface of a product and its "workhorse". The workhorse is that part of a program where the interactive user interface stops and the computer starts honouring the request.

By defining a very thin and precise gate between the user interface and the workhorse (see fig. 1), both parts can be seen as fully independent programs, the first is fed by the auditor, while the second gets its input from the user interface.

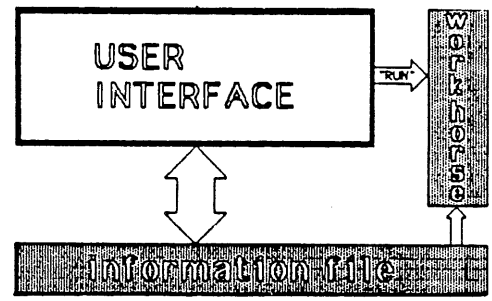


Figure 1.

It is clear that by using this approach the message that is passed through the gate must contain all information which the workhorse needs to perform its task. Focusing on FAT this means that the description of a complete file analysis can be found in the information transported through the gate. Since the KMG File Analysis Tool allows you to:
- define a request without actually performing it and
- run an audit test that is defined during another session;

the information passed through the gate must also be saved outside the program's memory. This information is therefore stored on a disk in an "information file".
It should be noted that the contents of an information file could also be interpreted to generate a program in a high level language, instead of being interpreted and executed directly by the workhorse. It is a matter of replacing this workhorse by an application generator.

KMG KKC developed a standard definition of how a user interface should be presented to its user. Two major topics in this standard are:
- the user controls; the user interface via a bar of function keys, which is displayed at the bottom of each screen;
- a limited number of screen types which can be distinguished.

In the next two paragraphs the implementation of both topics is described briefly.

2.1 Function keys

All products in the File Analysis Product Line have a bar of function keys displayed on the bottom line of the screen. In figure 2. a list of the function keys and their purpose is shown.

F1	<-PAGE	F6	DEL LN
F2	PAGE->	F7	CLEAR
F3	<-ITEM	F8	QUIT
F4	ITEM->	F9	FLOPPY
F5	INS LN	F10	HELP

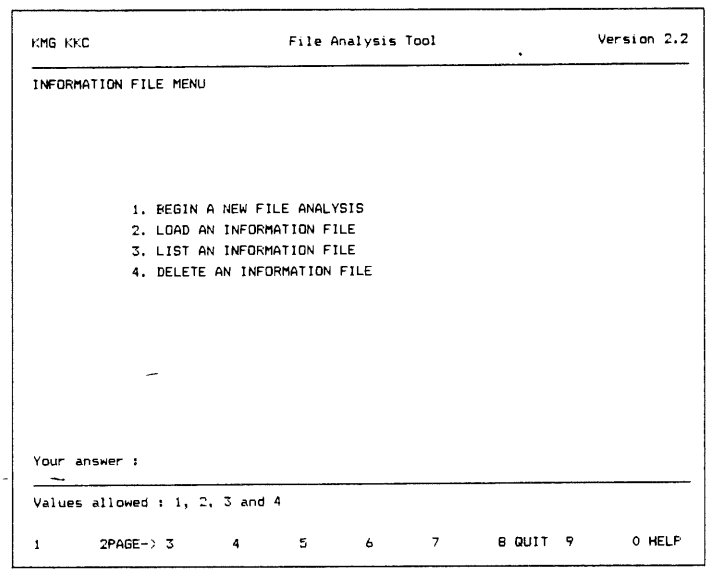
Figure 2.

2.2 Different types of screens

Looking to the user interface of the File Analysis Product Line the following screen types can be distinguished.

2.2.1 Menu screens

As the name implies, menu screens offer a number of choices. You can make a selection by positioning the highlight cursor bar onto your choice with the cursor keys and then pressing F2 PAGE- > . Fig. 3 shows what a FAPL menu screen looks like.



Information File Menu

Figure 3.

2.2.2 Input screens

Input screens are used to prompt you for information necessary to define a FAPL process. Not all input screens you encounter have to be filled in to proceed.
A highlight cursor bar indicates which item is active (i.e. which will be edited).

The F2 PAGE-> becomes active when all of the required items have been filled in and can then be used to proceed to the next screen.

2.2.3 Progress information screens

While the workhorse is active, it will keep you informed on how the process is evolving. Information will be displayed on how many records have been read, how many records have been converted, how many pages have been printed and so forth.

2.2.4 Help screens

Help is invoked by pressing the F10 HELP key. The HELP key is always active and will display one or more pages of context-specific help. (This means that the information provided is only what you need to know at that specific time.)

3. The interface between audit micro and client data

Basically there are two ways to make client data available for use on an audit micro, namely by ways of exchanging media like floppy disks or tapes, and by transmitting data via a data communications facility.

One should not forget, however, that availability of data, as a result of media exchange or data communications, does not give any guarantee that the data can be processed by an audit program directly. This because a lot of computers use different data representation standards. A well known example is the difference in representation of data on an IBM mainframe, and on an IBM personal computer: the first is in EBCDIC and the second in ASCII representation.
It therefore can be concluded that apart from the data being physically available on the audit micro, some data representation transformations also have to be made to make it logically available.

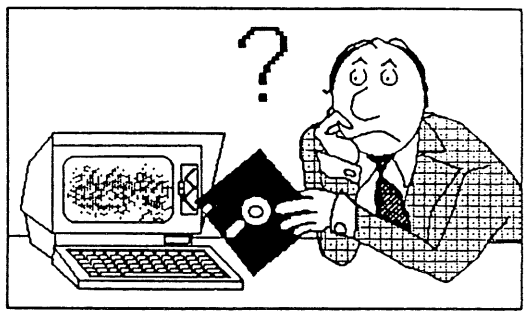


Figure 4.

4. Portability considerations

During the design of the File Analysis Product Line, a choice had to be made about the type of computer FAPL had to run on. The speed, availability and storage capacity needed to run FAPL at a reasonable price made clear that this computer had to be one of the 16 bit computers that were just becoming widely available. IBM's personal computer fitted the requirements nicely and appeared to become a new standard in personal computing.

It was however clear that it might someday be necessary to migrate to another type of computer. Besides that transportation of KMG's products to larger sites - e.g. client minis or mainframes - could also be one of the future demands.

Portability of the software was therefore a major design issue that was achieved by:
- using the UNIX development environment including the C programming language for building and maintaining the software; and
- enforcing a very strict separation between the product's portable and non-portable software modules.

IBM is a trademark of International Business Machines Inc.
UNIX is a trademark of Bell Laboratories.

This approach has proven to be successful since parts of the FAPL are now available on very different types of hardware.

5. The KMG KKC File Analysis Product Line

Focusing on the tasks that have to be performed to accomplish a successful analysis, we can distinguish three major functions:
- conversion and/or reformatting of client data;
- comparing or joining collections of data; and
- producing reports for audit purposes.

It is clear that these functions are quite different with regard to the goal each of them should achieve. Additionally each function requires a slightly different skill to be used properly.
For example, to set up a conversion, one should know some basic things about diskettes and data representations, while no actual audit skill is needed. Definition of an audit request, on the other hand, requires knowledge about auditing and not about storage media.

With this in mind, it was apparent to the KMG KKC development team that these functions had to be implemented in three separate modules.

Integration of the modules is effected by importing and exporting information files from one module to the other.

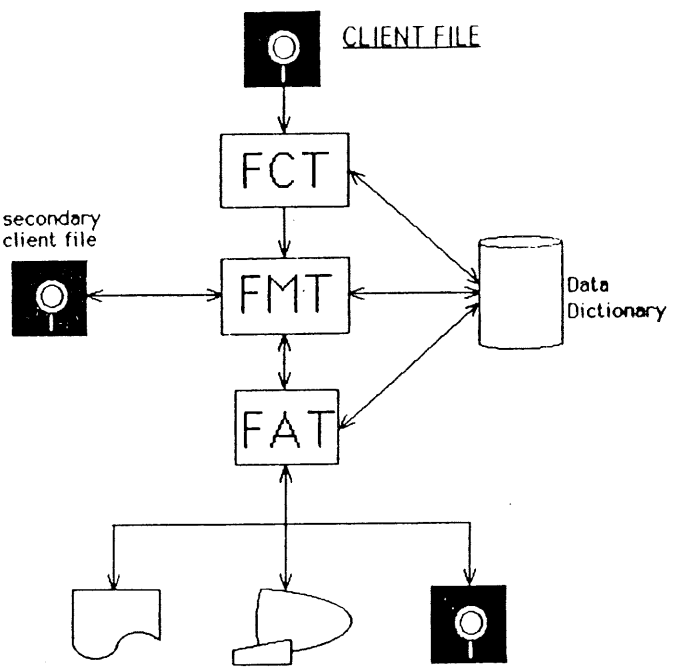


Figure 5.

5.1 The KMG File Analysis Tool (FAT)

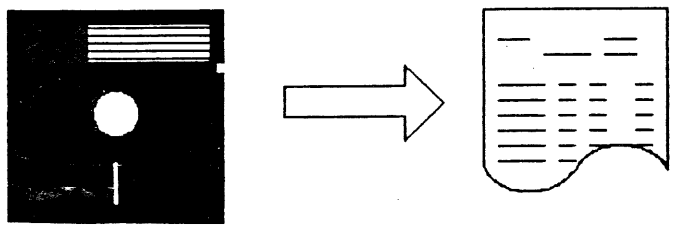


Figure 6.

FAT is a data-oriented audit tool you can use to examine client data files such as a general ledger or a sales journal to verify that the records on which financial reports are based reflect established accounting principles.
FAT is user-friendly and is designed for direct use by auditors; special programming knowledge is not necessary.

You can use FAT to support compliance as well as substantive and dual purpose testing. And, unlike general purpose data base programs, FAT has the built-in test routines auditors need and produces reports in a form suitable for direct inclusion in your working papers.

By automating this testing process, FAT makes the examination of large volumes of data more economical. Manual follow-up of processing results will remain an essential part of control procedures; however, FAT eliminates tedious and increasingly costly work and focuses attention on important judgement areas. Using FAT will save costs over a number of years and will result in more effective verification.

5.1.1 How FAT works

FAT uses five principle means of manipulating client data to carry out a wide variety of tests. These techniques can be used alone or in combination to analyse a file and they include:

1. summation;
2. sorting;
3. statistical sampling;
4. selection;
5. mathematical calculation.

With these five techniques, FAT gives you the flexibility needed to carry out effective audit testing. There is no single computer-assisted audit just as there never was a single "manual" audit.

Here are some examples of the many tests FAT can perform:

1. Total controls. FAT can be used to add all the debit and credit fields in a data file such as an accounts receivable file to see if the totals agree with each other and with control counters maintained outside the computer and in the general ledger.

2. Aging. FAT can be used to age the entries in a client file such as in an accounts receivable sub-ledger. For example, outstanding purchases older than 60 days can be listed to the printer or disk file for verification and review.

3. Tolerance controls. FAT can be used to examine values which may only deviate from the norm by a fixed percentage. For example, you can test to see if the gross profit for a certain article deviates by more than 15 percent.

4. Statistical sampling. FAT has a sophisticated built-in statistical sampling routine known as the sieve method which can be used to build a random sample of transactions or postings for subsequent compliance verification.
   The sieve method may select any record in a file; however, larger amounts have a greater chance of being selected and you can choose a sample size such that all amounts over a specified value are certain to be selected.

5.2 The KMG File Match Tool

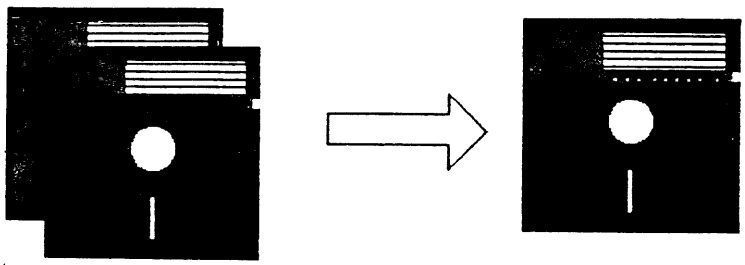


Figure 7.

When two collections of data have to be confronted to determine differences, to combine certain items just to merge the collections into one file, the File Match Tool will take care of these tasks for you.
FMT is to be seen as a preceding phase to a file analysis, and is therefore not able to produce reports. FMT produces a file from which a report can be derived by using FAT.

FMT offers four types of matching processes: COMPARE, MERGE, UPDATE and JOIN.
COMPARE lets you compare two files. Specify the record layout of both files (they may differ), specify the keys on which the comparison should take place and FAT will provide you with an output file containing the records that did not have an opponent in "the other" file. An indicator tells you which file the record comes from and the record number is also added.
MERGE enables you to merge two files into one; both files must have the same record layout and length. In other words: two input files will be sorted to one result file, in the sequence defined by the merge key.
UPDATE offers you the possibility of updating an existing file with changes. This can be a balance file that must be updated with new entries, but also a name-and-address file that must be updated. The first file may only have one record per key, while the second file can have zero, one or more records with a corresponding key.
JOIN is for the purpose of joining data of two files in one. The records layouts of the files may differ. It can be used for joining two files containing account numbers and account descriptions respectively.

5.2.1 The FMT information files

Like the File Analysis Tool the File Match Tool saves the information about a defined matching session on disk. Information files containing FMT definitions have a ".FMT" extension. Since FMT is generally used as a pre-processor to a FAT session and since each FMT session ends with generating a disk file, a ".FAT" Information File will be produced which contains the record layout of this file and can be directly imported by FAT.

5.3 The KMG File Conversion Tool

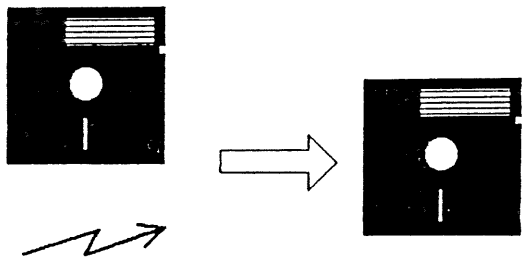


Figure 8.

Often client data is not directly processable by FMT and FAT, i.e. not available on the only medium the IBM PC knows about: the five and a quarter inch MS-DOS formatted diskette. To overcom this problem, FCT offers the possibility of converting files without being bothered with special knowledge of the way in which files are stored.
Neither is any knowledge required about the way in which the actual conversion takes place. You will just have to specify the necessary parameters and FCT does the job for you.

Similar to the other products of the File Analysis Product Line, the user interface of FCT is developed in such a way that using FCT is very easy. Even if something is not quite clear, detailed assistance is provided in the form of numerous help pages. These help pages are what is called Context Specific: this means that at any point within the user interface, you can call in the assistance you need for that specific screen.

FCT is user-friendly and is designed for direct use: no special programming knowledge is required.

5.3.1 Where diskettes differ

The way data is stored on a magnetic media differs from computer to computer and from operating system to operating system. In scrutinizing these discrepancies four layers can be distinguished:

- at the bottom layer the differences stem from the way the computer communicates with the hardware that writes on the disk and the hardware used itself. Matters like the size of the disks, single density, double density and group coded recording, single and double sided disks, the number of tracks per inch and so on are defined at this level;

MS-DOS is a trademark of Microsoft.

- the next layer determines the way the data is distributed on the disk; these differences mostly originate from the type of operating system used to create the files to the diskette. Some operating systems present a hierarchical file system with (sub)directories (MS-DOS, UNIX), whereas other systems present a flat file space (CP/M). The way disk space is allocated to files; the place where directories and file administration data (e.g. a file allocation table) are stored and how permissions to read or write from files and the users allowed to do so, is defined etc., are all defined by the operating system;
- the following layer is more or less determined by a combination of the operating system and the application. For example: if the application wants index sequential file access and the operating system does not support this, the application has to provide for the indexing itself. An illustration of this is: on the UNIX and MS-DOS based computers, where files are accessed as sequential arrays of characters, whereas other operating systems may block data resulting in non contiguous data streams;
- the topmost layer is almost fully application determined: the application determines what data types are stored in the files (although on an IBM mainframe it will be unlikely that the file will contain ASCII characters). The application is more or less free to choose the way it wants numbers to be represented in the file although some degree of standardization exists.

