Klynveld Kraayenhof & Co.
Accountants

Automatisering en Controle-groep

COMPACT 84/1

Computer en Accountant

Nummer 34
10e/11e jaargang winter 1983/lente 1984

Internationaal KMG Klynveld Main Goerdeler

COMPACT

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

INHOUDSOPGAVE

nummer 34 10e/11e jaargang winter 1983/lente 1984

COMPACT

winter 1983/lente 1984

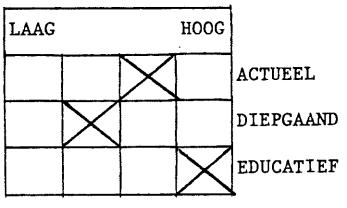
VAN DE REDACTIE

Voor u ligt een extra dik nummer.
De redactie heeft gemeend u het Overall-artikel van D. Steeman niet te mogen onthouden.
Ten einde uw leeslast niet te vergroten geven wij in dit nummer winter 1983/1984 en lente 1984 gecombineerd.

Met nummer 34 sluiten wij het 10e levensjaar van Compact af en maken een start met het 11e. Het jubileumjaar was vol actie met duidelijke betrokkenheid van lezers, schrijvers en alle (rubriek)redactieleden met staf. Wij zijn als KKC/KMG-ers u allen zeer erkentelijk. Wij hopen u -lezer- nog lang te kunnen bedienen.

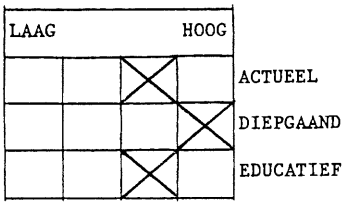
In dit Compactnummer worden de volgende hoofdartikelen behandeld:

Accountant en electronisch informatieverwerking
door D. Steeman



In grote stappen gaat de schrijver door de wordingsgeschiedenis van automatisering en controle sinds 1959 heen.
Daarna geeft hij een systematische opsomming van de huidige aandachtgebieden van de EIV.
Uit dit "overall"-artikel blijkt duidelijk dat de EIV-accountant een terrein van ons vakgebied bestrijkt, dat steeds weer boeit.

100 + 50 - 20 = 80 ????
De betekenis van Concurrency Control
door A. van der Drift

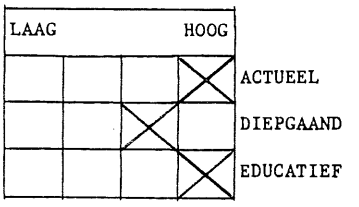


In dit artikel volgt een uiteenzetting over het automatiseringsbegrip Concurrency Control. Het doel hiervan is de accountant inzicht te verschaffen over dit technische en veel voorkomende begrip, dat zeker in een online-omgeving van bijzondere invloed is op de betrouwbaarheid van de gegevensverwerking.
Met dit inzicht dient de accountant in staat te zijn gevaren op dit gebied te onderkennen en waar nodig de gespecialiseerde EDP-auditor gericht in te zetten.

Achtereenvolgens worden een aantal problemen gesignaleerd, waarvoor oplossing worden gegeven met vermelding van de daaraan gerelateerde consequenties.

Vervolgens zal worden ingegaan op een situatie, waarin de bestaande oplossingen veelal niet adequaat zullen werken, waardoor aandachtsgebieden voor de EDP-auditor ontstaan.

De micro en de controlerende accountant
door L. Straathof



In dit artikel worden twee toepassingsgebieden onderscheiden:
- De micro in gebruik bij de cliënt als hulpmiddel bij de bestuurlijke informatievoorziening.
- De micro in gebruik bij de accountant als controlegereedschap.

De schrijver constateert dat er risico's zijn voor doorbreking van interne controle bij het gebruik van micro's. De micro als audit micro stelt zijn eisen op het gebied van de computer interface, betrouwbaarheid en gebruikersvriendelijkheid.

Na de eigen hoofdartikelen is het artikel over de "Opleiding Risk manager" geschreven door de heren Horbeek en Huyskens opgenomen. Wij zijn erkentelijk voor hun toestemming om het artikel in Compact te plaatsen.
Dit geldt ook voor de redactie van de Automatisering Gids voor hun bereidheid toestemming te verlenen om het artikel "Grens bij magnetische opslagtechnieken voorlopig niet in zicht" over te nemen.

De overige rubrieken geven het vertrouwde verslag van actualiteiten of belangwekkende artikelen.
Wij hebben ernaar gestreefd dit steeds te doen in de vorm het belichten van de voor ons van belang zijnde punten.

Voor uw commentaar op hoofdartikelen of besprekingen stellen wij steeds ruimte beschikbaar in ons blad.

Met dit nummer kunnen wij het 10e jubileumjaar gevoeglijk afsluiten om met frisse moed het tweede decennium aan te vatten.

winter 1983/lente 1984

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

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

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

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

Kopij kunt u inleveren bij de secretaris van de redactie.
Adres:
Prinses Irenestraat 59,
1077 WV Amsterdam.
Postadres:
Postbus 7137
1007 JC Amsterdam.

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

Internationaal KMG Klynveld Main Goerdeler

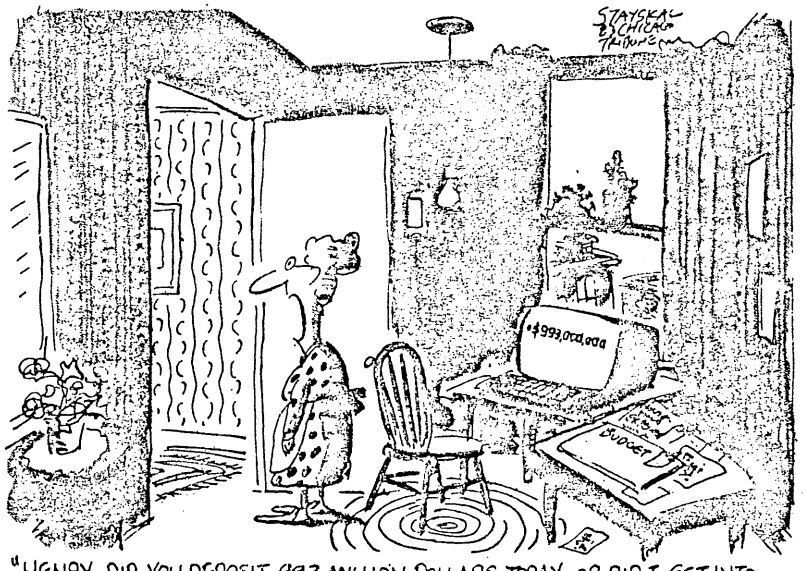
ACTUALITEIT

Nieuw verschenen:
Paulus B. Morssink en Aad Kranendonk
DE VOORKANT VAN HET AUTOMATISEREN

De voorkant van het automatiseren is een praktische handleiding bij automatiseringsprojecten voor zowel de gebruiker als de specialist. Maar al te vaak blijkt dat er zich problemen voordoen bij het gebruik op management- en uitvoeringsniveau van een computer, omdat er bij het ontwikkelen van het project te weinig overleg is geweest, de materie te ondoorzichtig was, men elkaars taal niet sprak, er te weinig gebruikersbegeleiding is of was, etc.
Dit boek geeft een helder beeld van wat automatisering is en doet! De automatisering wordt op levendige wijze en vanuit vele gezichtspunten gepresenteerd. Honderden ideeën, hints en concreet werkmateriaal, dat verzameld is op begeleidingsprojecten, gebruikerstrainingen en studiebijeenkomsten, vindt u hier bijeen.
Deze uitgave brengt de gebruiker en de automatiseringsspecialist bij elkaar en zal een grote bijdrage kunnen leveren aan een zinvolle inpassing van de computer in een organisatie.

De Redactie beveelt het boek ter lezing aan.

. . . und Bild



"HENRY, DID YOU DEPOSIT 993 MILLION DOLLARS TODAY, OR DID I GET INTO THE 1ST NATIONAL BANK'S COMPUTER AGAIN?"

Fact sheet van de Automatisering en Controle-groep
Gezien de betekenis, die de automatisering heeft voor de administratieve organisatie en daarmee voor de accountantscontrole, bestaat sinds 1973 binnen KKC een op het aspect automatisering en controle gespecialiseerde groep (A.C.-groep).

Taken

Primair: Ondersteuning van de collega's, die belast zijn met opdrachten voor de algemene jaarrekeningcontrole inzake betrouwbaarheidsonderzoeken van:
- automatiseringsorganisaties, computer operations
- informatiesystemen (in exploitatie, in het stadium van voorbereiding)

alsmede ondersteuning inzake het gebruik van de computer (mainframes zowel als micro's) voor bestandsonderzoek.