5.3.2 How FCT is built up

FCT is a tool that is designed to overcome all these differences. To do so it provides two global types of conversion:
1. disk-to-disk conversion;
2. datacom-to-disk conversion.

Using option 1. the auditor is enabled to convert any type of diskette into a new format, whereas option 2. is meant to be of use whenever data is received via a data communications link.
Straightforward conversion will look like a simple copy operation, but it is likely that the data on the "output" diskette must be stored in a format which is different.

The multitude of different diskette formats currently available (and to be expected), forced us to explore a way to bring order to the present chaos. In analysing diskette formats it is noticed that most of the differences found are easily parameterizable.

CP/M is a trademark of Digital Research, Inc.

An example will make this more clear: All diskettes coming from computers running CP/M will have the same design at the file organization level. Although diskettes may have different sizes, ranging from 3 inch to 8 inch and the density in which the data is written may differ, the diskette has the same layout. Every CP/M diskette will obey certain layout rules, specifying the relative place the directory will be stored, the layout of the directory and so on.

It is therefore possible to make just one (sub)program defining the CP/M characteristics, whereas all variable parts (such as directory sizes, disk density and so on) can be parameterized.

This viewpoint led to the definition of formats and categories:
- a format is one single diskette format. This can range from the MS-DOS single sided disks to MS-DOS double sided disks and even CP/M or UNIX disks, and
- a category is a set of formats that have similarity in the way data storage is organized. Therefore all CP/M formats occupy just one category. Parameters can then be used to distinguish all formats within the category.

It is clear that because of this definition programming is only required for each category, and not for each format.

Currently the following categories have been developed:
- for input CP/M, MS-DOS, UNIX and IBM 8" (IBM mainframe and mini computers), and
- for output, only MS-DOS.

5.3.3 Data representation

The differences between data on diskettes are however not just determined by category and format: The application layer defines the way data is stored in the file.

FCT therefore has two modes of operation: a raw mode, in which data is copied from one medium to another without transforming any part of it, and a sophisticated reformatting mode. In this mode, data can be transformed from one type to another, fields can be deleted from or added to the output record; fields can even be duplicated. This does not just include plain EBCDIC to ASCII conversions, but also provides for conversion of several types of floating point numbers, internal integer numbers, record types and so on.
A list of supported data types is shown in figure 9.

To offer these extensive conversion capabilities, three different record types have been defined:
- fixed layout;
- separator oriented layout, and
- repeating groups oriented layout.

Figure 9.

NAME	DESCRIPTION
A	Plain ASCII text.
AN	ASCII numeric data, no sign.
ALS	ASCII numeric data with separate leading sign.
ATS	ASCII numeric data with separate trailing sign.
E	Plain EBCDIC text.
EN	EBCDIC numeric data, no sign.
EL	EBCDIC numeric zoned with leading sign.
ET	EBCDIC numeric zoned with trailing sign.
ELS	EBCDIC numeric data with separate leading sign.
ETS	EBCDIC numeric data with separate trailing sign.
PD	Packed decimal numeric data.
MSF	Microsoft single precision floating point (Microsoft BASIC single precision).
MDF	Microsoft double precision floating point (Microsoft BASIC double precision).
ASF	ANSI standard single precision floating point (8087 format).
ADF	ANSI standard double precision floating point (8087 format).
I0	In-memory integer format type 0.
I1	In-memory integer format type 1 (Microsoft BASIC integer variables).
I2	In-memory integer format type 2.
I3	In-memory integer format type 3.
I5	In-memory integer format type 5.
I6	In-memory integer format type 6.

Fig. 9 FCT data types

Within each record fields can be deleted, copied and moved. Whenever record separators, field separators or end of file indicators are used, the user may define them, with a maximum of four bytes. Also a decimal separator may be defined by the user.

5.3.4 The Format and Drive Dictionary Files

As already stated FCT's disk formats are categorized on the basis of similar file storage structure, such as directory structure, allocation of disk storage, file allocation table(s) and so on.
The precise definition of one format is accomplished by filling in the remaining (category specific) parameters. This is done in the FCT Formats Dictionary, that can be manipulated by the user of FCT.
In this way diskette formats can be defined, altered or deleted by the user. Programming by the FCT development staff is only required if an entirely new category is to be added.

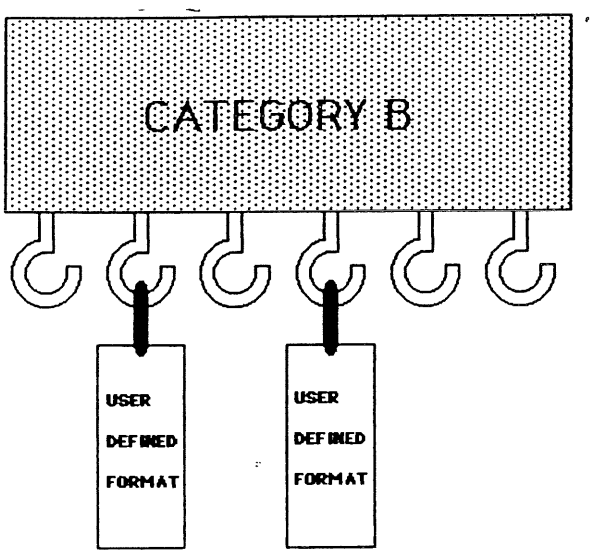


Figure 10.

The configuration of the hardware used to run FCT is also described in a dictionary. By editing the FCT Drives Dictionary the system can be informed about attachment of an extra drive, about a drive not being available due to maintenance, and so on.

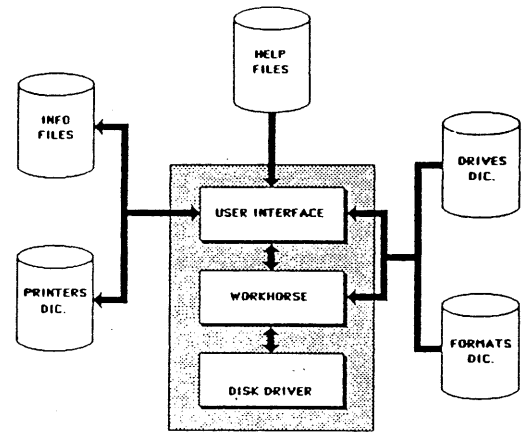


Figure 11.

5.3.5 Open endedness

FCT is an open ended product in three different ways: it is possible to add new categories, new formats within categories and new field types.

FCT was designed in such a way that the programming effort needed by the KMG Klynveld EDP Audit Services development team to add a new category or field type is minimal. A new format can be added by the user himself. The manual describes how this can be done.

One could say that FCT consists of a framework providing everything needed to handle data files. The category and data field software provides for the actual conversion. From this view one can easily see that FCT is a product that was made with the future in mind.

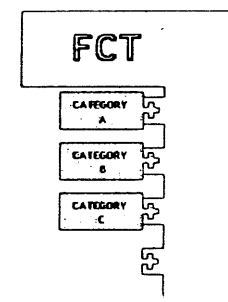


Figure 12.

5.3.6 The status of FCT development

The current version of FCT can address the following categories for input:
- IBM 8 inch;
- CP/M;
- UNIX;
- MS-DOS (IBM PC and AT disks);
- data communication.

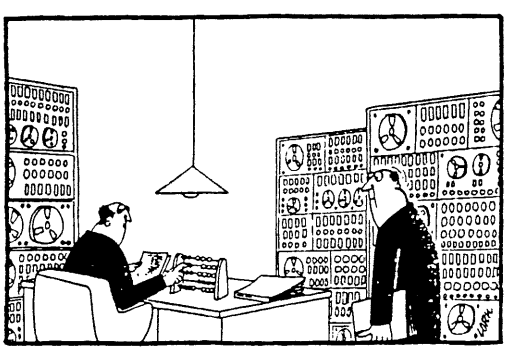
For output, only the MS-DOS category has been implemented.

Other categories like UNIX will be implemented in due course.

Contact KMG Klynveld EDP Audit Services for the conditions under which additional categories will be added.

File Analysis Tool in de praktijk
door J.A. van Rooden

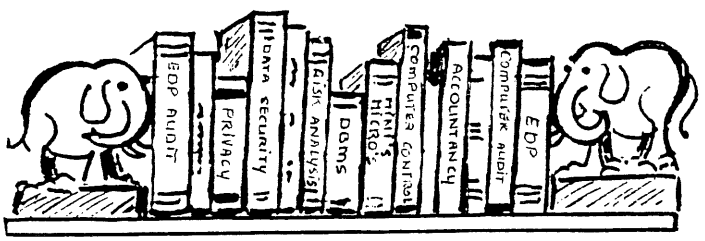
Het is al weer een poosje geleden dat het File Analysis Tool (kortweg FAT) in definitieve vorm werd geïntroduceerd. Om het pakket wat meer bekendheid te geven werd voor ons kantoor Rotterdam een presentatie verzorgd door twee leden van KMG Klynveld EDP Audit Services, sectie Support & Programming. Voor hen, die dachten FAT in de praktijk te kunnen gaan toepassen werd de mogelijkheid geschapen een cursus te volgen. Van deze mogelijkheid hebben circa 25 personen gebruik gemaakt. Deze FAT-gebruikers-in-spee zijn in december van, inmiddels, het vorig jaar gevraagd welke toepassingen van FAT zij hadden gerealiseerd met de in de cursus opgedane kennis van het pakket. In een aantal gevallen was men er door tijdgebrek nog niet toe gekomen een volledig draaiende FAT-toepassing te fabriceren. Veel van deze personen dachten echter wel in 1987 (goed voornemen?) tot toepassingen te komen c.q. waren reeds zover dat werd proefgedraaid. Van de toepassingen die nu volledig operationeel zijn kan worden gezegd dat deze voornamelijk steunen op de mogelijkheid van FAT om snel en effectief posten te selecteren, waarbij gebruik gemaakt wordt van selecties gebaseerd op vaste criteria. Selecties die veel werden genoemd waren die van algemene kosten, investeringen en het bepalen van de te onderzoeken posten vanuit de inkomende facturen. In een enkel geval wordt gebruik gemaakt van de mogelijkheid van FAT tot het sorteren van een bestand gecombineerd met het bepalen van totalen, die kunnen worden gebruikt voor de controle, in totalen, van journaalposten. Voorts is vermeldenswaard dat de eerste stappen op weg naar het gebruik van het File Match Tool (FMT) in combinatie met FAT voor analyse van opbrengsten (dit is overigens niet de enige mogelijkheid van deze twee programma's samen) zijn gezet.
Al met al kan worden gesproken van een bemoedigend resultaat van de inspanningen om FAT meer bekendheid te geven. Voor hen, die aangemoedigd door deze resultaten FAT willen gaan toepassen bij hun cliënten zij opgemerkt dat in principe geen problemen bij de conversie van bestanden zijn te verwachten indien deze zijn aangemaakt op een IBM-computer (of een compatible).



Indien de cliënt gebruik maakt van een ander merk computer is het raadzaam om eerst contact op te nemen met een microbeheerder, zodat vooraf kan worden bepaald of FAT technisch toepasbaar is.
Dit is namelijk in veel situaties wel mogelijk, doch niet in alle. Contact met een microbeheerder is eveneens zinvol indien u voor een eerste keer een conversie wilt laten uitvoeren door de KMG Klynveld EAS Support & Programming, zodat u niet het risico loopt dat een conversie niet kan worden uitgevoerd door gebrek aan gegevens over het te converteren bestand. Voorts wordt aangeraden om met name een eerste conversie tijdig te laten uitvoeren omdat zich daarbij praktische problemen kunnen voordoen, waardoor de conversie wordt vertraagd (een conversie duurt in het algemeen maximaal één week). Of de conversie goed is verlopen kunt u constateren door middel van proefdraaien.

Voor de geïnteresseerden volgt nu een globale beschrijving van een volledig operationele toepassing.
Opgemerkt wordt hierbij dat het hier gaat om een voorbeeld, waarbij niet alle mogelijkheden van FAT worden benut.
De gekozen toepassing wordt uitgevoerd bij een groeiende cliënt in de categorie stukproduktie. Voor de toepassing wordt gebruik gemaakt van een maandelijks crediteurenbestand dat verkrijgbaar is met een inkoopboek. Eens per kwartaal worden de diskettes (circa 15) naar kantoor Amsterdam gezonden ter conversie. Zodra de geconverteerde (maand)bestanden zijn terugontvangen worden deze gekopieerd naar de vaste schijf van een op kantoor Rotterdam aanwezige microcomputer en samengevoegd tot een totaal periodebestand. Op dit bestand worden selecties uitgevoerd van op orders c.q. algemene kosten of specifieke grootboekrekeningen geboekte facturen. Hierbij wordt per analyse een verschillende grens gehanteerd waarboven de facturen geselecteerd worden. Afgezien van enkele problemen in de aanvangsfase, welke met de komst van de definitieve versie van FAT werden opgelost, is de invoering vlot verlopen, terwijl men gaandeweg meer mogelijkheden zag de verschillende selecties in een verwerkingsgang uit te voeren.
Invoering van de toepassing heeft nu reeds geleid tot een besparing van assistentenuren (circa 2 weken op de controle van de eerste 9 maanden van 1986), omdat de selecties voor invoering handmatig werden uitgevoerd, waarbij dikke lijsten moesten worden doorgespit. Door aanwending van deze beschikbaar gekomen tijd voor controles welke in het verleden door de massaliteit niet konden worden uitgevoerd (denk hierbij bijvoorbeeld aan beoordeling van risico's voortvloeiend uit de Wet Ketenaansprakelijkheid, eveneens met behulp van FAT), werd gekomen tot een verbetering van de kwaliteit van de controle. Voorts heeft de invoering geleid tot positieve reacties van de cliënt omdat meer tijd kan worden besteed aan advieswerkzaamheden c.q. administratieve dienstverlening. Toepassing van FAT heeft er eveneens toe geleid dat, hoewel het een groeiende cliënt betreft, de controleploeg geen uitbreiding behoeft.

Winter 1986/Lente 1987



Boeken

door drs. D. de Kruif, ing. J.C. van Winkel en J.A.W. Winterink, met medewerking van mw. drs. A. Klaver

"Kwaliteit en kwaliteitszorg van moderne informatiesystemen". Studiedag ter gelegenheid van de oratie van prof.dr.ir. H.J. Oppelland, gehouden op 11 september 1986.
door mw. drs. A. Klaver

Voorwoord

In deze bespreking wordt stilgestaan bij de oratie van prof. Oppelland ter gelegenheid van zijn aanvaarding van het ambt van gewoon hoogleraar in de Bestuurlijke Informatiekunde aan de Erasmus Universiteit Rotterdam op 11 september 1986. In aansluiting hierop worden drie voordrachten besproken die gehouden werden op de studiedag "Kwaliteit en kwaliteitszorg van moderne informatiesystemen" ter gelegenheid van de hierboven genoemde oratie.

Vele aspecten zijn van belang bij het onderzoek op het gebied van informatiesystemen. Prof. Oppelland spreekt in zijn oratie over de wetenschappelijke bescheidenheid die de onderzoeker dient te sieren en de eisen die de maatschappij aan zijn onderzoek mag stellen. Vervolgens gaan de drie overige sprekers in op enkele aspecten van dit onderzoek. Prof. Velthuizen spreekt over kwaliteitseisen die aan informatiesystemen gesteld moeten worden. Hij bekijkt dit probleem (evenals de sprekers na hem met betrekking tot hun onderwerp) vanuit het gezichtspunt van de accountant. Prof. Hartman beoordeelt de betrouwbaarheid van informatiesystemen aan de hand van enkele door hem geschetste modellen. Prof. Steeman tenslotte gaat in op enkele onderwerpen van zijn voorgangers en op de reikwijdte van de accountantsverklaring.
In de discussie van de voordrachten argumenteren de sprekers over begrippen als kwaliteit, informele informatie en functiescheiding.

Winter 1986/Lente 1987

"Ontwikkelingen in de research van informatiesystemen: Wat mag verwacht worden en wat niet."
Rede, uitgesproken bij de aanvaarding van het ambt van gewoon hoogleraar in de Bestuurlijke Informatiekunde aan de Erasmus Universiteit Rotterdam, op donderdag 11 september 1986 door prof.dr.ir. H.J. Oppelland.

Prof. Oppelland vraagt zich af, wat verwacht mag worden van research op het gebied van informatiesystemen. Hiertoe geeft hij eerst een beschouwing van wat verwacht mag worden van wetenschap in het algemeen.

Veelal wordt datgene wat "de wetenschap" beweert, als een objectieve beschrijving van wetmatigheden in de wereld om ons heen aangemerkt. Prof. Oppelland betoogt dat wetenschappelijke objectiviteit niets anders inhoudt dan dat een aantal wetenschappers, die volgens op een bepaald moment gangbare methoden onderzoek doen, het met elkaar eens zijn. In dit licht is de wetenschap van vandaag, de dwaling van morgen.

Naast dit algemeen geldende probleem van wetenschappelijk onderzoek, is het onderzoek op het gebied van informatiesystemen met een tweede probleem behept: Het object van onderzoek laat zich moeilijk met de gangbare methoden grijpen. Een goed voorbeeld is het onderzoek naar factoren die bepalen of de ontwikkeling van een bepaald informatiesysteem succesvol is. Men zou de hypothese kunnen poneren dat dit succes afhangt van twee factoren: "Worden de verwachtingen van de gebruikers waargemaakt?" en "Staan de gebruikers positief ten opzichte van hun participatie bij de bouw?"

Dit roept meteen twee problemen op. Er zijn veel meer factoren die meespelen bij het succes van het informatiesysteem. Wanneer wij dit willen ondervangen, met behulp van een (uitgebreide) ceteris paribus clausule, hoe vinden wij dan testgevallen die hieraan voldoen?

Naast de hierboven beschreven problemen, stipt prof. Oppelland nog enkele andere problemen aan, waar de wetenschappelijk onderzoeker (op het gebied van informatiesystemen) mee te maken krijgt. Een hiervan is het probleem van communicatie. Het feit dat wij geleerd hebben een zonnebloem "geel" te noemen, betekent niet dat wij daadwerkelijk dezelfde kleur zien. Een tweede probleem is de verwarring van statistische correlatie met de aanwezigheid van een causaal verband.

Met deze beperkingen in het achterhoofd, schetst prof. Oppelland "the State-of-the-Art" in onderzoek op het gebied van informatiesystemen. Prof. Oppelland beschrijft verschillende aspecten van de huidige consensus. Een hiervan zal hieronder besproken worden. Het betreft de invloed van gebruikersparticipatie op het succes van het informatiesysteem.

De gangbare opvatting op dit moment met betrekking tot de invloed van gebruikersparticipatie op de kwaliteit van het informatiesysteem luidt als volgt:
- gebruikers zullen geneigd zijn te participeren:
  a. als het project hun persoonlijke situatie beïnvloedt;
  b. hun eerdere ervaringen met projectparticipatie positief zijn;
  c. zij vinden dat ze hier voldoende kennis voor hebben en;
  d. zij bereid zijn de hieruit voortvloeiende verantwoordelijkheid te dragen;
- gebruikersparticipatie zal leiden tot een beter systeem.

Prof. Oppelland wil deze relatie aan de hand van door hem geciteerd onderzoek enigszins nuanceren. Hij ziet deze positieve invloed alleen bestaan als de verwachtingen die de gebruikers van deze participatie hebben, uitkomen. Deze verwachtingen betreffen werkelijke invloed in besluitvorming.

Als laatste punt in zijn oratie tracht prof. Oppelland te komen tot een maatschappelijk verantwoorde aanpak van onderzoek naar informatiesystemen. Zo'n onderzoek moet leiden tot maatschappelijk nuttige kennis die voor iedereen toegankelijk is. Dit moet bijvoorbeeld leiden tot het ontwikkelen van "betere systemen" en de evaluatie van bestaande systemen. Het tweede aspect van het onderzoek van informatiesystemen betreft de bescheidenheid van de onderzoeker: zijn "objectieve" bevindingen kunnen morgen achterhaald zijn.

Eerste voordracht: Kwaliteit van informatiesystemen
Spreker: prof.drs. E. Velthuizen RA

In de inleiding van de voordracht geeft prof. Velthuizen aan, waarom kwaliteitsbeheersing van informatiesystemen belangrijk is geworden. Aan de ene kant wordt het werkingsgebied van de automatisering steeds groter en de structuur steeds complexer. Aan de andere kant neemt de afhankelijkheid van deze systemen toe. Een van de voorbeelden die de spreker geeft, is de afname van het chartale geld. Hierdoor wordt het object van de accountantscontrole "het geheel van informatiestromen", in plaats van "de waardenkringloop".

In het tweede deel van de voordracht, splitst professor Velthuizen het begrip kwaliteit van informatiesystemen op. Hij onderscheidt enerzijds kwaliteit van het systeem en anderzijds kwaliteit van het produkt: de informatie zelf. Het systeem kent een statisch aspect dat beoordeeld moet worden op transparantie. Hoe doorzichtig is de architectuur?

Een transparante architectuur moet bereikt worden met behulp van gelaagdheid en een modulaire opzet. Bij de bespreking van het dynamische aspect brengt de spreker ons naar de bekende eisen van betrouwbaarheid en continuïteit van het verwerkingsproces. Professor Velthuizen voegt hieraan effi-

ciency en effectiviteit van het proces toe. Hij beantwoordt de vraag of een goedkeurende accountantsverklaring tevens een goedkeuring van het geautomatiseerde informatiesysteem inhoudt, ontkennend.

De kwaliteit van het produkt (de informatie zelf) valt uiteen in semantische en syntactische kwaliteit. De inhoudelijke kwaliteit laat zich ook vertalen in termen van rationaliteit: bieden de gegevens alle informatie die objectief nodig is om een functie te kunnen uitoefenen. De spreker stelt de semantische kwaliteit ook afhankelijk van de inwerking op het specifieke individu en de bijdrage tot de (vaak ongestructureerde) besluitvorming. Deze kan zo van hetzelfde gegeven op ongelijke besluitvormingsniveaus geheel verschillend zijn. De syntactische kwaliteit betreft het psychisch effect van de presentatie op de ontvanger van de informatie: een grafiekje is vaak duidelijker dan een verhaal.

In het derde deel wordt ingegaan op de bewaking van de zojuist geschetste kwaliteitseisen. Hiertoe moet het begrip interne controle verruimd worden. Dit moet uitgebreid worden van controle op de volledigheid der opbrengsten naar zorg voor kwaliteit in informatiesystemen. Dit leidt bijvoorbeeld tot aandacht voor strategische, tactische en informele informatie, naast operationele en comptabele gegevens. In plaats van aandacht voor functiescheiding, moet de aandacht "organistisch" worden: hoe werken mensen samen in organisaties en hoe komt besluitvorming tot stand.

Omdat de kwaliteitsbewaking van geautomatiseerde informatiesystemen zo ingewikkeld wordt, is het specialisme van de EDP auditor ontstaan. Deze richt zich op een viertal gebieden, die de spreker aan de hand van checklists bespreekt. Deze punten zijn "de ontwikkeling en bouw", "de verwerking en exploitatie", "het onderhoud" en "het database-beheer".

Tweede voordracht: Betrouwbaarheid van informatiesystemen, een modelmatige benadering
Spreker: prof. W. Hartman RA

Prof. Hartman stelt dat het gebied van de inrichtingsleer een ontmoetingsplaats van verschillende disciplines is. Een gemeenschappelijke interesse van deze vakgebieden is de betrouwbaarheid van de gegevens waarvan ieder op een andere manier gebruik maakt. De bevordering van deze betrouwbaarheid kan vanuit verschillende hoeken bekeken worden. Hiertoe voert de spreker vijf modellen ten tonele.
Het organisatiemodel: betrouwbaarheid door statische structurering zoals functiescheiding.
Het procesmodel: de nadruk ligt hier op goede planning.
Het assurantiemodel: betrouwbaarheid door goed verzekeren tegen alles wat mis kan gaan.
Het juridische model: de risico's worden op acceptabele wijze tussen koper en verkoper verdeeld met behulp van een goed contract.
Het controlemodel: de accountant komt vooraf helpen bij inbouw van betrouwbaarheid bevorderende maatregelen.

Naar analogie van middeleeuwse riddersloten introduceert prof. Hartman hierna de "beveiligingsgordelstrategie". Zoals de ridder vroeger zijn gezin binnen hield in de "inner ward" van het kasteel, terwijl de horigen buiten moesten lopen, zo zal ook kritische informatie door meer beveiligingsgordels omgeven zijn.

Als laatste onderwerp van de voordracht brengt prof. Hartman enige twijfels naar voren die hij heeft ten aanzien van functiescheiding. De oude trits vindt hij achterhaald. Er wordt een nieuwe zesdeling geïntroduceerd (leiding, administratie, bewaring, ontwerpen, uitvoeren, controleren). Dit is een analysemiddel, waarbij vermengingen niet zonder meer desastreus zijn. Het is situatie-afhankelijk. Als voorbeeld geeft de spreker een kleinschalige automatiseringsorganisatie, waarbinnen vermengingen niet te voorkomen zijn.

Derde voordracht: Plaats en functie van de externe controle met betrekking tot moderne informatiesystemen: de reikwijdte van de accountantscontrole
Spreker: prof. D. Steeman RA

Prof. Steeman begint met de specifieke betekenis van het begrip externe controle in de jaarverslaggeving. Dit houdt in controle op de financiële verantwoording van een huishouding door iemand die van buiten die huishouding komt. Hiertoe dienen de informatiesystemen van die huishoudingen controleerbaar te zijn.

Bij het voortraject van de bouw van een informatiesysteem dienen vele belangen vertegenwoordigd te zijn. Evenals anderen (zoals in de oratie van prof. Oppelland besproken) is prof. Steeman van mening dat gebruikers meer bij de ontwikkeling van informatiesystemen betrokken moeten worden. Daarnaast vindt prof. Steeman dat ook de accountant zijn inbreng moet hebben. Dit leidt tot meer aandacht voor de controleerbaarheid van het systeem en daarmee tot hogere kwaliteit.

Prof. Steeman sluit in het vervolg van zijn voordracht aan bij opmerkingen van de vorige sprekers. Prof. Velthuizen zag graag de "mechanistische visie" van interne controle op basis van tegengestelde belangen, vervangen door een "organistische". Deze laatste visie kijkt naar de samenwerking van mensen in organisaties. Prof. Steeman kan zich nog voorstellen, dat de controle plaatsvindt binnen een groep die een bepaald administratief traject afwerkt, in plaats van in een aparte afdeling. Verder wil hij niet gaan. Er moet wel gecontroleerd worden. Prof. Hartman stelde dat de functiescheiding beschikken-bewaren-registreren achterhaald is. Prof. Steeman stelt dat wel degelijk functiescheiding gecreëerd kan worden, ook in moeilijke situaties, zoals in het beschreven geval van kleinschalige automatisering. De vraag is alleen of het altijd noodzakelijk is.

Het tweede punt in de laatste voordracht betreft de reikwijdte van de accountantscontrole. De spreker vindt dat een oordeel over de automatisering binnen een bedrijf niet automatisch begrepen is in een jaarrekeningcontrole. De EDP audit is bijvoorbeeld afhankelijk van de mate waarin systeemgericht gecontroleerd wordt. Bedoeld betrouwbaarheidsonderzoek is daarom meestal een bijzondere opdracht.

Discussieverslag

In de discussie die volgde op de voordrachten, kwamen nog enkele begripsverduidelijkingen naar voren. Prof. Hartman wil de kwaliteitseisen situatie-afhankelijk stellen. Kwaliteit kan volgens hem analoog aan het begrip gezondheid omschreven worden: Kwaliteit is datgene waar de gebruiker gezond bij blijft.
Prof. Steeman wil praktische kwaliteitsbeoordelingen laten resulteren in een "Kema-keur" voor software en het kwaliteitssysteem.

Prof. Steeman vult het begrip informele informatie anders in dan prof. Velthuizen. Hij acht informatie formeel als deze beschreven is en ingebracht in het informatiesysteem. Prof. Velthuizen acht een ander criterium van toepassing. Informatie is alleen formeel als de inhoud van het bericht past bij de functie van de verzender. Als de vestiaire juffrouw een bericht verzendt dat er een bom in de vestiaire ligt, is dit informele informatie. Als de veiligheidsbeambte dit doet, is de informatie formeel aangezien het verstrekken van dit soort informatie tot zijn normale taken behoort. Prof. Velthuizen spreekt in deze context over het circuit dat in de administratieve organisatie niet voorzien is.

Prof. Hartman betoogt met betrekking tot functiescheiding, dat een goede scheiding volgens de aloude trits niet mogelijk is omdat iedereen zijn functie probeert uit te breiden met beschikkende taken. Prof. Velthuizen ziet het belang van functiescheiding veranderen, omdat de invloed van de computer de mens terugdringt tot de fase van de eerste vastlegging. Prof. Steeman staat op het standpunt dat een goede functiescheiding basis is voor de accountantscontrole.

Epiloog

Het is interessant dat op een bijeenkomst als deze, tegenstellingen aan de orde komen die bestaan tussen registeraccountants, bijvoorbeeld met betrekking tot het begrip functiescheiding. Hopelijk worden deze tegenstellingen in de toekomst verder verduidelijkt.

Computer Control Guidelines
Canadian Institute of Chartered Accountants 1986, 197 blz.
door drs. D. de Kruif

Ruim vijftien jaar na de eerste editie van Computer Control Guidelines (CCG), uitgebracht onder auspiciën van het Canadian Institute of Chartered Accountants (CICA), is in 1986 de tweede editie verschenen.
In deze boekbespreking zal vooral een vergelijking tussen de beide edities worden gemaakt.

Vijftien jaar is in automatiseringsland een erg lange tijd, en men kan zich afvragen waarom het CICA niet eerder met een update van dit toch belangrijk geachte werk is gekomen.
Voor een deel is dit wellicht te verklaren, omdat het raamwerk dat in de editie van 1970 is geschetst, voor een belangrijk deel niet of nauwelijks is veranderd. Hier doel ik met name op de interne controledoelstellingen (control objectives) en de minimaal aan de interne controle te stellen eisen (minimum control standards).
Degenen die bekend zijn met de inhoud van de eerste editie weten dat deze als volgt was opgebouwd:
1. control areas;
2. control objectives (per "control area");
3. minimum control standards (per "control objectives");
4. control techniques (per "standard").

Volgens de schrijvers zijn het vooral de controletechnieken, die in de afgelopen vijftien jaar zijn veranderd als gevolg van de veranderingen in de (omgeving van de) informatiesystemen.

Zij vatten de laatstgenoemde veranderingen als volgt samen:
- increasing user responsibility and involvement in the design, acquisition, development and operation of information systems;
- integration of applications to form an entity information system capable of direct enquiry and update by users;
- increasing use of microcomputers, both independent of other systems and linked to entity databases;
- an increase in the complexity of applications;
- a move to on-line real time systems with a consequent loss of the traditional management trail;
- a greater variety of hardware configurations in entities, ranging from centralized to decentralized;
- a trend to total dependence of an entity on the integrity and continued availability of its information systems.

Als we in ogenschouw nemen dat de eerste editie voornamelijk georiënteerd was op batch processing, dan is het niet moeilijk om in te zien, dat de controletechnieken als gevolg van de hierboven geschetste veranderingen

aan herziening toe waren. Het is echter de kracht van de opzet van het boek, dat de algemene principes, in casu de "control objectives" en de "minimum control standards", zoals deze zijn onderkend in de eerste editie, nagenoeg ongewijzigd zijn gebleven.

In de eerste editie was gekozen voor een indeling van de hoofdstukken volgens de onderscheiden "control areas".
Per onderscheiden aandachtsgebied werden vervolgens de daarbij onderkende "control objectives, minimum control standards and control techniques" behandeld.
Deze aandachtsgebieden sloten redelijk aan bij de gebieden die de accountant/edp auditor tot zijn aandachtsgebieden zou moeten rekenen, en waren vrijwel geheel gericht op aspecten van interne controle in en rond een geautomatiseerde omgeving.