Secundair: Verzorgen van opleidingen (de brochure "Cursussen 1984/85")
Voorlichting (o.a. huisorgaan COMPACT).
Brochures: - Kleinschalige automatisering
- Computerbeveiliging

Research o.m. gericht op:
Data Base Management Systems
Besturingssystemen (MVS audit)
Audit micro
Data Communicatie
Risico-analyse.

Bijzondere opdrachten
Door de verkregen technische deskundigheid als gevolg van ervaring en research worden regelmatig ook opdrachten uitgevoerd welke buiten de jaarrekeningcontrole liggen, zoals op het gebied van:
- beveiliging van gegevens en rekencentra
- privacy
- beoordeling van de doelmatigheid en doeltreffendheid van organisaties en processen
- zelfstandig onderzoek naar betrouwbaarheid van opzet en werking van automatiseringsorganisaties en informatiesystemen, gevolgd door een mededeling ten behoeve van derden
- optreden als deskundige in arbitrages
- technische en operationele audit-reviews in het algemeen
- enquêtes met uitwerking daarvan met behulp van eigen programmatuur.

Bemanning
De A.C.-groep wordt centraal geleid door 7 vennoten en bestaat verder uit:
- 8 EDP-auditors
- 12 aankomend EDP-auditors
- 15 programmeurs.

Derhalve 42 personen die zich in volledige dagtaak met het vakgebied automatisering en controle bezighouden. Daarnaast ca. 35 A.C.-accountants, verspreid over de vestigingen van KKC in Nederland, België, etc. op part-time basis met A.C.-werk belast.
Allen hebben een gerichte opleiding ontvangen op het gebied van systeemontwerp, programmering, operating, controle met behulp van de computer en beoordeling van automatiseringsorganisaties en informatiesystemen.

Bovendien krijgen jaarlijks 3 à 4 stagiairs de gelegenheid om onder deskundige leiding hun stage-opdracht uit te voeren. Deze opdrachten houden nauw verband met de werkterreinen van de A.C.-groep.

Amsterdam, mei 1984

ACCOUNTANT EN ELEKTRONISCHE INFORMATIEVERWERKING

door D. Steeman

1. Inleiding

Het begrip computer en de termen automatisering en elektronische informatieverwerking zijn in onze maatschappij niet meer weg te denken. De afgelopen dertig jaren hebben een geweldige toename te zien gegeven van de automatisering in zowel het bedrijfsleven als semi-overheids- en overheidsinstellingen.
De invloed welke dit op het fungeren van de accountant heeft is reeds vroegtijdig zowel in ons land als bij beroepsorganisaties in het buitenland onderkend.
A.B. Frielink gaf daarvan in 1961 een overzicht in "Auditing Automatic Data Processing"; A survey of papers. In 1964 verscheen in Nederland het eerste boek op dit terrein van J.W. van Belkum en A.J. van 't Klooster met als titel "administratieve automatisering en controle".

In 1970 en 1975 verschenen als NIVRA-geschriften 1 en 13 twee voor het accountantsberoep in Nederland belangrijke documenten over Automatisering en Controle waarbij geschrift 1 zich richtte op de invloed van de administratieve automatisering op de interne controle en geschrift 13 verhandelingen bevatte over:
- de invloed van de geautomatiseerde gegevensverwerking op de accountantscontrole;
- standaard computerprogrammatuur voor de accountantscontrole.

Ook in het Handboek Accountancy') zijn reeds vanaf 1971 artikelen over de automatisering in relatie tot de accountantscontrole opgenomen. Het probleem waarmee de redactie, meer dan met artikelen over andere onderwerpen, kampt is de snelle veroudering.
Dit heeft als eerste verschijnsel reeds geleid tot herschrijving van het artikel over "Het gebruik van de computer in de accountantscontrole". Vooralsnog zal dit probleem blijven bestaan gezien de nog voortschrijdende technische evolutie die ons steeds verder brengt in de richting van een informatiemaatschappij.

De bedoeling van deze bijdrage is om een raamwerk te zijn voor het onderwerp dat door de titel wordt aangegeven. Getracht zal worden een overzicht te geven van de belangrijkste facetten in de relatie van de accountant tot de elektronische informatieverwerking. Voor zover deelonderwerpen van voldoende betekenis zijn of worden, zullen deze in afzonderlijke artikelen worden belicht.
Ook bij een raamwerk doet zich uiteraard het verouderingsgevaar gelden. Dit is evenwel naar het lijkt doelmatig op te vangen door aanvullingen.

') Het onderhavige artikel zal in het Handboek Accountancy worden opgenomen. Uitgever is Samsom.

Gekozen is voor de term elektronische informatieverwerking (EIV) om een betere aansluiting te krijgen met de in het buitenland gehanteerde begrippen. Vergelijk het Angelsaksische Elektronic Data Processing (EDP) en het Duitse Elektronische Daten Verarbeitung (EDV).
De hoofdindeling van deze bijdrage is als volgt:
1. Inleiding.
2. Invloed van de EIV op de interne organisatie.
3. EIV en accountantscontrole.
4. Hulpmiddelen en technieken bij het onderzoek en de controle van de EIV-organisatie en de EIV-systemen.
5. Overige onderwerpen.

2. Invloed van de EIV op de interne organisatie

2.1 **Algemene tendensen**

In het huidige tijdsbestek, wij schrijven 1984, omvat de EIV een breed spectrum van toepassingen welk varieert van grootschalig (met een computersysteem dat miljoenen guldens kost en ter beschikking staat van vele gebruikers) tot kleinschalig (met een computersysteem dat enkele duizenden guldens kost en de individuele gebruiker ten dienste staat). Daarbij komt dat via de moderne, zich snel ontwikkelende communicatietechniek de mogelijkheden van koppeling tussen de computerhardware steeds toeneemt zodat grenzen van informatiesystemen gaan vervagen. Dit roept het gevaar op dat informatiesystemen in organisatorische zin onbeheersbaar dreigen te worden, tenzij men passende maatregelen neemt. Dit is uiteraard in beginsel de taak van de leiding van de huishouding onder wiens verantwoordelijkheid de EIV plaatsvindt. De accountant is daarbij echter belanghebbend omdat zijn werkzaamheden afhankelijk zijn van het niveau van de procesbeheersing binnen de organisatie.

Het toepassen van computers heeft in principe tot gevolg dat de informatieverzorging sneller, meer gedetailleerd en nauwkeuriger wordt. Om deze voordelen te bereiken zal echter aan een aantal voorwaarden van organisatorische aard dienen te worden voldaan, teneinde te komen tot informatiesystemen welke voldoen aan de algemene organisatorische eisen van doeltreffendheid, betrouwbaarheid en doelmatigheid.

De voorwaarden hebben vooral betrekking op gedisciplineerd en systematisch handelen, zowel bij de ontwikkeling van informatiesystemen als bij de verwerking van gegevens op de computer.
Als belangrijkste voorwaarden kunnen worden genoemd:
- automatiseringsplan;
- samenwerking tussen verschillende disciplines;
- systematische informatie-analyse en systeemontwikkeling;
- standaarden en voorschriften;
- goedkeuringsprocedures;
- bewaking van de gegevensverwerking en -opslag.

Al deze voorwaarden zijn van administratief organisatorische aard, hetgeen inhoudt dat de accountant zowel in zijn algemene functie van controleur en adviseur alsook in enigerlei bijzondere functie het gebied dat door deze voorwaarden wordt bestreken, tot zijn kennisgebied dient te rekenen dan wel mag rekenen.

Zoals hiervoor werd gesteld dient ieder informatiesysteem en de organisatie daaromheen te voldoen aan algemene eisen van doeltreffendheid, betrouwbaarheid en doelmatigheid.
Het ligt in de rede dat de accountant zich met name met het aspect van de betrouwbaarheid zal bezighouden. Onder betrouwbaarheid is dan te verstaan de interne controle en de beveiliging.