In de tweede editie is van deze indeling afgeweken, waarbij opvalt dat niet alleen over interne controle-aspecten wordt gesproken, maar ook over zaken als efficiency en effectiviteit.

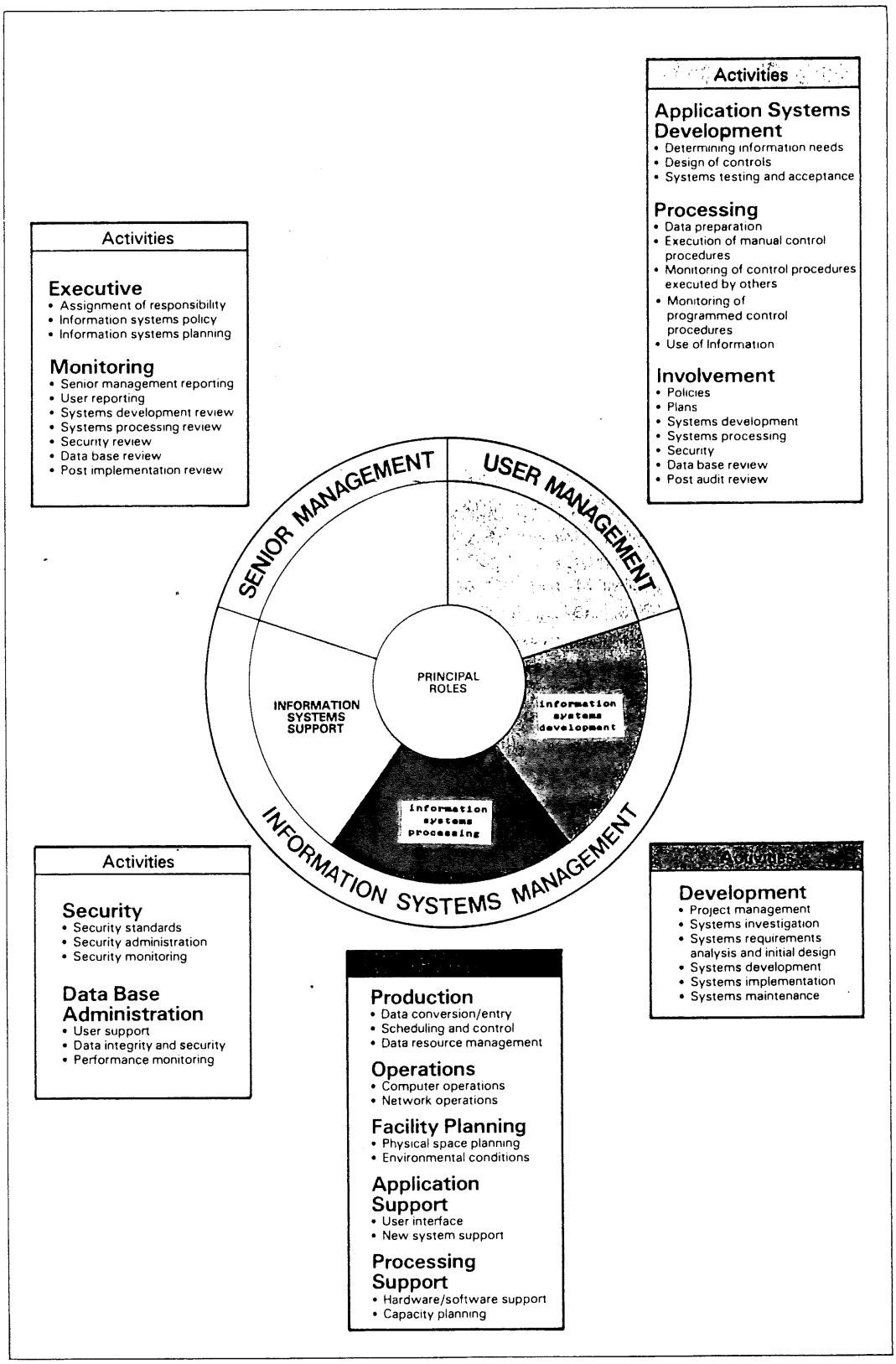
Men stelt, dat het stelsel van "Information systems control" een onderdeel vormt van het geheel van "internal control" in een organisatie.
Hierbij worden onderscheiden:
- General EDP controls: deze worden in de hoofdstukken 3, 4 en 5*) behandeld;
- Application controls: de application controls worden behandeld in de hoofdstukken 5*) en 6.

De hoofdstukken zijn als volgt:
1. information systems activities;
2. responsibility for control;
3. information systems development and acquisition;
4. information systems processing;
5. segregation of incompatible functions and security controls;
6. application controls;
7. distributed computing activities.

Hoofdstuk 1 vormt de basis van de behandeling van de onderwerpen in dit boek. Hierin wordt ingegaan op de te onderscheiden "roles, activities and functions" in de organisatie (zie figuur 1).

*) Zie toelichting auteur bij bespreking hoofdstuk 5.

Figuur 1: Principal roles and information systems activities



De hoofdstukken 2 tot en met 6 worden behandeld volgens de structuur, zoals deze aan het begin van deze bespreking is beschreven (control objectives, etc.).

In hoofdstuk 2 wordt de verantwoordelijkheid van het senior management voor de bouw en het onderhoud van efficiënte, effectieve en betrouwbare informatiesystemen belicht.

Hoofdstuk 3 behandelt zowel de eigen ontwikkeling van systemen, als de aanschaf van software-pakketten.

In hoofdstuk 4 worden drie activiteiten onderscheiden:
1. matching information processing to requirements;
2. controlling the use of information processing resources;
3. controlling day-to-day information processing activities.

Uit deze opsomming blijkt eens te meer, dat we te maken hebben met meer dan interne controle alleen.

Hoofdstuk 5 behandelt de onderwerpen functiescheidingen en security. Het apart behandelen van deze onderwerpen, vooral van functiescheidingen, is discutabel. De auteurs verdedigen deze methode door te stellen, dat deze onderwerpen gelden voor het gehele traject van de automatisering, en dat zij daarom beter apart behandeld kunnen worden.
Met een zelfde stelligheid zou men kunnen beweren, dat het per deelobject behandelen van de relevante functiescheidingen de overzichtelijkheid ten goede zou kunnen komen. Deze handelswijze is ook in de eerste editie van CCG gevolgd.

In hoofdstuk 6 wordt een onderscheid gemaakt in "user control procedures" en "application control procedures".
Met het eerstgenoemde worden bedoeld de manuale controlehandelingen door de gebruikers van applicaties.
Met het laatste wordt bedoeld de manuaal of automatisch uitgevoerde controles aan de hand van door de computer geproduceerde informatie.

In hoofdstuk 7 wordt vervolgens ingegaan op gedistribueerde gegevensverwerking. Hierbij wordt gesteld, dat de "control objectives and standards", zoals deze in de eerste zes hoofdstukken zijn behandeld, ook voor gedistribueerde gegevensverwerking gelden. Van de controletechnieken, die hier gebruikt kunnen worden, wordt een aanvullende opsomming gegeven. Hierbij wordt opgemerkt, dat deze technieken sterk afhankelijk zijn van de gebruikte configuratie. De nadruk zal (ook hier) liggen op de kosten/nutverhouding van de toe te passen controletechnieken.

Het boek eindigt met een verklarende woordenlijst (8 blz.) en evenals in de eerste editie, met een samenvattend overzicht van alle "control objectives, standards and techniques" per hoofdstuk (22 blz.).

Concluderend mogen wij stellen, dat het CICA er wederom in geslaagd is een boek samen te stellen, dat volgens een duidelijk concept is opgesteld, dat vrij gemakkelijk toegankelijk is en dat tevens (althans voorlopig) voldoende up to date is.

Men kan zich wel afvragen waarom het CICA van de indeling, zoals zij die in de eerste editie van CCG heeft gehanteerd, is afgeweken.
Zeker is wel, dat de term "control" in de tweede editie in een ruimere zin is opgevat dan in de eerste editie, namelijk het beheersen van geautomatiseerde informatiesystemen in algemene zin. Daarom is in de tweede editie ook aandacht gegeven aan zaken als efficiency en effectiviteit. Ook is er een grotere nadruk gelegd op de rol van het senior management.

Het boek draagt geen methode(n) aan op basis waarvan bijvoorbeeld een EDP audit gedaan zou kunnen worden. Er worden slechts richtlijnen gegeven, zoals de titel terecht weergeeft. Deze richtlijnen worden op een zodanige wijze weergegeven, dat het boek te gebruiken is als studiemateriaal, maar ook als een (globale) checklist.
In sommige gevallen, met name in het laatste hoofdstuk (netwerken) zijn de richtlijnen zeer summier, maar wellicht mag men van een boekwerk van deze omvang niet meer verwachten.

Tenslotte nog een opmerking betreffende een zinsnede uit het voorwoord van het boek, waar staat: "Computer Control Guidelines is not intended to be an educational tool and it is assumed that readers will be familiar with the fundamental elements of information systems and controls".
Wat het eerste deel betreft; hiermee ben ik het niet geheel eens. Al mag dit boek niet als leermiddel zijn bedoeld door het CICA, het zou mijns inziens wel als zodanig gebruikt moeten (blijven) worden. Deze stof behoort tot de bagage van elke accountant. Men zal echter wel, meer dan bij de vorige druk het geval was, met zorg de onderwerpen en (delen van) hoofdstukken moeten selecteren, omdat er een aantal zaken worden behandeld die voor de accountant van minder belang zijn.

Ten aanzien van het tweede deel van bovenstaand statement kennen wij een uitstekend alternatief, ook voor hen die nog weinig automatiseringskennis bezitten, namelijk de cursus BAIC (Basiskennis Automatisering en Interne Controle), die wordt verzorgd door KMG Klynveld EDP Audit Services.

Systeemsoftware, controleren of negeren?
Bespreking symposium Nederlands Genootschap voor Informatica, sectie EDP auditing, gehouden op 3 februari 1987
door mw. drs. A. Klaver

Voorwoord

In deze bespreking worden een aantal voordrachten behandeld, waarin het al dan niet controleren van systeemsoftware centraal staat. De meningen over het feit of dit al dan niet gewenst is lopen tussen de vakbroeders en -zusters in de accountancy nogal uiteen.

De eerste voordracht die hier besproken wordt, is van mevrouw M.E. van Biene. In tegenstelling tot veel van haar collega's is zij duidelijk voorstander van het controleren van systeemprogrammatuur. Zij vindt steun voor deze mening in gezaghebbende literatuur. De tweede spreker, prof. G. Nielen, gaat in op de vraag hoe diep men moet gaan bij het doorgronden van programmatuur. Deze voordracht is niet bedoeld voor het oplossen van een praktisch probleem. De voordracht is beschouwend van aard. De derde voordracht, door leden van de NGI werkgroep "Systeemprogrammatuur", behandelt een aanpak welke men in een praktisch geval kan hanteren, om systeemsoftware te controleren.

"Systeemprogrammatuur controleren!"
Mevrouw M.E. van Biene-Hershey

Mevrouw Van Biene stelt de noodzaak van het controleren van systeemsoftware ter discussie. Zij vraagt zich af of dit valt binnen de taakopdracht van de accountant, die een oordeel uit moet spreken over de getrouwheid van het beeld in de jaarrekening.
Voor het onderzoek naar de noodzaak van het controleren van systeemprogrammatuur, gaat zij te rade bij het "IFAC Handbook". Volgens mevrouw Van Biene stelt dit handboek duidelijk dat de interne controles binnen de geautomatiseerde omgeving onderzocht dienen te worden. De IFAC definieert in dat kader vijf onderzoeksgebieden, waarbij ook het gebied van de systeemprogrammatuur genoemd wordt.

De wijze waarop gecontroleerd moet worden is afhankelijk van een aantal zaken. Een belangrijk punt vindt mevrouw Van Biene hierbij de configuratie van het systeem. Deze vormt immers de basis voor het te controleren geheel.

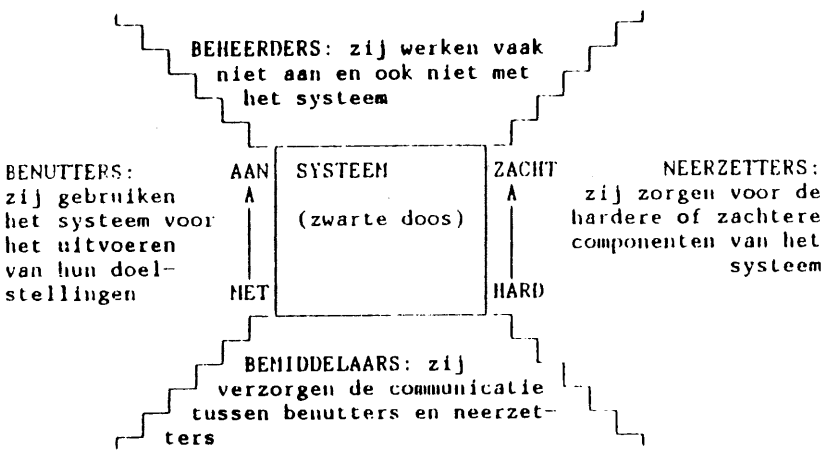
Hierna draagt mevrouw Van Biene enkele voorbeelden aan, om haar stelling te ondersteunen dat controle van systeemprogrammatuur noodzakelijk is. Het eerste punt betreft het feit dat de systeemprogrammatuur de functiescheiding weer tracht aan te brengen, die door de automatisering in eerste instantie ontkracht is. Het tweede aspect is dat van de autorisatie, die in

de systeemprogrammatuur eenduidig geregeld moet zijn. Er mag geen misverstand bestaan over de verdeling van bevoegdheden. Tevens moet de systeemprogrammatuur een vroegtijdig ontdekken van misbruik van bevoegdheden ondersteunen.
Mevrouw Van Biene sluit haar voordracht af met de volgende stelling:

> Het aansluiten van gegevens uit de computer op gegevens uit de organisatie, hetzij intern of extern, is geen bewijs dat de gegevens uit de computer een volledig beeld geven van het bedrijfsgebeuren, behalve als men een toereikend oordeel heeft kunnen vormen met betrekking tot de interne controle binnen de EDP omgeving.

"Systeemprogrammatuur negeren?"
Prof.dr.ir. G.C. Nielen

In deze enigszins filosofisch getinte voordracht, komt prof. Nielen langs twee wegen tot de conclusie, dat gebruikers zich niet kunnen veroorloven systeemprogrammatuur te negeren. De vraag die in dit symposium aan de orde is, luidt: "Moeten wij weten hoe iets werkt?" Prof. Nielen vraagt zich af: "Waarom willen wij weten hoe iets werkt?"
Om deze vraag te kunnen beantwoorden introduceert prof. Nielen een model, dat als volgt afgebeeld kan worden.



Figuur 1. Vier categorieën van personen betrokken bij een systeem, dat hierbij wordt weergegeven door een zwarte doos.

Welke van de genoemde "rollen" weet nu hoe het systeem werkt? Prof. Nielen geeft hierop als antwoord: "Geen enkele".

Volgens de spreker zijn er vier redenen, waarom iemand zou willen weten "hoe iets werkt":
1. men is nieuwsgierig;
2. het functionele beeld is niet stabiel;
3. niemand kan helpen als het fout gaat;
4. men heeft geen vertrouwen in "de neerzetters".

Het betoog wordt nu toegespitst op de situatie van een geautomatiseerd systeem. In deze situatie zijn vooral de tweede en de vierde reden van belang. Prof. Nielen gaat als eerste in op de vierde reden.

Het gebrek aan vertrouwen in de neerzetters berust op een ontoereikende communicatie tussen "benutters" en "neerzetters". De koop van een geautomatiseerd systeem is qua belang te vergelijken met de koop van een huis. De marktsituatie is echter niet vergelijkbaar: "bemiddelaars" zoals makelaars, notarissen en kadasters, zijn nauwelijks aanwezig.

De tweede reden, de afwezigheid van een stabiel functioneel beeld, nodigt uit tot een filosofisch uitstapje.
De spreker schetst hier een beeld, dat aansluit bij het model van de virtuele machine. Dit model houdt in dat het gezicht dat de machine toont afhankelijk is van de manier waarop er naar gekeken wordt. Voor de ingenieur bestaat een computer uit digitale poorten, voor de programmeur in basic bestaat hij uit een interpreter van basic statements. De grens tussen hardware en software vervaagt. Hardware en software zijn logisch equivalent. (A. Tanenbaum)

Analoog hieraan beschrijft prof. Nielen een functie, zoals deze zich voordoet op het te beschouwen niveau, als een "complexe functie". Door een niveau lager te gaan, treft men de verzameling "elementaire functies" aan die samen de "hogere" functie vormen. Zoals de begrippen "complexe functies" en "elementaire functies" afhankelijk zijn van het niveau dat beschouwd wordt, zo wordt in deze zienswijze ook het "weten hoe iets werkt" relatief. Weten hoe het werkt, houdt in: Eén niveau lager de elementaire functies kennen. De vraag: "Moeten wij weten hoe het computersysteem werkt?" gaat nu over in de vraag: "Hoe diep moeten wij graven in de functionele structuur?"

Wanneer het functionele beeld van een systeem volledig stabiel is, is er sprake van een formeel systeem. Een verdere interpretatie van de structuur heeft geen andere betekenis dan een virtuele: het is zoals je het wilt zien.

Gaat dit model van een formeel systeem nu op voor een gegevensverwerkend systeem? Dit moet ontkennend beantwoord worden, omdat alleen al de interpretatie van degene die het systeem beschouwt het beeld instabiel maakt.

Als laatste opmerking in zijn voordracht, doet prof. Nielen de suggestie (systeem)programmatuur uit te rusten met meta informatie. De systemen dienen zelfverklarend te worden.

Bespreking van de NGI-uitgave "Systeem-software, controleren of negeren?", uitgebracht door de NGI werkgroep "Systeemprogrammatuur" ter gelegenheid van het symposium op 3 februari 1987 van het Nederlands Genootschap voor Informatica, sectie EDP-auditing (ISBN 90-5005-011-5)
door mw. drs. A. Klaver

Doel

Het doel van de werkgroep "Systeemprogrammatuur" is te komen tot een evaluatie van getroffen maatregelen in systeem-software om juistheid, vertrouwelijkheid en beschikbaarheid van gegevens te garanderen. Hierbij wil de werkgroep niet uitgaan van een specifiek produkt of leverancier, maar tot een logische en objectieve benadering komen die bij alle systeemprogrammatuur gebruikt kan worden.

Benadering

Hiertoe kiest de werkgroep de benadering van de risico-analyse. Zij deelt hiertoe de systeem-software op in functies. Per functie kan vervolgens bekeken worden welke bedreigingen de gewenste juistheid, vertrouwelijkheid en beschikbaarheid van gegevens zouden kunnen aantasten. Het geschetste raamwerk moet bruikbaar zijn, onafhankelijk van leverancier en implementatie. Daarom worden de functionele componenten bekeken op een hoog abstractieniveau.

De werkgroep onderscheidt drie niveaus. Het laagste niveau, het "occurrence" niveau, betreft de feitelijke verschijningsvorm. Een voorbeeld hiervan is "het pakket IDMS/DB". Het tweede niveau wordt het "type" niveau genoemd. Het gaat hier om de rol die de software binnen de implementatie speelt. "IDMS/DB" behoort tot het type database management-systemen. Het hoogste abstractieniveau is dat van de functies van systeem-software met als hoofdfuncties transportverzorging, verwerkingsbesturing en gegevensbeheer. Daarnaast zijn ondersteunende functies te onderscheiden, te weten toegangsbeheer, componentenbeheer, cyclusbeheer en registratie. Deze ondersteunende functies bevatten maatregelen tegen bedreigingen ten aanzien van de hoofdfuncties. Per functie zijn de verantwoordelijkheden, activiteiten en bevoegdheden vastgelegd. Zo zal de hoofdfunctie verwerkingsbesturing bijvoorbeeld alleen jobs van geautoriseerde opdrachtgevers verwerken (verantwoordelijkheid), hiertoe de identiteit en bevoegdheden van opdrachtgevers (doen) vaststellen (activiteit) en eventueel een opdracht afwijzen (bevoegdheid).

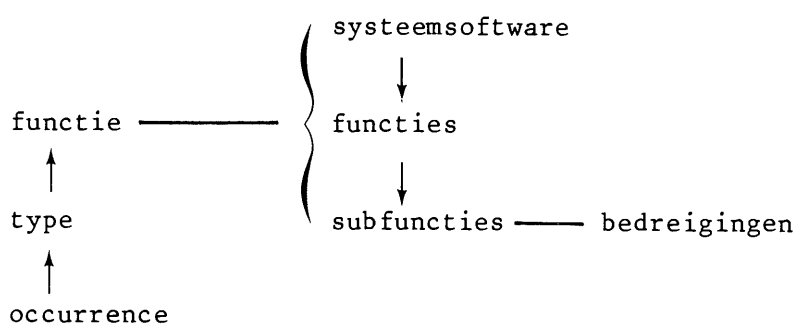
Audit aanpak

Het voorgaande moet de auditor voldoende houvast geven om de gewenste controle van een bepaalde systeemsoftware-component te kunnen uitvoeren. Hiertoe is de volgende stapsgewijze benadering aan te bevelen:
- inventariseer de specifieke implementaties;
- breng deze inventarisatie terug tot types systeemsoftware zoals het basic operating system en aanvullende programmatuur (bijvoorbeeld een database management systeem);
- kom van hieruit tot de basis van de aanpak: de implementatie-onafhankelijke functies;
- formuleer de concrete operationele controledoelstellingen per functie, in samenhang met de bedreigingen per functie;
- vertaal deze weer terug naar het niveau van de specifieke implementaties;
- voer de audit uit en stel rapportage samen.

Om de bedreigingen goed te kunnen inventariseren en vooral om de plaats waar deze optreden goed te kunnen preciseren moeten de relaties binnen het functioneel model duidelijk zijn. Hiertoe wordt het functioneel model van de systeem-software met behulp van PALET in kaart gebracht.

Enerzijds zijn er de relaties met datgene wat zich buiten de systeemsoftware bevindt en anderzijds zijn er relaties binnen de systeemgrenzen van de systeemsoftware zelf. Een voorbeeld van het eerste is de relatie van de transportverzorging met de gebruiker. De gebruiker toetst gegevens in, die door transportverzorging naar de centrale computer worden verstuurd. Van de relaties tussen de systeemsoftware functies onderling, worden die tussen hoofd- en ondersteunende functies bekeken. Zo zal de hoofdfunctie verwerkingsbesturing een aanvraag naar de ondersteunende functie componentenbeheer sturen voor processorcapaciteit. Componentenbeheer stelt deze ter beschikking.

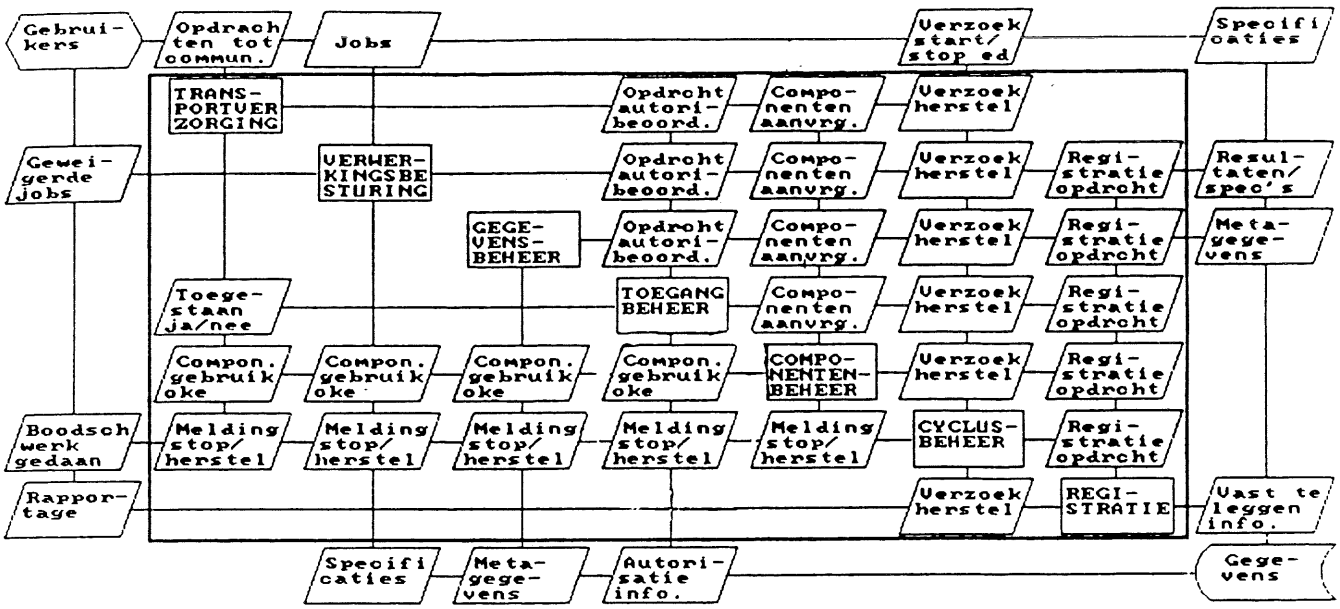
Het blijkt noodzakelijk de bedreigingen op een lager niveau vast te stellen. Deze zijn concreter te bepalen op subfunctieniveau. Hiertoe kan men een functie uitdiepen met behulp van subschermen binnen PALET. Het bovenstaande kan als volgt samengevat worden in schema:



Voorbeelden

De werkgroep geeft twee voorbeelden van de functionele decompositie. Eén hiervan (gegevensbeheer) zal hieronder kort worden besproken.
De functie van gegevensbeheer, zoals onder andere te vinden in database management systemen, is te verdelen in twee functionele niveaus. Naast fysiek beheer en beheer van de fysieke structuur is er sprake van logisch beheer. Dit houdt het beheer van de onderlinge verwantschappen in, gezien vanuit het gebruik dat van de gegevens gemaakt wordt. Omdat programmatuur en operator fouten maken is een vierde functie nodig, die deze fouten opvangt. Dit is het beheer van de functie gegevensbeheer. Dit is te zien als een niveau dat boven de overige drie functies staat. De inbreuken die op de doelstellingen van vertrouwelijkheid, juistheid en beschikbaarheid van gegevens gemaakt kunnen worden zijn te splitsen in opzettelijke handelingen, menselijke fouten en architectuurfouten. Een voorbeeld is te vinden in het deadlock-mechanisme. Dit kan expres uitgeschakeld worden (opzettelijke handeling), de gebruiker kan verkeerde parameters invoeren (menselijke fout) en er kan bijvoorbeeld een "deadly embrace" in de architectuur niet uitgesloten zijn (fout in de architectuur).

De relaties (gegevensstromen) tussen de functies kunnen overzichtelijk in een PALET-schema worden gevisualiseerd.



Systeemsoftware in een PALET-schema

Wij zien dus nu dat we onze te controleren omgeving (de systeemsoftware) op een overzichtelijke wijze hebben kunnen onderverdelen en weergeven.

Winter 1986/Lente 1987

TIJDSCHRIFTEN

door mw. D. Jansen Heijtmajer, mw. drs. A. Klaver en J.L.H. Kooijman

Nadat geruime tijd J.C. Boer naar aller tevredenheid deel heeft uitgemaakt van de rubrieksredactie van Tijdschriften - Han onze hartelijke dank daarvoor -, hebben wij mevrouw drs. Annelies Klaver bereid gevonden zitting te nemen in deze rubrieksredactie. Je enthousiasme is ons bekend, reden waarom wij met de anderen een vernieuwd élan verwachten.

Redactie Compact.

"Lastige klanten: Een interactioneel gezichtspunt"
door J. Hendriks
Management en Organisatie, januari 1987
door mw. drs. A. Klaver

Het artikel gaat in op het probleem van een vastlopend adviesproces. Dit kan natuurlijk veroorzaakt worden door een voor de hand liggende reden, namelijk een slecht advies. Er kan echter ook iets anders aan de hand zijn: de relatie zoals deze tussen klant en adviseur bestaat, is verstoord. Er is sprake van een "gevecht" en niet van een vruchtbare samenwerking.

Het samenspel tussen adviseur en klant laat zich beschrijven met behulp van een psychologisch model. Elk van beiden zendt volgens dit model drie signalen uit. Hij maakt duidelijk hoe hij zichzelf ziet (expressief aspect), hoe hij de ander ziet (attributief aspect) en wat hij van de ander wil (appelerend aspect). In een goed adviesproces zijn beide partijen het met elkaar eens. Dit is tot uitdrukking te brengen in het volgende schema:

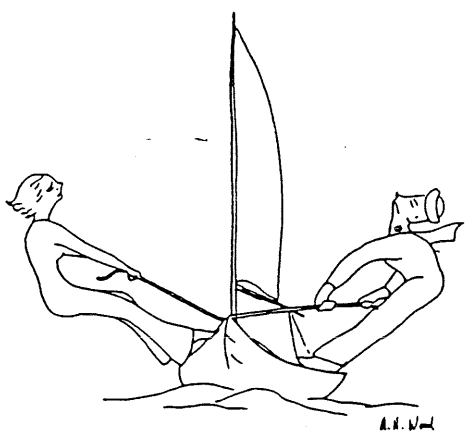
	klant	adviseur
Expressief aspect	"Ik heb een probleem"	"Ik ben deskundig"
Attributief aspect	"U bent deskundig"	"U heeft een probleem"
Appelerend aspect	"Help me, verander mijn situatie"	"Accepteer mijn leiding om eruit te komen"

Het op deze wijze analyseren van een relatie, wordt in de psychologie het kijken op betrekkingsniveau genoemd.
In een vastgelopen adviesproces kan de oorlog zich op één of meer van deze drie fronten afspelen. De klant zendt dan één of meer van de volgende signalen uit:
"Ik heb geen probleem";
"Ik betwijfel uw deskundigheid";
"Hier valt niets te veranderen".

Deze boodschap zendt hij niet rechtstreeks uit, maar op verscholen wijze. Hij kan dit bijvoorbeeld doen met lichaamstaal, zoals het geringschattend aankijken van de adviseur.

De adviseur moet in staat zijn deze aanvalssignalen te herkennen zodat hij er wat mee kan doen in plaats van ze (onbewust) te bestrijden.

In een normale adviessituatie vraagt de klant om advies. De adviseur vraagt hem het probleem uit te leggen, de klant doet dit, waarna de adviseur probeert een goed advies te geven. In een verstoorde adviesrelatie is het gedrag van beiden niet langer complementair. De situatie ontaardt in de zogenaamde "zeilbootsituatie". Beiden "trekken" even hard in tegengestelde richting, zodat er geen beweging meer in het adviesproces te krijgen is. Onderstaand plaatje geeft deze situatie weer.



De remedie die de schrijver van het artikel aanbeveelt tegen de zeilbootsituatie, wordt door hem de "tegenparadox" genoemd. De adviseur beëindigt zijn eigen bijdrage aan het gevecht, dat zich ontwikkeld heeft. Dit is paradoxaal, omdat het neerkomt op het accepteren van de weerstand van de klant tegen een adviesrelatie.

Het komt erop neer, dat de adviseur toegeeft aan de druk van cliënt. De situatie komt dan in beweging. De tegenparadox kan in milde vorm beoefend worden (accepteren en bevestigen van de signalen van de klant), maar ook in extreme vorm (het probleem voorschrijven). In het laatste geval "geeft" de adviseur "toe" dat het probleem hopeloos is en raadt de klant aan vooral in zijn foute gedrag te volharden. Dit doorbreekt het vastgelopen patroon en brengt de situatie in beweging.

Het artikel brengt de aandacht naar een aspect dat in de adviesrelatie misschien niet genoeg aandacht krijgt. Het bekijken van deze relatie op betrekkingsniveau, zoals hierboven beschreven, kan verhelderend werken.