Ten aanzien van de interne controle kan worden gesteld dat deze als gevolg van de EIV vooral wordt beïnvloed door de tendens tot integratie. Deze integratie komt enerzijds tot uitdrukking in het samenvoegen van opeenvolgende handelingen in het traject van de gegevensverwerking, anderzijds heeft de integratie tot gevolg dat registraties van dezelfde informatie welke voorheen op verschillende plaatsen en/of afdelingen aanwezig waren thans slechts op één plaats in de huishouding worden aangehouden. Integratie kan bij EIV tevens betekenen het samenvoegen van voorheen gescheiden informatiesystemen. Daarbij is de tendens aanwezig dat minder overzichten ten behoeve van tussentijdse afstemmingen worden gemaakt in voor de mens leesbare en controleerbare vorm. De noodzaak tot het maken van geautomatiseerde afstemmingen wordt overigens dikwijls ten onrechte niet onderkend. Door gemeenschappelijk gebruik van programmatuur en gegevens wordt bovendien het patroon van de functiescheidingen beïnvloed. De behoefte aan het beperken van redundante opslag van informatie leidt tot samenvoeging van computerbestanden. Dit heeft tevens tot gevolg een concentratie van in vele gevallen slechts eenmalig geregistreerde gegevens, hetgeen de kwetsbaarheid van de informatiesystemen en wellicht zelfs van de onderneming verhoogt.
Het uitvallen van informatiesystemen, welke voor de dagelijkse bedrijfsvoering van levensbelang zijn, kan leiden tot een aantasting van de continuïteit van de onderneming.

Indien voorts nog wordt vermeld dat in de computerprogramma's vele beslissingsregels worden opgenomen en dat het in het algemeen de tendens is om zo weinig mogelijk voor de mens leesbare overzichten te verstrekken, is het duidelijk dat aan de EIV afzonderlijk aandacht moet worden besteed, met name aan de maatregelen ten behoeve van de interne controle en de beveiliging.

2.2 **Verschillende soorten gegevensverwerking**

Bij de beoordeling en controle van informatiesystemen dan wel van de EIV-organisatie waarin deze systemen worden ontwikkeld en waarin de gegevensverwerking plaatsvindt is de soort gegevensverwerking van grote betekenis.

Daarbij is vooral van belang het onderscheid tussen seriegewijze (batch) georiënteerde verwerking en postgewijze (transactie) georiënteerde verwerking.
Zowel in de seriegewijze als in de postgewijze verwerking kan gebruik worden gemaakt van gegevenstransport, waarbij de computer "on-line", dus rechtstreeks is verbonden met het station waarop de gegevensinvoer en -uitvoer plaatsvindt.

Hierbij kunnen mengvormen ontstaan. De meest geavanceerde vorm van verwerking is het real-time/on-line transactieverwerkend systeem, waarbij gegevens omtrent voorraden, debiteuren, onderhanden werk, enz. à la minute kunnen worden gewijzigd en waar de klant - als ware hij in een zelfbedieningswinkel - zijn order zelfstandig samenstelt.

Naarmate een informatiesysteem meer transactie-georiënteerd is dan batch-georiënteerd zal de beoordeling op de aspecten van betrouwbaarheid en doelmatigheid in moeilijkheid toenemen.
Transactie-georiënteerde verwerking vereist veelal meer complexe en aanvullende besturingsprogrammatuur die van invloed is op de betrouwbaarheid en doelmatigheid.

De evolutie van batch-georiënteerde naar transactie-georiënteerde systemen is mogelijk geworden door de technische ontwikkeling in de:
- computerapparatuur;
- programmatuur;
- datacommunicatie.

Als gevolg van de ontwikkeling in apparatuur en programmatuur hebben zich verdergaande mogelijkheden voorgedaan ten aanzien van:
- centralisatie/decentralisatie;
- integratie.

Deze ontwikkelingen zullen hiernavolgend kort worden besproken. Hierbij dient te worden opgemerkt dat de ontwikkeling in apparatuur, programmatuur en datacommunicatie (gegevenstransport over lijnen) elkaar onderling sterk beïnvloeden.

2.3 **Ontwikkelingen in de computerapparatuur**

In de zestiger jaren werden de eerste computers op de markt gebracht die in principe geschikt waren voor postgewijze verwerking met behulp van datacommunicatie. Deze als "main-frames" aangeduide apparatuur werd ingezet vanuit de conceptie van centrale gegevensverwerking.

Capaciteitsverhoging voor de diverse onderdelen van de apparatuur doet zich nog steeds met de regelmaat van een klok voor om huishoudingen die eenmaal vanuit de historie hebben gekozen voor centrale gegevensverwerking, in staat te stellen daarmee door te gaan en steeds meer toepassingen op één computer te verwerken.

Zo geeft men de grootte van interne geheugens niet meer zoals bij de systemen uit de jaren '60 aan in duizenden eenheden (K voor Kilo) doch in miljoenen eenheden (M voor Mega). De snelheid van verwerking, aangegeven in miljoenen instructies per seconde (mips) was in 1970 1 à 2 mips tegen thans circa 15 mips.

Ook de externe geheugenvormen hebben geweldige capaciteitssprongen gemaakt van magneetbanden met ca. 21 MB (nu 154 MB) naar (vaste) schijfeenheden van toen zo'n 7,25 MB (nu 2,5 gigabytes) per eenheid of naar massageheugens met momenteel circa 472 gigabytes.

(Giga, een voorvoegsel dat 10^9 aangeeft of wel een miljard.)

De meest spectaculaire verandering in de wijze van externe geheugenopslag is daarbij nog altijd het direct adresseerbare medium vooral in de vorm van schijven geweest. Dit is, met de toepassing van datacommunicatie, de belangrijkste impuls geweest welke naast seriegewijze verwerking ook verwerking per post of transactie mogelijk maakte.
Hoewel de grote "main-frames" door de technische ontwikkeling een steeds gunstiger prijs/prestatieverhouding te zien gaven waren zij, behalve bij gemeenschappelijk gebruik, toch nog altijd te duur voor de meeste huishoudingen.

Als gevolg hiervan ontwikkelde men reeds in de jaren '60 de zogenaamde officecomputer voor administratieve doeleinden welke meestal een soort boekhoudmachine was, voorzien van enige interne geheugencapaciteit. Derhalve programmeerbaar en tevens voorzien van alle mogelijke vormen van externe geheugencapaciteit alsmede invoer- en uitvoermogelijkheden.

De verkleining van interne geheugens en de geïntegreerde schakelingen thans bekend onder de naam chips, waarbij op een fysieke eenheid ter grootte van een contactlens (Ø 1/2 cm^2) zo'n 100.000 schakelingen kunnen worden uitgevoerd leidde vooral in de technisch-wetenschappelijke wereld tot de bouw van microcomputers. Evenals dit bij de eerste "main-frames" in de jaren '40 en '50 het geval is geweest kwam ook bij deze microcomputers al gauw de behoefte aan snellere dan handmatige in- en uitvoerapparatuur alsmede grotere externe geheugencapaciteit naar voren. Daarmede waren deze micro's rijp voor commerciële toepassing op de administratieve markt die vooral bij de kleinere ondernemingen zoals gezegd braak lag.

Naar de aanduiding doet veronderstellen ligt de zogenaamde minicomputer van de jaren '70 tussen de grote reeds lang bestaande "main-frame" computer en de microcomputer in. In de praktijk blijkt de terminologie niet eenduidig te zijn. Wellicht was er oorspronkelijk reden om onderscheid te maken in die zin dat de minicomputer veelal een verkleinde uitgave was van de "main-frame" computer, terwijl de microcomputer een zelfstandige ontwikkeling was uit wat hiervoor als de technisch-wetenschappelijke hoek werd aangegeven. In de administratieve wereld spreekt men thans van kleinschalige computers, waarmee dan in feite die computerconfiguraties worden bedoeld die permanent met een minimum aan bedienend personeel kunnen opereren.
Vandaag de dag moet ook rekening worden gehouden met huiscomputers welke zowel geschikt zijn om met voorgeprogrammeerde spelletjes te werken als om administratieve verwerkingen te verrichten met behulp van standaardpakketten dan wel met zelf gemaakte programmatuur.

2.4 Ontwikkelingen in de programmatuur

2.4.1 Besturingsprogrammatuur

De eerste computers kenden eenvoudige invoer- en uitvoerprocedures waarbij slechts één toepassingsprogramma tegelijk werkte, de invoer via één soort medium plaatsvond en wellicht de uitvoer eveneens. Met de ontwikkeling van de computerapparatuur werd de wijze waarop het gegevensverkeer in de computerconfiguratie moest worden bestuurd steeds complexer.

Als voorbeeld moge dienen de mogelijkheid die de moderne computer biedt om niet met één programma doch schijnbaar met meerdere programma's tegelijk bezig te zijn. Daarbij zijn de verschillende programma's vaak zo groot dat zij niet geheel in het reële interne geheugen aanwezig zijn doch slechts die stukken die werken of net gewerkt hebben.