"Detection of control deterioration using DSS"
William T. Tener
Computers & Security mei 1986
door mw. drs. A. Klaver

Het artikel bevat een pleidooi voor het gebruik van decision support systems bij interne audits. Deze audits worden vaak met zekere intervallen uitgevoerd. Tussentijdse veranderingen in het stelsel van interne controlemaatregelen worden niet of te laat gesignaleerd. Dit kan leiden tot een minder beheersbare bedrijfsvoering en brengt risico's voor het bedrijf met zich mee. Daarom dient gestreefd te worden naar auditing op meer continue basis. Een hulpmiddel hiervoor ziet de schrijver in het gebruik van decision support systems.

Een decision support system is een interactief geautomatiseerd systeem, dat een besluitvormer kan helpen bij het oplossen van semi-gestructureerde problemen. Hiervoor zijn drie componenten nodig: een databank die operationele bedrijfsgegevens bevat, de mogelijkheid om modellen te definiëren en een query-taal, om de databank te kunnen benaderen. De gebruiker kan met behulp van deze componenten de resultaten van alternatieve acties en de effecten van veranderingen in situaties doorrekenen.

Met dit gereedschap kan de accountant het bedrijfsgebeuren op continue basis kritisch volgen. Als zijn manipulaties met de data resultaten opleveren die zijn nieuwsgierigheid prikkelen, kan dit aanleiding zijn tot het uitvoeren van een audit.

Het artikel is geënt op de praktijk van een interne accountantsdienst. Dit werk wordt gekarakteriseerd door een gedetailleerder aanpak. Het artikel heeft bovendien betrekking op een Amerikaanse situatie. Dit heeft als consequentie dat de interne accountants zich bezighouden met taken die een Nederlands bedrijf bij de bedrijfsfuncties zelf zou leggen, zoals het verstrekken van management-informatie. Dit geeft meer gebruiksmogelijkheden voor DSS, dan een externe accountant hier voor zou zien.

De Amerikaanse schrijfstijl getuigt ook van een optimistische kijk: zonder problemen worden de bestanden van een bedrijf aan elkaar gekoppeld. Dit resulteert in één grote database, die gegevens bevat die de accountant voor zijn analyses nodig heeft. Verder heeft het bedrijf de beschikking over "management science models" (wiskundige modellen, om in gestructureerde probleemstellingen tot een optimale beslissing te komen). Dit alles heeft de accountant on-line tot zijn beschikking.

De conclusie met betrekking tot dit onderwerp is, dat de hier omschreven aanpak een interessante ontwikkeling blijkt, die de moeite waard is om te betrekken bij de ontwikkeling van de gereedschapskist van de accountant.

Certificering van software - een betrouwbare benadering
drs. F.H.M. Peters en drs. J.C.A.M. Ramaekers
door mw. D. Jansen Heijtmajer

In dit artikel wordt een methode besproken, die door beide schrijvers wordt gehanteerd bij het beoordelen van standaardpakketten.
Deze methode betreft een onderzoek en het op basis daarvan afgeven van een oordeel in de vorm van een certificaat.
Buiten een algemeen oordeel wordt in dit certificaat een overzicht gegeven van de interne controlemaatregelen opgenomen in het software-pakket. Tevens worden de additioneel te treffen maatregelen zowel in het pakket als in de organisatie aangegeven.
In dit opzicht verschillen de auteurs van mening met de heren Buné en De Lange, die in het artikel "Het beoordelen van standaard software-pakketten voor de financiële administratie op een microcomputer" stellen, dat het opnemen van een beschrijving van het in het pakket aangetroffen stelsel van maatregelen en procedures overbodig is.
De heren Peters en Ramaekers menen, dat een dergelijke beschrijving nodig is voor de uiteenzetting van de grondslag en motivering van de conclusies die tot het uiteindelijke oordeel hebben geleid. De beperkte geldigheidsduur van de mededeling wordt zowel door de heren Buné en De Lange als door de heren Peters en Ramaekers onderkend.
Auteurs stellen voor om belanghebbenden van het gecertificeerde pakket de toetsingsmiddelen en de analyse die de grondslag hebben gevormd voor de conclusies, te overhandigen, zodat zij zelf wellicht mogelijke modificaties op het pakket kunnen beoordelen. Eveneens moet regelmatig worden nagegaan in hoeverre de oorspronkelijke normen nog steeds relevant zijn.

Als belanghebbenden worden onderscheiden de gebruikers van de pakketten, de controlerend accountant en softwarehouses die pakketten ontwikkelen c.q. verkopen.
Bij gebruikers komt deze behoefte voornamelijk voort uit het streven naar beheersing van bedrijfsprocessen op basis van betrouwbare informatie.
De accountant wordt in toenemende mate geconfronteerd met software-pakketten, die voor de jaarrekening essentiële gegevens verwerken. Wanneer in het certificaat eveneens de noodzakelijke maatregelen in de organisatie worden beschreven kan de accountant nagaan of deze maatregelen zijns inziens voldoen en worden nageleefd.
De methode speelt in op de behoeften van gebruikers, hun accountant en softwarehouses en voldoet tevens aan het NIvRA-geschrift 26, waarin aanbevelingen worden gedaan voor mededelingen van de accountant over de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking.
Het totale onderzoek is bij de gehanteerde methode ingedeeld in onderstaande zes stappen:

1. Analyse van het functionele gebied waarin het software-pakket geacht wordt bepaalde doelstellingen te bereiken.
   Deze worden in relatie gebracht met andere functies in het bedrijf, om het pakket in de organisatie te kunnen plaatsen en eventuele interfaces te onderkennen.

2. Risico-analyse met behulp van algemene doelstellingen van interne controle, zoals juistheid, volledigheid, tijdigheid, geautoriseerdheid en reconstrueerbaarheid van informatie die gebruikt wordt voor besturing van de organisatie en voor het afleggen van verantwoording.
   In deze stap wordt het pakket verdeeld in opeenvolgende processen met bijbehorende gegevensverwerkende transacties en gegevensverzamelingen.
   Als de aard van de risico's is onderkend, worden deze beoordeeld op relevantie (importantie of belang).

3. Opstellen van concrete doelstellingen van interne controle gericht op het functionele gebied waarin het software-pakket wordt gebruikt.

4. Beschrijving van het pakket gezien vanuit interne controle-oogpunt en toetsing ervan aan de gestelde concrete interne controledoelstellingen.

   Hoewel de auteurs in principe de voorkeur hebben voor in het pakket opgenomen maatregelen, dient de accountant in het geval van onvoldoende maatregelen in het pakket zelf organisatorische procedures te ontwerpen.
   Het geheel moet dan leiden tot het bereiken van de gestelde interne controledoelstellingen.

5. Testen van het pakket aan de hand van een vooraf samengestelde goed gedocumenteerde testset om te constateren of het in werkelijkheid voldoet aan hetgeen is beschreven in de documentatie.
   De uitkomsten van de tests worden getoetst aan de voorspelling van de uitkomsten.
   Het testen dient te geschieden binnen een afgeschermde omgeving, waarbij de testresultaten niet kunnen worden verstoord door invloeden van buiten de te testen applicatie.

6. Opstellen van een rapport met conclusies. Hierbij wordt gebruik gemaakt van reeds tijdens de vorige onderzoekfasen opgebouwde rapportdelen.
   In de conclusie wordt melding gemaakt van de eventueel alsnog in te bouwen geprogrammeerde controles en van te nemen organisatorische maatregelen om tot een verantwoord gebruik van het pakket te komen.

Ter afsluiting wordt in het artikel nog een voorbeeld van een toepassing van de methode gegeven.

COMPACT is een uitgave van
KMG Klynveld EDP Audit Services

Winter 1986/Lente 1987

Automatisering Beveiliging Controle NIEUWS

door M.C. Duym, J.F.C. van Epen en drs. J. Kuipers

Automatisering

Netwerknieuws

X.400 is een standaard voor het elektronisch berichtenverkeer. Het hoort thuis in de toepassingslaag (ook wel applicatielaag) van het OSI-netwerk model. In de loop van 1987 zullen alle computerleveranciers deze standaard gaan ondersteunen volgens een onderzoek van Bakkenist Spits en Co. De Franse PTT zal als eerste dit jaar een op deze standaard gebaseerd publiek netwerk exploiteren.

Een andere standaard voor de toepassingslaag die in 1987 een verdere stap naar volwassenheid zal maken is MAP 3.0, een protocol voor fabriekscommunicatie. De beschrijving van deze versie, die volledig OSI-compatibel is, zal deze zomer beschikbaar komen. Demonstraties met deze versie worden echter pas in 1988 verwacht.

Dichter bij huis, zijn op netwerkgebied eind 1986 ook een tweetal interessante overeenkomsten afgesloten. De eerste betreft die tussen de Stichting Uniforme Artikelcodering (UAC) en General Electronic Information Services (GEIS). De tweede tussen Binnenlandse Zaken (BiZa), Gemeentelijke Bevolkingsadministratie (GBA) en eveneens GEIS.

In de Stichting UAC zijn voornamelijk leveranciers en afnemers in de levensmiddelenbranche vertegenwoordigd. Met de toepassingslaag implementatie onder de naam Transcom kunnen de aangeslotenen via elektronische weg bestellingen, retouren, facturen, artikel- en adresinformatie uitwisselen. Op basis van de gesloten overeenkomst zullen de faciliteiten van de andere zes lagen van het OSI-model via de GEIS-transnetdienst aan de Transcom-gebruikers ter beschikking worden gesteld. De transnetdienst maakt op zich weer onderdeel uit van het Mark III-netwerk van GEIS.

De overeenkomst met BiZa betreft het proefnetwerk voor een studie naar de volledige automatisering van de GBA. Gebruik wordt gemaakt van het Mark III-netwerk. Doorslaggevend in de keuze zouden geweest zijn de beveiligingsfaciliteiten van het netwerk (encryptie) en het voldoen aan de X.400 standaard.

Naar aanleiding van artikelen in Computable d.d. 14 november 1986, 5 december 1986, 12 december 1986, Automatisering Gids 26 november 1986 en 21 januari 1987.

Schaalvergroting

PCM-fusie Siemens en BASF

In een per 1 januari 1987 opgerichte gemeenschappelijke dochteronderneming van BASF en Siemens hebben deze hun activiteiten op het gebied van IBM-compatible mainframes ondergebracht.

De nieuwe onderneming zal de grootste PCM'er (Program Compatible Manufacturer) zijn binnen Europa. Voorlopig zullen zowel de Fujitsu-computers die Siemens verkocht en de Hitachi-computers die Basf verkocht geleverd worden. Het Siemens/Fujitsu-computermodel 7500 met het BS2000 besturingssysteem staat buiten de fusie.

Verwacht wordt, dat de onderneming in de toekomst alleen de Hitachi-lijn zal blijven voeren.

Naar aanleiding van artikel in Computable d.d. 14 november 1986.

Samenwerking Bull, Honeywell en Nec

Bijna alle activiteiten van de Honeywell Information Systems division zullen worden verkocht aan een begin 1987 op te richten onderneming. In deze onderneming zullen in eerste instantie Bull en Honeywell voor 42,5 procent deelnemen en Nec voor 15 procent. Het gesloten contract geeft Bull de mogelijkheid nog 22,6 procent van het Honeywell-belang over te nemen. Nadere informatie over gevolgen voor de gevoerde produkten is nog niet bekend.

Naar aanleiding van artikel in Computable d.d. 12 december 1986.

Uccel verwerft onder meer eigendom ACF2

SKK, de bouwer van het toegangsbeveiligingspakket ACF2 en houder van de internationale marketing-rechten ervan, alsmede de houders van de verkooprechten in de VS, de Cambridge Systems Group, zijn door Uccel overgenomen. Uccel is een belangrijke leverancier voor software op het gebied van produktiviteitsverbetering van de automatiseringsproduktie binnen IBM mainframe-omgevingen.

Naast de twee genoemde bedrijven werden er nog meer overgenomen, waardoor Uccels marktpositie zeer sterk is geworden. Mededelingen over afstemming of integratie van pakketten zijn niet gegeven.

Naar aanleiding van artikel in Computable d.d. 9 januari 1987.

Winter 1986/Lente 1987

CGE en ITT samen in Alcatel N.V.

De verwachte en, gezien de toename van research-kosten, onontkoombare samenwerkingsvormen tussen leveranciers van telecommunicatie-apparatuur heeft zich verder voortgezet. Net op de valreep van 1986 werd Alcatel N.V. opgericht. Het is een gezamenlijke onderneming van het Franse Staatsbedrijf Compagnie Général d'Electricité (CGE) en de Amerikaanse International Telephone & Telegraph Corporation (ITT).

Deze verdergaande schaalvergroting met deelname van staatsbedrijven, zal hopelijk als gevolg hebben, dat de standaardisatie op telecommunicatiegebied de zo noodzakelijke duw in de rug krijgt.

Naar aanleiding van artikel in NRC Handelsblad d.d. 8 januari 1987.

Beveiliging

Modem met terugbelfaciliteiten

In het maartnummer van het personal computer magazine Byte wordt melding gemaakt van een modem met terugbelfaciliteiten. Dit "modem" kan ook worden gebruikt voor het vanaf afstand inschakelen van apparatuur.

De beller maakt zich bekend met zijn telefoonnnumer. Dit nummer wordt door het modem opgezocht in het CMOS RAM-geheugen. Is het nummer bekend, dan wordt teruggebeld en om een password gevraagd. Na een aantal mislukte password-pogingen wordt het nummer uit het geheugen verwijderd.

Het modem is gezien de gehanteerde Bell 212A standaard niet geschikt voor de Nederlandse markt. Toch wilden wij als redactie de aandacht op dit nieuws vestigen. Want voor zover ons bekend is dit de eerste maal dat geen afzonderlijke dial-back-apparatuur nodig is om de kieslijnen te bewaken.

Betaaldiskette

Gebruik

Begin 1986 zijn een aantal grote banken op de markt gekomen met de "betaaldiskette" of "betaalschijf". Met het betaaldisketteprogramma kunnen betaalopdrachten op een 5 1/4 inch diskette worden weggeschreven.

De diskettes met betaalopdrachten kunnen door de Bank Giro Centrale (BGC) worden verwerkt. De BGC verwerkt een diskette alleen indien deze vergezeld is van een geldig geleideformulier. Het geleideformulier vermeldt het totaalbedrag, aantal opdrachten en optioneel een controletelling van de rekeningnummers, alsmede de handtekening van de procuratiehouder.

Op één diskette kunnen maximaal 800 (binnenlandse) betaalopdrachten met een totaalbedrag van 10 miljoen gulden worden aangeleverd. De diskette is met name bedoeld voor de gevallen waarbij vanuit de crediteurenmodule geen betaaltape of diskette kan worden aangemaakt.

De "betaaldiskette" is een op zich zelf staand produkt en zal vooral in het midden- en kleinbedrijf worden aangetroffen, hoewel ook grote bedrijven deze manier van betalen gebruiken.
Eigenlijk is het aanleveren van betaalopdrachten op diskettes niet nieuw.

Nieuw is dat het aanmaken van diskettes plaatsvindt buiten het traditionele rekencentrum. Het programma werkt namelijk als zelfstandige toepassing op een PC.

Als voordeel van de betaalschijf wordt genoemd dat het aanmaken van betaalopdrachten sneller gaat dan het uitschrijven of uittypen van opdrachten. Daar komt bij dat de individuele opdrachten elk afzonderlijk dienen te worden getekend terwijl bij de betaaldiskette alleen het geleideformulier wordt ondertekend.

Tot het moment van definitief maken van de diskette kunnen met het invoerprogramma wijzigingen worden aangebracht in reeds eerder ingebrachte opdrachten. Het definitief maken van de opdrachten bestaat uit het berekenen van de (controle)totalen en het afdrukken van een controlelijst waarop alle opdrachten staan vermeld.

Risico's

Functioneel verschilt de betaaldiskette niet van opdrachtformulieren of magneetbanden (betaaltapes). Het kenmerkende van een betaaldiskette is de grote eenvoud waarmee wijzigingen in de betaalopdrachten kunnen worden aangebracht nadat de controlelijst is afgedrukt. Dit is de reden waarom wij in dit artikel aandacht besteden aan de betaaldiskette.

Met een tekstverwerker, die veelal op personal computers voorkomt, of een eenvoudig BASIC programma kan het bestand met betaalopdrachten rechtstreeks worden gewijzigd. Het is bijvoorbeeld relatief eenvoudig verschuivingen tussen opdrachten te realiseren zonder dat het totaalbedrag of de controletellingen, die op het geleideformulier moeten worden aangegeven, aangepast hoeven te worden.

In vergelijking met het betalen per computertape of optisch leesbaar formulier zal de noodzaak tot het uitvoeren van controle op het traject dat volgt op het aanmaken van opdrachten en het ondertekenen van het geleideformulier toenemen. Immers steeds meer mensen kunnen omgaan met PC's, die veelal vrij toegankelijk zijn, dit in tegenstelling tot een mainframe-computer.

Gebruik van betaaldiskettes vereist daarom procedurele maatregelen gericht op het voorkomen van ongeautoriseerde wijzigingen.

Maatregelen

Hieronder worden enkele maatregelen genoemd gericht op de beheersing van het betalen per betaaldiskette.

Vanwege de mogelijkheid tot verschuiven van bedragen tussen rekeningnummers verdient het aanbeveling de betalingen aan personeelsleden te scheiden van betalingen aan crediteuren. Omdat de BGC geen controle uitvoert op de juistheid van de combinatie tussen naam, bedrag en bankrekeningnummer zal een

fout rekeningnummer en ditto bedrag niet herkend worden en leiden tot uitbetaling aan een verkeerde begunstigde. Het is daarom belangrijk nadruk te leggen op de controle van het rekeningnummer en het daarbij behorende bedrag.

Na het aanmaken van de diskette met opdrachten dient de definitieve betaallijst (de lijst met de betaalopdrachten die op de diskette staan) ondertekend te worden door degene die de opdrachten heeft aangemaakt, om aan te geven dat de betaaldiskette de definitieve opdrachten bevat.

De diskette dient direct na het definitief maken van de opdrachten aan de procuratiehouder te worden overhandigd. De procuratiehouder geeft door ondertekening van het geleideformulier aan dat de bank de opdrachten mag laten uitvoeren door de BGC.

Het verdient aanbeveling de blanco geleideformulieren door de procuratiehouder in een afgesloten ruimte te laten bewaren.
De procuratiehouder zal er zeker van willen zijn dat de inhoud van de lijst met betaalopdrachten overeenstemt met de inhoud van de diskette. Dit kan hij controleren door zelfstandig een afdruk te maken van het bestand met betaalopdrachten.

Voor het afdrukken kan bijvoorbeeld gebruik worden gemaakt van een tekstverwerker of van een daarvoor beschikbaar commando van het besturingssysteem van de PC. Bij gebruik van MS-DOS is dit commando bijvoorbeeld COPY "bestandsnaam" PRN. Deze afdruk wordt nu gecontroleerd met de definitieve betaallijst en de bijhorende facturen.

Na het ondertekenen van het geleideformulier dient de procuratiehouder ervoor te zorgen dat een onbevoegde niet over de diskette en het geleideformulier kan beschikken. De procuratiehouder zal dus zorgen voor een goede postprocedure. Voor het geval dat de verwerking van de betaaldiskette door de BGC problemen geeft wordt in het geleideformulier een contactpersoon opgegeven, die beslist over de eventuele verdere verwerking.

Het is ongewenst dat degene die de betaalopdrachten aanmaakt aangewezen wordt als contactpersoon met de BGC. Klachten of storingen dienen bij een onafhankelijke contactpersoon te worden gemeld.

Voor het geval de betaaldiskette door beschadigingen niet verwerkt kan worden, dient men te beschikken over een kopiediskette om alsnog tijdige uitvoering van opdrachten mogelijk te maken. Het beste kan deze kopie door de procuratiehouder worden aangemaakt, na goedkeuring van de betalingsopdrachten. Deze kopie moet in een beveiligde ruimte worden bewaard totdat de betalingsopdracht is uitgevoerd.

Regelmatig dient de juiste uitvoering van opdrachten gecontroleerd te worden door het dagafschrift van de bank af te stemmen met de definitieve betaallijst. Een functionaris die niet betrokken is bij het aanmaken of on-

dertekenen van betaalopdrachten dient dit te controleren. Om deze controle mogelijk te maken dient de bank te voorzien in gedetailleerde dagafschriften. Het is daarom niet wenselijk met de bank overeen te komen dat op het dagafschrift alleen het totaalbedrag en de controletellingen zullen worden vermeld.

Conclusie

Betaaldiskettes zijn geen nieuw produkt, maar worden wel steeds vaker toegepast. De diskette met betaalopdrachten kan met een tekstverwerker eenvoudig worden aangepast.

Het op zichzelf staand gebruik van betaaldiskettes vereist goede procedures gericht op het voorkomen van ongeautoriseerde wijzigingen van de opdrachten.

De accountant zal bij de beoordeling van het stelsel van interne controle deze procedures inzake geautomatiseerde betalingen moeten beoordelen. Een hulpmiddel hierbij is de KKC-controlelijst met "Attentiepunten inzake geautomatiseerde betalingen".

Naschrift redactie

Binnen het interbancaire overleg is deze problematiek onderkend. Met behulp van het project authenticiteitscontrole wordt beoogd te komen tot maatregelen met behulp van cryptografische technieken om een eenduidige overdracht van verantwoordelijkheid tussen de procuratiehouder en de bank mogelijk te maken.
Thans ontbreekt deze mogelijkheid, hetgeen als een leemte kan worden gekenschetst. Hierbij gevoegd de eenvoudige fout- en manipulatiemogelijkheden van PC's, is terughoudendheid bij het geven van een oordeel geboden.

Controle

Certificering van software

Aanleiding voor de behandeling van dit onderwerp is het voorpagina-artikel in Computable van 16 januari 1987 met de titel "Commerciële aanpak van software-keuring".
Dit artikel maakt melding van de plannen van een systeemhuis tot oprichting van een dochteronderneming met als doelstelling het certificeren van programmatuur, zowel standaardpakketten als bedrijfsspecifieke applicaties. Gekozen is voor het onderbrengen van de keuringsactiviteiten in een afzonderlijke dochteronderneming teneinde, volgens het bericht, de onafhankelijkheid van de keuring te garanderen. De directeur van het systeemhuis stelt in het genoemde artikel: "Het is onze bedoeling daarmee een positie in te nemen als accountant in de software-markt en produkten te testen op de door de leverancier verstrekte specificaties. ...."

Voor het tijdschrift Computable is deze ontwikkeling reden geweest voor een redactioneel commentaar. De redactie wijst op de behoefte van de markt naar een kwaliteitsmerk. Voor vele consumentenprodukten bestaat een kwaliteitskeuring al langer, maar ook voor software zijn inmiddels in Europees verband reeds een aantal onafhankelijke keuringscentra aangewezen.
Opgemerkt wordt dat het predicaat "onafhankelijk", ook in het licht van de eerder genoemde plannen, beter tussen aanhalingstekens kan worden geplaatst.

In het kader van onze rubriek is het van belang na te gaan in hoeverre deze vorm van certificering van belang is voor de controlerend accountant. Met andere woorden: Kan de accountant aan een dergelijk certificaat enige zekerheid ontlenen?
Ons inziens niet. Want het certificaat houdt slechts in dat, en nu citeren wij het genoemde artikel, "aan de opdrachtgever de zekerheid wordt gegeven, dat de door hem zelf geformuleerde specificaties goed zijn ingevuld".
Geen garanties worden gegeven dat de gekeurde software of de daaraan ten grondslag liggende ontwerpen voldoen aan de daaraan te stellen eisen.
Een slecht systeem, ontstaan als gevolg van een slecht ontwerp, wordt derhalve gecertificeerd!

In dezelfde maand, waarin genoemd artikel verscheen, zagen meerdere publicaties over software-certificering het daglicht. Dit schetst onder meer de behoefte eraan.
Eén daarvan is te vinden in De Accountant nr. 5 (januari 1987) onder de titel "Certificering van software - een betrouwbare benadering". Deze publicatie is overigens een reactie op eerdere in dit kader verschenen artikelen in hetzelfde tijdschrift.
Wij lezen hierin een opvatting over software-certificering die ons inziens beter aansluit op de controlewerkzaamheden van de accountant.

De schrijvers (drs. F.H.M. Peters en drs. J.C.A.M. Ramaekers) stellen: "Het af te geven certificaat bevat een oordeel over de betrouwbaarheid van de informatieverzorging door de applicatie. Bedacht moet worden dat betrouwbare pakketten een noodzakelijke, doch geen voldoende voorwaarde zijn voor een betrouwbare informatievoorziening. De kwaliteit van de organisatie rond de applicatie is hier mede van belang."
Hun logische gevolgtrekking is derhalve dat een af te geven mededeling bij een software-pakket tevens de eisen dient te bevatten die aan de organisatie dienen te worden gesteld. De accountant kan dan nagaan of genomen maatregelen zijns inziens voldoende zijn en worden nageleefd.
Zij merken elders in hun verhandeling op, dat ook het besturingssysteem, waaronder de applicatie wordt verwerkt, van belang kan zijn voor het certificaat. Indien bijvoorbeeld het besturingssysteem bepaalde beveiligingen regelt, behoeven deze niet nogmaals in de applicatie te worden opgenomen, Voorwaarde is dan wel dat de combinatie applicatie/besturingssysteem gehandhaafd blijft.

Een advies, dat ons inziens bijdraagt tot de langere bruikbaarheid van het certificaat, is dit vergezeld te doen gaan van de toetsingsmiddelen en de analyse, die de grondslag hebben gevormd voor de conclusies, teneinde de gebruiker in ieder geval in staat te stellen toekomstige modificaties op het pakket zelf te beoordelen.

Vervolgens geven de schrijvers van het artikel een beoordelingsmethode voor software-pakketten, die raakvlakken heeft met de methodiek zoals deze binnen onze eigen organisatie wordt gehanteerd. Een aanpak derhalve, die leidt tot een certificaat van goede kwaliteit.

Zo zijn, vrijwel tegelijk, twee artikelen verschenen die eenzelfde behoefte als achtergrond hebben, namelijk het voorzien van software van een kwaliteitskeur, maar tot eindprodukten concluderen waaraan wel sterk uiteenlopende normen ten grondslag liggen.

Het systeemhuis heeft terecht een duidelijk gat in de markt onderkend en is daarin gesprongen, maar gezien de verschillende benaderingswijzen die thans ontstaan, lijkt het dringend gewenst dat in "informatieland" consensus wordt bereikt omtrent vereiste betekenis en inhoud van een software-keurmerk (zie inzake ontwikkelingen op dit terrein overigens het artikel van J.H. Urbanus in de Compact jubileum-uitgave "24 over EDP-auditing").

ONDERWIJS

Inleiding

De jaarrekeningcontroles gericht op 1986 lopen ten einde, waardoor de aandacht weer meer wordt gericht op andere c.q. toekomstige aspecten. Daartoe behoren onder andere het volgen van cursussen om enerzijds kennis op te doen om bepaalde posities te verwerven anderzijds om kennis op te doen om bij te blijven.

In dit kader wordt in deze Compact uitvoerig ingegaan op wat KMG Klynveld EDP Audit Services op cursusgebied inzake automatisering en controle c.q. EDP audit te bieden heeft. In 1986 zijn de diverse cursusonderdelen op elkaar afgestemd en gestroomlijnd. Een eenduidige en logische benadering van de problematiek inzake automatisering en controle is verankerd in de cursussen. Hierna is het volgende opgenomen:

- beschrijving van de onderlinge samenhang van de cursussen gericht op de automatisering zoals die bij ondernemingen/cliënten kan voorkomen;
- gedetailleerdere beschrijving per cursus waarin opgenomen duur, inhoud, voor wie de cursus bestemd is en welke voorstudie vereist is om de cursus met vrucht te kunnen volgen;
- cursussen gericht op automatisering als hulpmiddel bij de uitvoering van interne c.q. externe accountantscontrolewerkzaamheden.

Beschrijving van de onderlinge samenhang van de cursussen Automatisering en Controle

De hieronder beschreven cursussen, richten zich op de automatisering zoals die bij bedrijven (cliënten) kan worden aangetroffen. Tussen 5 cursussen op dit gebied bestaat een duidelijke samenhang, terwijl er één (AKSO) gericht is op een specifieke organisatie.

Basiscursus Automatisering en Interne Controle (BAIC)

De Basiscursus Automatisering en Interne Controle richt zich op het bijbrengen van algemene kennis op het gebied van automatisering en interne controle. Op systematische wijze wordt het totale terrein van de automatisering verkend, waarbij de nadruk ligt op het onderkennen van de invloeden op de interne controle als gevolg van de diverse vormen van automatisering. Deze cursus bevat de basiskennis die gewenst is om de hierna volgende cursussen met vrucht te kunnen volgen. In die volgende cursussen worden de onderwerpen verder uitgediept.

Automatiseringsorganisatie (AUTO)

Deze cursus behandelt de interne controleproblematiek van een automatiseringsorganisatie. De organisatorische functies, besturingsprogrammatuur, procedures en voorschriften worden behandeld. Daarnaast wordt vanuit gedefinieerde controledoelstellingen nagegaan wat de bedreigingen kunnen zijn - en welke compenserende maatregelen kunnen worden genomen - indien de organisatie niet aan de gestelde eisen voldoet.

Cursus Aanpak Systeembeoordeling en Accountantscontrole (CASA)

De cursus CASA gaat nader in op het beoordelen van het geautomatiseerde informatiesysteem. Beantwoord wordt de vraag: waar zijn welke controles noodzakelijk en hoe wordt hierin in het onderhavige systeem voorzien? De cursus toont tevens waar "blinde vlekken" voor de systeembeoordelaar kunnen ontstaan, doordat controles niet in de applicatie zitten, doch beïnvloed worden door controles in de automatiseringsorganisatie en de systeem-software. Voorts behandelt de cursus de invloed van de bevindingen van de beoordeling op de aanpak van de accountantscontrole.

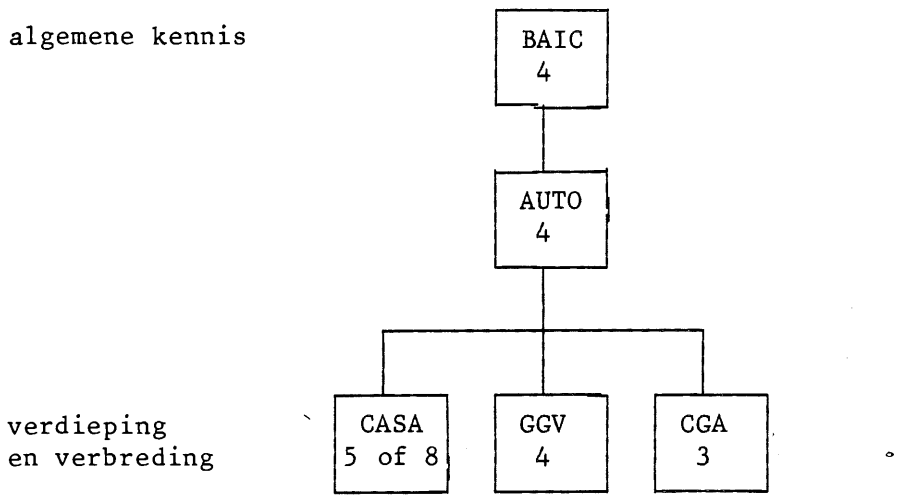
Geïntegreerde Gegevensverwerking (GGV)

De cursus gaat in op wat onder geïntegreerde gegevensverwerking moet worden verstaan. In detail wordt - vanuit een ideale situatie - gedemonstreerd hoe en wanneer standaard systeemprogrammatuur voor gegevensbanken en interactieve verwerking controlefuncties van de organisatie en applicatieprogrammatuur kunnen overnemen of beïnvloeden. Tevens wordt aangegeven wat de invloed op de interne controle is bij afwezigheid van de desbetreffende systeemprogrammatuur. Voorts wordt ingegaan op organisatorische consequenties bij geïntegreerde gegevensverwerking.

Cursus Gedistribueerde Automatisering (CGA)

Deze cursus gaat in op de interne controle- en beveiligingsaspecten van de verschillende vormen van gedistribueerde automatisering. Er vindt een bespreking plaats van de organisatorische functies, de apparatuur, systeemprogrammatuur, procedures en voorschriften in die situatie. De cursist is na afloop van de cursus in staat de problemen op het gebied van interne controle te onderkennen in geval van gedistribueerde automatisering.