De kernfunctie van een besturingsprogramma is de centrale verwerkingseenheid zo veel mogelijk tegelijk met in- en uitvoercomponenten bezig te houden en daartoe op geschikte momenten te wisselen van instructiereeks, hetgeen veelal betekent dat afwisselend aan stukjes van verschillende toepassingen wordt gewerkt.
Het besturingsprogramma zorgt nu in letterlijke zin voor zowel de besturing van de programmadelen in hun uitvoering van instructie tot instructie door het instructie-interpreterende orgaan van de computer, als voor de administratie van de stand van zaken per instructie. Het valt te begrijpen dat naarmate het aantal gebruikers, programma's en gegevensverzamelingen toeneemt het besturingsprogramma meer functies dient te hebben en dus complexer wordt en ook een groter deel van de computercapaciteit gaat bezetten. Een belangrijke taak uit de vele wordt bijvoorbeeld de zorg dat programma's niet in elkaars gebied in het interne geheugen kunnen komen. Dit zou uit het gezichtspunt van zowel ongestoorde verwerking als gegevensbeveiliging een ongewenste zaak zijn.

2.4.2 Toepassingsprogrammatuur

Onder toepassings- of wel applicatieprogrammatuur is te verstaan alle programmatuur waarmee gegevensverwerking plaatsvindt. Toepassingsprogramma's worden geschreven in een programmeertaal.
De algemene tendens is dat men de talen steeds meer gebruikersvriendelijk tracht te maken door aansluiting te zoeken bij de eigen menselijke taal en het vereenvoudigen van de taalregels. Dit betekent dat het gebruik van de computer steeds meer gemeengoed gaat worden althans voor eenvoudige applicaties.

2.4.3 Toepassingspakketten

Het ontwerpen en schrijven van meer omvangrijke toepassingsprogrammatuur is zodanig tijdrovend en kostbaar dat het lonend wordt voor problemen die zich voor automatisering lenen en voor een veelvoud van gebruikers ongeveer hetzelfde liggen, uniforme programma's te maken welke in de vorm van een pakket worden aangeboden.

Hoewel de gedachte op zich aanlokkelijk is, blijken in de praktijk de eisen en wensen van de gebruikende huishoudingen toch weer zodanig te verschillen dat onderzoek vooraf op doeltreffendheid en betrouwbaarheid zeer gewenst is. Of de toepassing, na onderzoek, nog doelmatig is zal blijken uit de aanvullingen die al dan niet noodzakelijk zijn en die uiteraard extra kosten met zich brengen.

Van betekenis voor de continuïteit van de toepassing is de mogelijkheid tot aanpassing van het pakket en het onderhoud alsmede de gegoedheid van de leverancier. Voor het overige moge worden verwezen naar NIVRA-geschrift nummer 16, "Accountant en computerservicebureaus".

2.4.4 **Teleprocessingprogrammatuur**
De behoefte om gegevens sneller en eenvoudiger te verwerken (te registreren en te representeren) heeft in de laatste 10 jaren geleid tot gegevensverwerking waarbij de gebruiker rechtstreeks met de computer is verbonden door middel van terminals.
Deze vorm van gegevensverwerking wordt als teleprocessing (T.P.) aangeduid. De programmatuur die het verkeer tussen een centrale computer en de daaraan aangesloten terminals regelt wordt meestal T.P.-monitor genoemd.
Deze programmatuur kan worden aangevuld met datacommunicatieprogrammatuur welke het gegevensverkeer door middel van complexe verbindingen over langere afstand regelt.

Ook de T.P.-monitor kan voor de accountant evenals de gewone monitor onderwerp van onderzoek zijn. Met name zal het hier aspecten van betrouwbaarheid betreffen zoals de toegang tot de centrale computer en het gebruik van toepassingsprogrammatuur welke voor een belangrijk deel door de T.P.-monitor wordt geregeld door middel van in tabellen opgenomen beveiligingsinformatie, waaronder sleutelwoorden.

2.4.5 **Hulpprogrammmatuur**
Rond de besturingsprogrammatuur welke zeker bij de "main-frames" door de leverancier wordt gemaakt en bijgeleverd kennen alle computers programmatuur die de computergebruiker in staat stelt snel standaardbewerkingen uit te voeren. Deze programmatuur wordt zowel door leveranciers als door softwarehouses geleverd. De programma's dienen bijvoorbeeld om snel fouten te kunnen opsporen of te herstellen met behulp van opvraag- en kopieerroutines.

Dit kan betekenen dat buiten de normale procedure om inzage wordt verkregen, respectievelijk wijzigingen kunnen worden aangebracht in toepassingsprogramma's en in gegevensverzamelingen. Dit kan vanuit het oogmerk van interne controle minder wenselijk zijn, doch om reden van doelmatigheid juist wel. Hier ligt een controverse welke voor de accountant van betekenis is bij zijn beoordeling van de kwaliteit van de interne controle, als ook bij een eventueel advies over de doelmatigheid van de organisatie van een computercentrum.

2.4.6 **Gegevensbeheersingsprogrammatuur**
Een van de belangrijkste problemen in de automatisering van administratieve processen is de beheersing van omvangrijke gegevensverzamelingen veelal georganiseerd in de vorm van databases. Daarbij is het doel deze gegevensverzamelingen zodanig te structureren en te beschrijven, dat de toepassingsprogrammatuur op eenvoudige wijze die delen van de database ter beschikking krijgt, die voor de betreffende toepassing relevant zijn.

Er zijn een aantal gegevensbeheersingsprogramma's, beter bekend als data base management systems (DBMS), welke de afgelopen 15 jaar zijn ontwikkeld. Tussen deze DBMS's bestaan grote verschillen zowel in de wijze waarop de door hen te beheersen databases gestructureerd, bewerkt als beveiligd worden.

Het beheersen van de gegevens door middel van een DBMS brengt opnieuw, zoals ook bij besturingssystemen en T.P.-monitors, met zich mee dat zich binnen een huishouding specialismen gaan ontwikkelen.
Dit betekent zowel voor algemeen management als voor de accountant een probleem van beheersing van de functies en de processen rond de organisatie van de database(s) waarbij nu de gegevens, meestal reeds informatie, van de huishouding rechtstreeks in het geding zijn.

2.5 **Centralisatie/decentralisatie**
Het aloude dilemma van de keuze tussen centrale of decentrale organisatie wordt thans, voor wat betreft de decentrale verwerking en decentrale opslag van gegevens, niet meer belemmerd door de automatisering.

Zoals uit voorgaande uiteenzetting omtrent de ontwikkeling in apparatuur en programmatuur kan worden afgeleid, bestond vanuit de gedachte van de grote "main-frame" apparatuur en de dáárvoor tot stand gekomen teleprocessing en database programmatuur een sterke tendens tot centrale gegevensverwerking met grote centrale databases.

2.5.1 **Apparatuur**
De mogelijkheden tot decentralisatie bezien vanuit de apparatuur hebben langs verschillende wegen impulsen ontvangen:
- beeldschermapparatuur wordt uitgerust met interne geheugencapaciteit en plaatselijk koppelbare invoer- en uitvoermogelijkheden, alsmede externe geheugencapaciteit;
- stand-alone computers van micro- tot minicomputer krijgen faciliteiten om aan andere apparatuur te worden gekoppeld;
- datacommunicatiefaciliteiten worden uitgebreid;
  .telefoonlijnen krijgen hogere snelheden en worden betrouwbaarder;
  .andere vormen van gegevenstransport komen beschikbaar zoals straalverbindingen, eventueel via satellieten.

Daarnaast behoort uiteraard spreiding van EIV door middel van niet gekoppelde kleinschalige apparatuur tot de mogelijkheden.

2.5.2 **Programmatuur**
Ten behoeve van het verzenden, transporteren en ontvangen van gegevens via lijnen dient programmatuur te worden ontwikkeld. Zolang programmatuur en apparatuur door dezelfde leverancier worden gemaakt is er geen probleem. Iedere leverancier ontwikkelt zijn eigen "protocol". Problemen ontstaan zodra men computers, invoer-, uitvoer- en opslagmedia van verschillende fabrikaten direct of via lijnverbindingen aan elkaar wil koppelen.
Op dat moment ontstaat de strijd wiens protocol tot standaard zal worden verheven, dan wel hoe men de verschillende protocollen aan elkaar kan koppelen.

2.5.3 **Gegevens**
Vanuit de van oudsher bekende mogelijkheden tot beheersing bij centrale verwerking en opslag zullen de gegevensverzamelingen, welke als resultaat van invoer en verwerking beschikbaar komen, in het algemeen beter onder controle kunnen worden gehouden dan bij decentrale verwerking en gehele of gedeeltelijke decentrale opslag van gegevens.
In het geval van sterk gedecentraliseerde verwerking en opslag zullen aan de organisatie hoge eisen worden gesteld ten aanzien van coördinatie tussen de verschillende decentrale verwerkingspunten en de handhaving en naleving van uniforme procedures indien er althans sprake is van onderlinge koppeling.