De samenhang van de cursussen is schematisch als volgt weer te geven. De cijfers stellen de cursusduur in dagen voor.



Automatisering in een kleinschalige omgeving (AKSO)

De cursus automatisering in een kleinschalige omgeving staat los van bovenstaande cursussen en is gericht op de interne en accountantscontrole-aspecten in een kleinschalige omgeving waar sprake is van automatisering. De controle-aspecten worden diepgaand behandeld en de cursus is bedoeld voor administrateurs en (aankomende) accountants die in een dergelijke omgeving werkzaam zijn.

Winter 1986/Lente 1987

Basiscursus Automatisering en Interne Controle (BAIC)

Cursusduur: 4 dagen

Inhoud

De cursus heeft ten doel de cursisten vertrouwd te maken met basisbegrippen op het gebied van automatisering en interne controle. Hierbij komen aan de orde de automatiseringsorganisatie, informatiesystemen, geïntegreerde gegevensverwerking en gedistribueerde automatisering.

Aan de orde komen de betrouwbaarheids- en continuïteitsaspecten van onder meer:

- functies in de:
  - . organisatie van de automatisering (ontwikkeling);
  - . automatiseringsorganisatie (rekencentrum).
- ontwikkeling van systemen/projecten;
- test-, acceptatie-, overdrachtsprocedure;
- systeem-software (operating system, bibliotheken);
- maatregelen binnen het rekencentrum:
  - . functiescheiding;
  - . back-up-procedures.
- geïntegreerde gegevensverwerking:
  - . organisatie van het gegevensbeheer;
  - . database;
  - . aard van de verwerking (on-line/real time etc.).
- gedistribueerde automatisering:
  - . soorten distributie;
  - . netwerken.

Bestemd voor

Administrateurs en functionarissen van (interne) accountantsdiensten en interne controle-afdelingen, alsmede voor systeemanalisten en systeemontwerpers.

Voorstudie

Geen.

Automatiseringsorganisatie (AUTO)

Cursusduur: 4 dagen.

Inhoud

De cursus beoogt de kennis van de automatiseringsorganisatie te verbreden en te verdiepen.

De cursus gaat in op:
- structuur en functies;
- interne controle-eisen;
- procedures;
- systeemprogrammatuur en apparatuur met betrekking tot:
  . transport van gegevens;
  . verwerking van gegevens;
  . opslag van gegevens.
- continuïteit, beveiliging;
- accounting:
  . doorberekening van de kosten; grondslag voor de facturering;
  . opstellen van een controleprogramma gericht op de volledigheid van de opbrengsten.

De deelnemer is na het volgen van de cursus in staat te onderkennen welke knelpunten met betrekking tot interne controle en beveiliging een automatiseringsorganisatie met zich mee brengt. De cursus biedt de basis voor het contact met specialisten (medewerkers van de automatiseringsafdelingen, EDP auditors, organisatie-adviseurs).

Bestemd voor

Interne controlefunctionarissen (bijvoorbeeld van een rekencentrum), (aankomend) accountants die fungeren in de interne en externe controlepraktijk, alsmede voor hen die zich verder wensen te ontwikkelen op het "EDP audit"-gebied.

Voorstudie

Geen.

Winter 1986/Lente 1987

Aanpak systeembeoordeling en accountantscontrole (CASA)

Cursusduur: 5 of 8 dagen.

Inhoud

De cursus beoogt de cursist de CASA-methode voor de aanpak van systeembeoordeling bij te brengen, die wordt toegepast om:
- de kwaliteit van de interne controle van een in belangrijke mate geautomatiseerd systeem van gegevensverwerking te kunnen beoordelen;

Voorts verschaft de cursus kennis en inzicht om:
- een doelmatige aanpak van accountantscontrole, al dan niet met behulp van de computer, op basis van het verrichte systeemonderzoek te kunnen vaststellen;
- op doelmatige wijze de mogelijkheden tot systeemonderzoek in het kader van de controle van de jaarrekening te kunnen bepalen en de resultaten ervan te gebruiken.

In deze cursus wordt voor de vastlegging van de administratieve organisatie gebruik gemaakt van het geautomatiseerde hulpmiddel PALET.

Bestemd voor

Degenen die werkzaam zijn in de interne en of accountantscontrole alsmede systeembeheerders aan gebruikerszijde.

Voorstudie

- Enkele syllabi;
- Informatie omtrent de casus.

Winter 1986/Lente 1987

Geïntegreerde gegevensverwerking (GGV)

Cursusduur: 4 dagen.

Inhoud

In de administratieve organisatie en accountantscontrole worden gebruikers en accountants in toenemende mate geconfronteerd met interactieve (on-line) gegevensverwerking met gebruikmaking van geïntegreerde gegevensverzamelingen. De interne controlemaatregelen kunnen daarbij worden verschoven naar standaard systeemprogrammatuur op het gebied van interactieve verwerking (on-line/real time) en gegevensbanken (databases).
Deze cursus beoogt deze materie doorzichtig te maken voor niet softwaretechnisch onderlegde gebruikers en accountants. Ook worden de gevaren en mogelijkheden aangegeven ten aanzien van de beheersbaarheid van gegevens en gegevensverwerking. Daartoe worden software-produkten als Data Dictionary/ Directory Systems behandeld vanuit het gezichtspunt van beheersbaarheid en functionaliteit en wordt aandacht besteed aan de organisatie in een dergelijke situatie.

Bestemd voor

Functionarissen belast met interne c.q. externe controle in situaties waar sprake is van geïntegreerde gegevensverwerking, bijvoorbeeld niet softwaretechnisch onderlegde gebruikers en accountants, alsmede voor (aankomend) EDP auditors.

Voorstudie

- Deel van hoofdstuk 3 van het boek Data Base & Accountant, derde druk;
- Casus-beschrijving.

Winter 1986/Lente 1987

Cursus Gedistribueerde Automatisering (CGA)

Cursusduur: 3 dagen.

Inhoud

De cursus richt zich op de verschillende vormen van "gedistribueerde automatisering" en de daarmee samenhangende controle en beveiligingsproblematiek.

Deze aspecten worden aan de orde gesteld ten aanzien van de volgende onderwerpen:
- netwerken met onder andere spreiding van intelligentie;
- systeemprogrammatuur;
- gegevens;

met de daarbij behorende organisatorische consequenties.
In deze cursus wordt gebruik gemaakt van een aangepaste versie van de casus die in AUTO wordt behandeld.

Bestemd voor

Interne controlefunctionarissen, (aankomende) accountants die fungeren in de interne c.q. externe accountantspraktijk, alsmede voor hen die zich verder wensen te ontwikkelen op "EDP audit"-gebied.
Kennis op het niveau van de cursussen BAIC en AUTO is noodzakelijk.

Voorstudie

De casus.

Winter 1986/Lente 1987

Automatisering in een kleinschalige omgeving (AKSO)

Cursusduur: 2 dagen.

Inhoud

Met de cursus wordt beoogd inzicht te geven in de invloed op de interne controle van automatisering in een kleinschalige omgeving. Daarnaast komt aan de orde de aanpak van de accountantscontrole die afhankelijk is van de aanwezige interne controle.

Enkele punten uit de inhoud:
- het begrip kleinschalige automatisering;
- aspecten van interne controle in het kader van automatisering in een kleinschalige omgeving;
- mogelijke benadering van de accountantscontrole: systeem- of gegevensgericht;
- gebruik van de automatisering door de accountant als hulpmiddel bij zijn controle;
- continuïteitsaspecten bij kleinschalige automatisering;
- geautomatiseerd betalingsverkeer.

Bestemd voor

Functionarissen werkzaam in een kleinschalige automatiseringsomgeving.

Voorstudie

De casus + 1 opgave.

Winter 1986/Lente 1987

Algemene informatie en reserveringsvoorwaarden

Alle open cursussen staan vermeld in de brochure
"Programma 87/88 cursussen"
Van iedere cursus bestaat ook een afzonderlijk leaflet.

- Alle open cursussen, waarvan de cursusdata in deze brochure zijn vermeld, worden gehouden onder voorbehoud van voldoende deelname.

- In de prijzen van de cursussen zijn niet begrepen de eventuele kosten van het verblijf en de maaltijden in het conferentie-oord, tenzij anders vermeld.
  De kosten van een dergelijk arrangement worden door de administratie van het conferentie-oord bij vertrek direct met de deelnemers verrekend.

- In het algemeen wordt de inschrijving één maand voor de datum van aanvang van de cursus gesloten.

- Bij annulering van de aanmelding binnen 14 dagen voor aanvang van de cursus zal 50% van de prijs in rekening worden gebracht.

- Voor kosten verbonden aan de annulering van reeds gereserveerde kamers geldt de regeling van het desbetreffende conferentie-oord.

- Na afloop van de cursus ontvangen de cursisten desgevraagd een certificaat van deelneming.

- U wordt verzocht voor iedere cursus een afzonderlijk aanmeldingsformulier te gebruiken.

Alle aanvullende brochures alsmede informatie kunt u krijgen bij

KMG Klynveld Kraayenhof & Co.
Bureau Opleidingen
Antwoordnummer 17414
1000 SN AMSTERDAM
Telefoon 020 - 546 1243

waar u kunt vragen naar Pien Schepel.

Automatisering als hulpmiddel voor uitvoering van (interne c.q. accountants)controlewerkzaamheden

De te verrichte werkzaamheden in dit kader kunnen onder andere als volgt worden geschetst:

1. het inventariseren, vastleggen en evalueren van de administratieve organisatie;
2. het verrichten van cijferbeoordelingen en cijfercontrole;
3. het bepalen en uitvoeren van deelwaarnemingen c.q. (wiskundige) steekproeven;
4. het vormen en bijhouden van dossiers.

Voornoemde werkzaamheden kunnen met betrekking tot "mainframe" en "micro" worden uitgevoerd:

Micro

Langzamerhand neemt de PC als controlehulpmiddel de overhand. Vandaar dat KMG Klynveld EDP Audit Services voor de microprodukten cursussen heeft ontwikkeld c.q. beschikbaar heeft om de aangegeven werkzaamheden met ondersteuning van de microcomputer efficiënt te kunnen verrichten.
Deze produkten en/of cursussen zijn:

0. MS-DOS: een ééndaagse cursus om inzicht te krijgen in de (beveiligings)mogelijkheden van het besturingssysteem MS-DOS. Onder dit besturingssysteem "draaien" de beschikbare pakketten.
1. Palet: een pakket om de AO en IC te inventariseren, vast te leggen en te evalueren. Bij dit pakket is een zodanige handleiding beschikbaar dat de kennis om er efficiënt mee om te kunnen gaan door middel van zelfstudie kan worden verkregen. Het is mogelijk om een demonstratie te arrangeren, duur circa ½ dag.
2. Multiplan: een spreadsheet-pakket waarvoor een cursus van twee dagen is ontwikkeld.
2/3. FAT/FMT: (file analysis tool) een pakket dat door KMG Klynveld EDP Audit Services is ontwikkeld om met name bestandsonderzoeken te kunnen verrichten. Hiervoor is een cursus van twee dagen ontwikkeld.
4. WISPR: een pakket ten behoeve van dossiervorming en waarvoor een cursus van één dag is ontwikkeld.

Mainframes

Voor het mainframe is één cursus beschikbaar. Het betreft hier een cursus gericht op het gebruik van het pakket "EDP Auditor". Met dit pakket kunnen cijferbeoordelingen, cijfercontroles alsmede bestandsonderzoeken worden verricht.

Volledigheidshalve wordt vermeld dat de sectie Support & Programming van EAS een groot aantal op maat toegesneden audit-programma's heeft vervaardigd en op afroep ontwikkelt.

Inlichtingen

Voor de informatie over de diverse produkten (onder andere aanschaf en demo's) kunt u zich verder wenden tot de EAS-sectie Support & Programming, telefoon 020 - 546 1214.

De diverse cursussen kunnen voor een relatief klein aantal deelnemers al dan niet in-house worden verzorgd. Voor informatie hieromtrent kunt u zich wenden tot Bureau Opleidingen.

Overzicht hoofdartikelen 1984/1986

nummer		
34	10e Jaargang (84/1), winter 1983/ lente 1984	
	- Accountant en elektronische informatie-verwerking	prof. D. Steeman
	- 100 + 50 - 20 = 80 ??????? De betekenis van concurrency control	A. van der Drift
	- De micro en de controlerende accountant	L. Straathof')
	- Opleiding risk manager	F.H. Horbeek (RB) H.A. Huyskens (RB)
35	11e Jaargang (84/2) zomer 1984	
	- Controls in systems using modern technology	W. List CA MBCS, (TMcL)
	- Het beoordelen van database-systemen	A. van der Drift')
	- Data dictionary systemen in relatie tot het gebruik van data base en data communicatie-technieken	H. Weerd')
	- Interactieve consolidatie op de microcomputer met behulp van het pakket Multiplan	drs. P.A.M. Diekman
36	11e Jaargang (84/3) herfst 1984	
	- Security management: from the past to the future	drs. H.C. Kocks
	- De organisatie rond een Systeem/38	H.J. Lijnes
	- Beveiligingsaspecten in netwerken: Theorie en Praktijk	ing. C.J.M. Gielen') en H. Weerd
37	11e Jaargang (85/1) winter 1984/1985	
	- Hoe betrouwbaar zijn onze computers?	A.W. Neisingh
	- Beveiliging in lokale netwerken	ing. H.A.J.M. Spape')
	- Basic groeit	J.E. de Bue
38	12e Jaargang (85/2) lente 1985	
	- "Capabilities, het wenkend perspectief", theorie, praktijk en toekomst van op capabilities gebaseerde computersystemen	H. Roos
	- Knowledge based systems: een stap vooruit in de beheersbaarheid van administratieve processen	A. van der Drift')
	- Vierde generatietalen	drs. J.E. Huizenga')
	- Informatie over (elektronische) informatie "Werken met een database"	D. Boom

Noot afkortingen

RB = Rabobank, leden werkgroep NGI en VBB
TMcL = KMG Thomson McLintock & Co UK
') = (geactualiseerd) in "24 over EDP-auditing" opgenomen

Winter 1986/Lente 1987

Nummer		
39	12e Jaargang (85/3) zomer/herfst 1985	
	- De overdrachtsprocedure is meer dan een gebruikerstest	J.C. Boer')
	- New technology and new risks in security and control: beveiligings-problematiek in POS en ATM systemen bij banken	A.W. Neisingh en H. Weerd
	- Documentatie van geautomatiseerde informatiesystemen en systeemonderzoeken; vragenlijsten	J.M. Verheul')
40	12e Jaargang (86/1) winter 1985/1986	
	- Schutz vor EDV-Kriminalität - ein Entschleierungsversuch	Max F. Bretscher (F)
	- Accountant - automatisering en continuïteit	H.C. Kocks')
	- Beoordeling betrouwbaarheid van een (geautomatiseerd) informatiesysteem: de CASA-methode	A.H.C. Koedijk')
	- Identification and Evaluation of Operating System Controls (using IBM's Multiple Virtual Storage (MVS) operating system as an example)	H. Weerd')
41	13e Jaargang (86/2) lente 1986	
	- Automatisering & Controle bij grootschalige organisaties	H.B. Moonen en J.A.W. Winterink')
	- Betrouwbaarheidsmaatregelen in relatie tot verwerkingstypologieën	J.G. de Vries')
	- Grenzen van de techniek, beperkingen van apparatuur en programmatuur	H. Roos
	- De Wet Persoonsregistraties, zijn structuur en zijn invloed op de organisatie	J.F.C. van Epen')
42	13e Jaargang (86/3) zomer 1986	
	- Beveiliging: automatiserings- of organisatieprobleem	drs. H.C. Kocks
	- Conversie, Compilatie uit literatuur	drs. J. Kuipers')
	- De microcomputer in de accountantscontrole	H. Veenman')

Noot afkortingen

F = KMG FIDES Treuhandgesellschaft (Zwitserland)
')= (geactualiseerd) in "24 over EDP-auditing" opgenomen