2.6 **Geïntegreerde verwerking**
De in 2.1 genoemde algemene tendens tot integratie heeft zich als gevolg van de in de paragrafen 2.2 tot en met 2.5 van dit hoofdstuk behandelde ontwikkelingen in versterkte mate voortgezet. Door de toepassing van centrale computers heeft de situatie zich vanuit het begin van de ontwikkeling van de EIV, waarin één gebruiker (gebruikersafdeling) op gemeenschappelijk gebruikte apparatuur met zijn eigen programmatuur zijn eigen gegevens kon verwerken en bewaren, zich zodanig ontwikkeld dat zeer complexe situaties kunnen ontstaan, waarbij men van elkaars programma's en elkaars gegevens gebruik maakt.
Vanuit de toepassing van micro- en minicomputers ontstaat dezelfde situatie, met dien verstande dat de prijs/prestatieverhoudingen massaal gebruik op kleine schaal mogelijk maakt. Uiteindelijk zal de situatie gaan ontstaan waarbij alle mogelijke apparatuur aan elkaar gekoppeld zal kunnen worden. Dit is eigenlijk slechts een probleem van standaardisatie op het gebied van netwerkprotocollen. Naarmate dit wordt gerealiseerd zal er in hoge mate sprake zijn van gemeenschappelijk gebruik van zowel apparatuur als programmatuur als - en met name - van gegevens.

Een dergelijk gemeenschappelijk gebruik van hulpbronnen in een organisatie mag er natuurlijk niet toe leiden dat verantwoordelijkheden onduidelijk worden en daardoor niet meer door natuurlijke personen kunnen worden gedragen.

De besturing van het gemeenschappelijk gebruik van hulpbronnen geschiedt voornamelijk door middel van programmatuur, welke in het algemeen als besturingsprogrammatuur kan worden aangeduid.

Dit betekent dat niet langer uitsluitend de toepassingsprogramma's object van beoordeling en controle dienen te zijn doch dat ook de besturingsprogrammatuur en met name de wijze van installatie in zijn veelheid van verschijningsvormen object van beoordeling en controle dient te zijn, zowel vanuit het oogpunt van managementbeheersing als van accountantscontrole.

Deze taak zal toevallen aan de technisch georiënteerde EDP-auditor die in staat zal moeten zijn om zich met hoog gekwalificeerde automatiseringsdeskundigen op het gebied van besturingsprogrammatuur te kunnen verstaan en te kunnen meten.

3. EIV en accountantscontrole

3.1 **De ratio van een afzonderlijke behandeling**

Zowel in de opleiding voor het accountantsexamen als in de praktijk wordt gepleit voor een geïntegreerde behandeling van de aspecten van EIV, welke van betekenis zijn voor de administratieve organisatie en de controle.

Men dient echter het beestje eerst te kennen alvorens men er over kan praten, laat staan dat men kan beoordelen welke invloed ervan uitgaat. In hoofdstuk 2 is de betekenis van de EIV aangegeven. Zolang de techniek nog voortschrijdt en dat doet zij, zal in de ontwikkeling van het beroep en de opleiding daarvoor aan het fenomeen automatisering afzonderlijke aandacht moeten worden besteed. De administratieve organisatie is de basis van de accountantscontrole. Zonder administratieve organisatie geen accountantscontrole.
Aangezien vrijwel elk aspect van de administratieve organisatie door de EIV wordt beïnvloed zal de accountant de EIV tot zijn deskundigheidsgebied dienen te rekenen.

3.2 **Het onderscheid tussen het onderzoek en de controle van de EIV in algemene en in bijzondere zin**

Vanuit het gezichtspunt van de accountant is het doelmatig indien onderscheid wordt gemaakt tussen het onderzoek en de controle, welke door de accountant wordt verricht in het kader van zijn algemeen fungeren als controleur van de jaarrekening en het onderzoek en de controle voortvloeiend uit een afzonderlijke opdracht.

3.3 **Het algemene EIV-onderzoek en de controle in relatie tot de controle van de jaarrekening**

Voor de systematische behandeling van het algemene EIV-onderzoek en de controle wordt onderscheid gemaakt tussen de beoordeling van de maatregelen ten behoeve van interne controle en beveiliging, welke in de EIV-organisatie en de EIV-systemen zijn getroffen en de controle op de naleving daarvan door toetsing van die maatregelen. (Te vergelijken met het Amerikaanse begrip "compliance testing").

Men dient te bedenken dat het EIV-onderzoek in het kader van de jaarrekeningcontrole geen doel op zich is. De accountant onderzoekt en controleert de EIV slechts voor zover hij dit nodig acht voor de controle van het cijfermateriaal zoals dat in de winst- en verliesrekening en balans wordt weergegeven.

Het kan voor de accountant doelmatig zijn indien hij zich voor zijn controle rechtstreeks richt op het cijfermateriaal, waarbij het onderzoek naar de administratieve organisatie en de daarin begrepen EIV tot een minimum wordt beperkt.
Bij gebrek aan beter hanteert men hiervoor het begrip verificatie van het cijfermateriaal hetgeen vergeleken kan worden met het Amerikaanse begrip "substantive testing".

Het zal duidelijk zijn dat rechtstreekse controle op het cijfermateriaal dikwijls zowel verificatie als toetsing inhoudt. Dit is bijvoorbeeld het geval indien een uitgave wordt geverifieerd met externe bescheiden, welke hun waarde voor de accountantscontrole mede ontlenen aan maatregelen ten behoeve van interne controle.

Het zal tevens duidelijk zijn dat naar gelang de maatregelen ten behoeve van interne controle worden geautomatiseerd de betekenis van de toetsingscontrole toeneemt. Dit zal nimmer zover kunnen gaan dat de verificatieve controle op de gegevens geheel wordt vervangen door toetsingscontrole op het systeem.

Een specifiek controleprogramma of onderdeel van een controleprogramma zal hoogstens gekenmerkt kunnen worden door een systeemgerichte, dan wel een gegevensgerichte aanpak.

3.4 **Het bijzondere EIV-onderzoek en de controle**

Ter onderscheiding van het werk dat door de accountant in het kader van de jaarrekeningcontrole wordt verricht met betrekking tot de EIV, is het doelmatig al het overige werk te beschouwen als bijzonder onderzoek en controle.
Deze onderscheiding wordt gemaakt vanuit het algemeen fungeren van de accountant als controleur van jaarrekeningen. Vanuit het oogmerk van de accountant is al datgene wat door hem niet behoeft te worden gedaan omdat dat niet nodig is voor de jaarrekeningcontrole als bijzonder aan te merken. Dergelijk werk behoeft dan ook een afzonderlijke opdracht van de leiding op grond van haar behoefte aan:

- een meer diepgaande beoordeling over betrouwbaarheid en continuïteit van de EIV, dan wel méér of gerichtere controle op bepaalde onderdelen;
- een oordeel over doelmatigheid van EIV-systemen en EIV-organisatie;
- een oordeel over doeltreffendheid van de verstrekte informatie als produkt van de EIV.

4. Hulpmiddelen en technieken bij het onderzoek en de controle van de EIV-organisatie en de EIV-systemen

4.1 Documentatie

4.1.1 Documentatie als basis voor onderzoek en controle

Abstracte zaken als een EIV-organisatie en de daarbij behorende EIV-systemen vereisen een adequate systematische vastlegging welke voor een huishouding van essentiële betekenis is. Een zo getrouw mogelijke documentatie als weergave van de EIV-organisatie en de EIV-systemen dient voor een aantal doelen, waarvan te noemen:

- verantwoording door de opstellers;
- basis voor goedkeuring door gebruikers;
- overdracht van kennis;
- middel voor onderhoud;
- middel tot controle.

Documentatie van actueel en redelijk niveau is voor een ieder die op grond van een onderzoek een oordeel wil verkrijgen over het EIV-gebeuren in een huishouding onmisbaar. De vormen waarin documentatie wordt gepleegd zijn velerlei en steeds groeiend naar gelang nieuwe technieken worden toegepast.
Voor de accountant zijn niet limitatief de volgende soorten documentatie van belang.
EIV-organisatie:

- organisatiestructuurschema;
- functie- en taakbeschrijvingen;
- procedures voor systeemontwikkeling;
- procedures en instructies voor machinebediening, acceptatie en overdracht;
- leveranciershandboeken voor hardware en software.

EIV-systemen:

- systeembeschrijving (vooral het hoofdstuk interne controle);
- programmadocumentatie;
- gebruikershandleiding;
- gegevensmodellen;
- data-dictionaries en data-directories.

4.1.2 Documentatie van een onderzoek

Iedere onderzoeker zal ook zelf behoefte hebben aan documentatie over zijn onderzoek.
In het kader van het onderhavige handboek ligt het in de rede dat met name aan de eigen documentatie van de accountant als onderzoeker van EIV-organisaties aandacht wordt besteed.
Op grond van artikel 11 van de Gedrags- en Beroepsregels Registeraccountants kan worden gesteld dat de accountant zijn werkzaamheden dient te documenteren om mede daardoor te kunnen aantonen dat hij zijn werk volgens deugdelijke grondslag heeft verricht.

4.2 **Vragenlijsten**
Het doelmatigheidsprincipe dwingt er toe om daar waar eenzelfde soort van werkzaamheden met enige regelmaat wordt verricht de uit te voeren handelingen te systematiseren. Dit kan geschieden in een vorm variërend van algemene vragenlijsten tot gedetailleerde checklists.

4.3 **Het gebruik van de computer in de accountantscontrole**

4.3.1 **Gegevensgericht gebruik**
Zoals de computer niet meer weg te denken is uit het bedrijfsleven en steeds meer ingeburgerd raakt in de huiselijke sfeer is de computer ook als hulpmiddel van de accountantscontrole een steeds belangrijker rol gaan spelen.

In de praktijk wordt de computer het meest intensief gebruikt voor het onderzoeken van gegevensverzamelingen welke in computerbestanden zijn opgeslagen.
Het gebruik van de computer neemt snel toe door interactief gebruik waarbij de accountant door middel van een terminal als gebruiker met de computer converseert, dan wel met een eigen eventueel draagbare microcomputer, welke al of niet wordt gekoppeld aan een computer, te onderzoeken bestanden benadert (zie ook 4.3.3).

4.3.2 **Systeemgericht gebruik**
In het kader van het toetsen van de werking van informatiesystemen is een grote verscheidenheid aan technieken ontwikkeld.

Deze technieken variëren van het loslaten van testgevallen op een nog in gebruik te nemen informatiesysteem tot het opnemen van extra routines in de programmatuur ten behoeve van het continu testen van operationele systemen en het creëren van loze gegevensverzamelingen of bedrijfseenheden om de handhaving en naleving van eenmaal in bedrijf gestelde systemen te toetsen.

Naar onze waarneming in de praktijk hebben deze technieken, in verhouding tot het gebruik van de computer voor gegevensgericht onderzoek, voor de acountantscontrole veel minder toepassing gevonden. Deze technieken die ook wel bekend zijn onder de verzamelnaam geïntegreerde testfaciliteiten vinden bij uitstek hun toepassing ten behoeve van de interne controle van complexe systemen.

4.3.3 **De controle-micro**
Een zich snel aandienend hulpmiddel voor de accountant is de microcomputer. Naarmate de draagbaarheid van het apparaat, de overdraagbaarheid van de programmatuur en de koppelbaarheid van de apparaten onderling toenemen zal de betekenis voor de accountantscontrole toenemen.

Hier is niet alleen sprake van het onder 4.3.1 genoemde bestandsonderzoek, maar ook van een ruimer gebruik ad hoc voor allerlei doeleinden welke verband houden met de uitvoerende arbeid van de accountant zoals:
- vastleggingen van organisaties in schema's;
- dossieraantekeningen;
- ad hoc doorrekenen van kostprijzen, financieringsschema's, afschrijvingsschema's etc.;
- cijfermatige vastleggingen en analyses;
- vergelijking van voor- en nacalculaties;
- rapportering.

Men kan zich voorstellen dat de term "elektronisch dossier" reeds is gevallen. Op dit moment (wij schrijven 1984) zijn allerwege inspanningen te bespeuren om programmatuur te ontdekken of te ontwikkelen om aan vorengenoemde doeleinden tegemoet te komen.

5. Overige onderwerpen

5.1 **Accountant als adviseur op het gebied van de EIV**

In hoofdstuk 3 is een indeling gegeven van de werkzaamheden van de accountant, zoals deze zich met EIV bezighoudt. Daarbij hebben wij ons beperkt tot de accountant in de controlerende functie met een onderscheid naar het algemene en het bijzondere EIV-onderzoek alsmede de controle.

Niet ter sprake is gekomen de accountant als adviseur op het gebied van de EIV.

Voor zover de accountant zich vanuit een algemene of bijzondere controle-opdracht bezighoudt met EIV, vloeit daaruit een natuurlijke adviesfunctie voort, welke zich echter in het algemeen beperkt tot de invalshoek van waaruit de accountant opereert.
Deze invalshoek kan het best worden omschreven als die van betrouwbaarheid en continuïteit van de EIV.

Accountants kunnen zich naast hun specifieke deskundigheid op het gebied van de controle ook bekwamen op andere vakgebieden. De EIV is één van die vakgebieden waarop ook accountants zich kunnen toeleggen zodanig dat zij na het verwerven van voldoende deskundigheid als adviseur op het terrein van de EIV kunnen gaan opereren. Daarbij zal het vrijwel altijd gaan om de organisatorische aanpak van de EIV aangezien de opleiding van de accountant zich niet erg leent voor een zeer specialistische vorming op het gebied van software of hardware.
Als voorbeeld kan dienen de accountant die, als doctorandus afgestudeerd in de Bestuurlijke Informatiekunde (BIK), na het behalen van het post-academische accountantsdiploma niet in de algemene controlefunctie gaat opereren, doch na eventuele verdere praktische scholing, als adviseur gaat optreden bij de ontwikkeling van informatiesystemen.

5.2 De accountant, de EIV-accountant en de EDP-auditor

5.2.1 De functies

De snelle ontwikkeling en de omvang van het terrein van de EIV hebben, vanaf het moment dat de EIV invloed begon te krijgen op de administratieve organisatie van huishoudingen en daarmee op de accountantscontrole, voor accountants in de algemene controlefunctie geleid tot een discrepantie tussen de noodzakelijke en werkelijke kennis op het gebied van de EIV.

De accountant die zich bezighoudt met het certificeren van jaarrekeningen dient een zodanige kennis van EIV te hebben dat hij de invloed van de EIV op zijn controle kan beoordelen.

Er is vrijwel geen accountant die zijn kennis gedurende zijn actieve beroepsuitoefening van ca. 30 jaar, in voldoende mate door middel van permanente educatie up to date kan houden over de ontwikkelingen in de EIV.

In de meeste accountantsorganisaties heeft men sinds het eind van de zestiger jaren de behoefte gevoeld aan ondersteuning door meer op de EIV gespecialiseerde personen.

Dit heeft enerzijds geleid tot de situatie waarbij registeraccountants en niet-registeraccountants zich meer gingen specialiseren op de aspecten van betrouwbaarheid en continuïteit van de EIV. Deze "echte" specialisten willen wij in navolging van de Angelsaksische terminologie aanduiden als EDP-auditor. Hier is sprake van een volledige specialisatie met het uitoefenen van het vak als permanente functie.

Anderzijds kwam er behoefte aan het over een breed front opleiden van jonge studerende of pas afgestudeerde accountants die zich gedurende een zekere tijd (beperkt in intensiteit en/of jaren) bezig hielden met de EIV ter ondersteuning van hun algemene collega's. Deze aldus gevormde EIV-accountants konden op zijn minst langer steunen op eenmaal opgedane ervaring wanneer zij weer geheel in de algemene functie zouden optreden.

5.2.2 De opleiding

Voor degenen die studeren voor accountant staat in de opleiding een steeds toenemend pakket aan EIV-kennis ter beschikking dat de tendens heeft om van technische naar functionele aspecten te evolueren. Voor de afgestudeerde accountants bestaat de permanente educatie.

De opleiding tot EIV-accountant is binnen de grote accountantsorganisaties ter hand genomen.
Ook hier zien we een tendens van het verkrijgen van technische kennis naar het verwerven van kennis op de functionele aspecten van de automatisering en het verkrijgen van oefening in de beoordeling van EIV-organisatie en EIV-systemen, alsmede in het gebruik van de computer.
Er bestaan ideeën om deze opleidingen te institutionaliseren.

Voor EDP-auditor bestaat geen opleiding, zij het dat iedereen met een behoorlijke EIV-opleiding dit vak kan gaan uitoefenen. Onder een behoorlijke opleiding kan worden begrepen die aan een Hogere Informatica School, de Bedrijfsinformaticarichting van een Hogere Economische Administratieve Opleiding of een van de universitaire opleidingen.
Ook de Ambi-opleiding is van oudsher een goede basis. Het is noodzakelijk dat deze opleiding wordt aangevuld met onderdelen uit de Bedrijfseconomie en belangrijke stukken uit de Administratieve Organisatie met de nadruk op de Interne Controle. Ook het onderdeel Controleleer uit de accountantsopleiding dient voor het grootste deel te worden gevolgd, waarbij de EDP-auditor die de accountant ten behoeve van de samenwerking goed wil begrijpen eigenlijk het gehele leerstuk van de Controleleer dient te beheersen.

5.3 Mededelingen met betrekking tot betrouwbaarheid en continuïteit van de EIV

Onderzoek en controle van EIV-organisatie en EIV-systemen kan geschieden ten behoeve van de eigen arbeid als accountant of ten behoeve van een andere accountant in het kader van de jaarrekeningcontrole.
Ook buiten het kader van de jaarrekeningcontrole bestaat behoefte aan onderzoek en controle van EIV-organisaties en EIV-systemen zowel bij leidinggevende functionarissen als bij belanghebbende derden.

Wanneer het EIV-onderzoek door de accountant voor eigen oordeelsvorming nodig is kan worden volstaan met dossieraantekeningen in de gebruikelijke zin. Zodra het oordeel of de bevindingen uit onderzoek of controle aan anderen moet worden kenbaar gemaakt ontstaat behoefte aan codificatie ten aanzien van vorm en strekking van de rapportering. In de Nederlandse literatuur bestaat hiervoor in de serie NIVRA-geschriften het deel nummer 26 dat tot titel heeft "Mededelingen door de accountant met betrekking tot de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking".

Dit geschrift kan worden beschouwd als de voorlopige neerslag van de ervaringen opgedaan met het verstrekken van mededelingen aan derden, waarbij aansluiting is gezocht met de Gedrags- en Beroepsregels voor Registeraccountants.

5.4 Onderzoek en controle ingeval van uitbesteding van de EIV aan een servicebureau

Aan de gehele of gedeeltelijke uitbesteding van de EIV aan een servicebureau zijn enkele bijzondere aspecten verbonden welke voornamelijk voortvloeien uit het feit dat er een zakelijke scheiding is tussen partijen. Dit vereist vooral meer formele regelingen in het onderlinge dagelijkse verkeer alsmede afgrenzing en bepaling van verantwoordelijkheden met betrekking tot de dienstverlening. Genoemd kunnen worden onder meer:
- duur van de overeenkomst;
- eigendom van programmatuur;
- kwaliteit van documentatie;
- wie maakt de gebruikershandleidingen;
- hoe vindt acceptatie van nieuwe programma's plaats.

Naarmate de betekenis van de uitbesteding voor management en accountant groter wordt zal de behoefte aan een oordeel over de organisatie en de verwerking van de systemen, voor zover dit niet uit de uitkomsten blijkt, toenemen.
In deze behoefte kan worden voorzien door onderzoek en controle te laten uitvoeren door een onafhankelijke deskundige. Rapportage kan plaatsvinden in de vorm van een mededeling, eventueel met repeterend karakter, zoals genoemd onder 5.3.
NIVRA-geschrift nummer 16 behandelt de onderhavige problematiek onder de titel "Accountant en computerservicebureaus".

5.5 **Beoordeling en controle van standaardprogrammatuur**

Daar waar uniforme problematiek in een aantal verschillende huishoudingen bestaat zal men trachten tot doelmatiger oplossingen te komen in de vorm van standaardprogrammatuur.
Deze ontstaat doordat één gebruiker een toepassing heeft ontwikkeld welke hij in zijn branche tracht te verkopen of doordat een softwarebureau een probleem analyseert dat bij vele bedrijven bestaat en daarvoor een pakket ontwerpt, dit programmeert en op de markt aanbiedt.

Het meest voor de hand liggend als voorbeeld zijn de pakketten op het gebied van de financiële administratie waarvan er een groot aantal wordt aangeboden voor verschillende soorten van apparatuur en met een verscheidenheid aan mogelijkheden. Hieruit zal reeds duidelijk zijn dat de oplossingen niet zo uniform zijn als het probleem vaak lijkt.

Bij de potentiële gebruiker bestaat primair behoefte aan deskundigheid over de toepasbaarheid in zijn situatie. Het is meestal aan de accountant om de aspecten van betrouwbaarheid te belichten.

Deskundige ondersteuning ten aanzien van de toepasbaarheid is het terrein van de organisatie-adviseur. Door zijn gecombineerde deskundigheid met betrekking tot toepasbaarheid en betrouwbaarheidsaspecten kan de (EIV) accountant veelal eveneens doelmatig adviseren.

Ten aanzien van de betrouwbaarheid is het zeer wel denkbaar dat ten behoeve van toekomstige gebruikers een zodanig onderzoek naar de opzet van een pakket wordt gedaan, dat daarover een mededeling voor algemeen gebruik wordt afgegeven dan wel een mededeling wordt verstrekt aan de opdrachtgever waarvoor per keer toestemming tot afgifte wordt gegeven.

5.6 **Functiescheiding en toegangscontrole**

De evolutie in de automatisering van seriegewijze naar postgewijze verwerking is vooral van invloed geweest op de bevoegdheidscontrole bij gemeenschappelijk gebruik van hulpbronnen. Dit kwam reeds ter sprake in de paragrafen 2.4 en 2.6.

Het komt er op neer dat het effectueren van de functiescheiding steeds meer afhankelijk wordt van de wijze waarop de toegangscontrole in de EIV is geregeld.

Dit betekent dat leiding en accountant in toenemende mate afhankelijk worden van een beperkt aantal (soms één) functionarissen die het toegangsbeveiligingsmechanisme in de vorm van één of meer functiematrices beheersen.

Aangezien de accountantscontrole per definitie afhankelijk is van de onvervangbare interne controle door middel van functiescheidingen, is het onderzoek naar en de controle van het systeem van toegangsbeveiliging een onontkoombare noodzaak.

Het probleem wordt in belangrijke mate vergroot door het feit dat de automatiseringsindustrie in het algemeen niet voldoende doordrongen is van de noodzaak om vanuit de hardware de beveiliging te regelen.
Wel zijn tal van softwarematige beveiligingen mogelijk, doch deze kunnen meestal weer op eenvoudige wijze worden doorbroken of omzeild. Dit betekent een verhoogde risicofactor met het oog op de veelal onvervangbare maatregelen ten behoeve van de interne controle.

Advisering over opzet en bewaking van een gerealiseerd toegangscontrolesysteem is een belangrijke taak van EIV-accountant en EDP-auditor.

De in dit verband in onderlinge relatie te onderzoeken en eventueel te controleren objecten zijn:
- het besturingssysteem;
- de teleprocessingmonitor;
- het gegevensbeheerssysteem;
- applicatieprogramma's en standaardpakketten;
- de eventueel in gebruik zijnde overkoepelende beveiligingssoftware;
- eventueel de architectuur van de hardware.

5.7 **Conversie**

Naar de onderdelen waaruit een automatiseringssysteem bestaat kan men, bij de overgang van een bestaande naar een nieuwe situatie, spreken van conversie van:
- computers;
- besturingssystemen;
- programma's;
- gegevensverzamelingen.

Iedere soort conversie brengt zijn eigen problematiek mee en meestal is het niet zo dat conversie van het ene deel de rest niet beroert. Vooruitlopend op een conversie van welke aard dan ook dient een conversieplan te worden opgezet waarin de verschillende aspecten, waaronder de onderlinge beïnvloeding en de controle op de conversie, dienen te worden bekeken.

Men spreekt in het algemeen van technische conversie indien er inhoudelijk vanuit de toepassing gezien niets verandert aan het informatiesysteem. Vanuit de automatiseringsdiscipline behoeft dan de gebruiker niet te worden ingeschakeld. Deze zienswijze is niet altijd terecht en verdient een kritische benadering van de gebruiker en accountant.

5.8 De invloed van de kleinschalige automatisering op de accountantscontrole

Zoals in 2.3 geschetst heeft de komst van kleine doch krachtige computerapparatuur het beeld van de automatisering sterk veranderd.

In die ondernemingen waar de computer als centraal verwerkingsorgaan reeds lang in gebruik was kon, vanuit het oogpunt van beheersing en derhalve ook van interne controle, van een redelijk niveau worden gesproken. Dit niveau was dikwijls eerst na vele jaren bereikt.

Kleinschalige automatisering door middel van minicomputers en microcomputers dreigen de organisatorische verworvenheden uit de grootschalige automatisering te verdringen. De uitgangspunten van betrouwbaarheid wat betreft juistheid, volledigheid, autorisatie en beveiliging van de verwerking blijven gelijk doch dienen, doordat een nieuwe generatie gebruikers van apparatuur aantreedt, opnieuw onder de aandacht te worden gebracht.

Voor wat betreft de toegangscontrole ontstaat zeker bij kleine installaties een nieuwe problematiek omdat nog slechts weinigen direct bij de verwerking zijn betrokken en doorbreking van functiescheidingen voor de hand ligt.

Onder verwijzing naar 4.3.3 wordt hier nog eens gewezen op de te verwachten betekenis van het gebruik van de microcomputer voor de accountant.

5.9 Fysieke beveiliging en accountant

Een niet geheel te verwaarlozen terrein voor de accountant is dat van de fysieke beveiliging van computercentra of decentraal geplaatste apparatuur programma's en informatiedragers. Over de diepgang van het onderzoek en de verantwoordelijkheid van de accountant voor de fysieke beveiliging in het kader van de jaarrekeningcontrole wordt verschillend gedacht.

De betekenis van goede beveiligings- en reconstructiemaatregelen laat zich onderscheiden naar die voor:
- administratie en verslaggeving;
- operationele bedrijfsprocessen.

Van de accountant kan op z'n minst worden verwacht dat hij zich ervan vergewist dat directie en leiding van de EIV-organisatie, zich rekenschap hebben gegeven van de risico's die tijdelijk of langdurige uitval van de verwerking met zich brengen. Hij dient zich globaal op de hoogte te stellen van de getroffen maatregelen met een marginale toetsing van de effectiviteit ervan.

De technische kennis welke voor een beoordeling van de effectiviteit van getroffen maatregelen nodig is gaat meestal boven het kennispakket van zowel de EIV-accountant als de EDP-auditor uit.
Voor hen ligt er wel een werkterrein waar het gaat om de controle op de naleving van de procedures en voorschriften die ter zake gelden.

Het geheel van maatregelen van preventieve beveiliging dient te worden gedragen door een duidelijk beveiligingsbeleid, gecompleteerd door een calamiteitenplan en een noodvoorzieningenplan dat in werking moet treden indien zich ernstige storingen voordoen.
Bij het regelmatig testen van de effectiviteit van een dergelijk plan kan de EDP-auditor een rol spelen.

5.10 **Computersabotage**
Een met beveiliging samenhangend doch van het werkterrein van de accountant en zelfs van de EDP-auditor nogal verwijderd onderwerp is dat van de sabotage door middel van aanslagen op rekencentra of via verborgen routines in programmatuur. Met name de laatste vorm van sabotage kan preventief worden bestreden door een goed personeelsbeleid en door organisatorische maatregelen gericht op gestructureerd en gedocumenteerd programmeren gevolgd door toezicht en een permanente testorganisatie.

5.11 **Automatisering, fraude en accountant**
De komst van de computer heeft een nieuw terrein geopend voor fraudeurs.
De accountant is in beginsel niet verantwoordelijk voor het ontdekken van fraudes, doch het niet ontdekken van grote of systematische fraudes kan hem worden aangerekend indien hij deze uit hoofde van zijn jaarrekeningcontrole had moeten ontdekken.

De literatuur, vooral de Amerikaanse, vermeldt vele gevallen van misbruik van en met behulp van de computer, waaronder fraudes van dikwijls omvangrijke aard. Bedacht dient te worden dat het nooit de computer is die fraudeert maar altijd de mens. Dat de computer daarbij een hulpmiddel kan zijn is evident.

5.12 **EIV en risico-analyse**
Een van de moeilijkste zaken in de organisatiekunde en derhalve in de interne controle is het bepalen van de effectiviteit van getroffen maatregelen. Dit geldt uiteraard evenzeer voor de EIV als onderdeel van de administratieve organisatie.

Niettemin zijn er, weliswaar globale, methoden ontwikkeld waarmee via een systematische benadering calculaties te maken zijn van het schadebedrag bij disfunctioneren van (deel)systemen tegenover de kosten van de te treffen voorzieningen. Het voordeel van een dergelijke risicoanalyse is wellicht niet zozeer gelegen in de afweging van de kosten/nutverhoudingen als wel in de systematische benadering van het afbreukrisico bij disfunctioneren van een (deel)systeem.

5.13 **Betalingsorganisatie en EIV**
Hoewel voor vele onderdelen van de organisatie en de daarop betrekking hebbende automatisering specifieke opmerkingen zijn te maken wordt dit hier niet gedaan. Een uitzondering wordt gemaakt voor de organisatie van het betalingsverkeer in relatie tot de EIV.

Anders dan in landen met chequeverkeer als voornaamste middel tot betalen, beschikt Nederland over een systeem van giraal verkeer dat buitengewoon sterke waarborgen biedt tegen fraude bij betalingen, gezien de directe terugmelding van uitgevoerde betalingen.

De verdere automatisering van het betalingsverkeer door het met behulp van betaaltapes overdragen van detailinformatie met betrekking tot betalingen aan de bank- en postgiro-instellingen, vereist nadere maatregelen van interne controle.
Deze worden mede nodig doordat de in gebruik zijnde betalingssystemen bij huishoudingen somtijds betalingen genereren die niet meer in detail worden gecontroleerd voordat de opdracht naar bank of giro wordt gezonden.

Betrokkenheid bij de opzet en vooral blijvende controle op de uitvoering zijn zaken waar (EIV)-accountant en EDP-auditor dienen te worden ingeschakeld, gezien de kritische betekenis van de uitgaande geldstroom.

5.14 **Kantoorautomatisering en interne controle**
Op het eerste gezicht zal de kantoorautomatisering geen directe invloed hebben op de interne controle voor zover van betekenis voor de accountantscontrole. Het kan echter voorkomen dat koppelingen tot stand worden gebracht waarbij zodanige integratie van verwerking en gezamenlijk gebruik van gegevens zich voordoet, dat ook de kantoortoepassingen in het onderzoek en de controle van de accountant moeten worden betrokken.

Bij toepassing van lokale netwerken is het reeds zo dat apparatuur, welke vooral bestemd is voor het bijhouden van adressenbestanden, tekstverwerking, telexverkeer en elektronische post, gekoppeld is aan grotere computers. De toegangscontroleproblematiek speelt hier reeds een rol.

Uit oogpunt van administratieve organisatie en ten behoeve van eigen gebruik dient de vooruitgang van de automatisering van het kantoor zeker te worden gevolgd.

5.15 **Privacywetgeving en accountant**
In 1976 heeft de "Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistraties" (de zogenaamde commissie Koopmans) een eindrapport uitgebracht waarin een voorstel tot wettelijke regeling is opgenomen.
Inmiddels is op 30 november 1981 een ontwerpwet aan de Tweede Kamer aangeboden.
Sinds die tijd is er op wetgevend gebied niets gebeurd.

Het is duidelijk dat bij een eventuele in werking treden van een Privacywet de accountant hiermede te maken krijgt, aangezien maatregelen ten behoeve van interne controle de bescherming van gegevens mede dienen te waarborgen.

De vraag in hoeverre de accountant een actieve rol zou kunnen vervullen in het kader van de wet is nog niet beantwoord aangezien de nadere detaillering van de functie van de Registratiekamer, door middel van algemene maatregelen van bestuur, zal moeten worden geregeld.

5.16 **Grensoverschrijdend gegevensverkeer**
De vrees voor het ongecontroleerd wegvloeien van informatie heeft sommige landen (bijvoorbeeld Frankrijk) ertoe gebracht regels op te stellen met betrekking tot de uitvoer van informatie.
Tot nu toe hebben deze regels weinig effect gesorteerd.
Men tracht in mondiaal verband te inventariseren welke maatregelen van overheidswege in de verschillende landen bestaan.

De algemene opvatting binnen het OECD, die zich onder meer met deze zaak bezighoudt, is dat er vrijheid van gegevensverkeer dient te zijn.

5.17 **Data encryption**
Naarmate meer gegevens over openbare lijnen en netwerken worden verzonden neemt de behoefte om de gegevens in niet voor derden leesbare vorm te versluieren toe. Hierbij past ook de wens om vast te stellen dat gegevens welke verzonden worden goed aankomen en bij de juiste persoon of organisatie arriveren.
Omgekeerd wil ook de ontvanger weten of hij de juiste gegevens van een tot verzenden bevoegde persoon ontvangt. Er zijn enige, op mathematische grondslag gebaseerde, methoden ontwikkeld.

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

100 + 50 - 20 = 80 ??????????
De betekenis van Concurrency Control

door A. van der Drift

A formal Criterion for Correctness

Any serializable execution of a given set of concurrent transactions can be considered correct, in the sense that it produces the same result as running those transactions one at the time in some arbitrary sequence.

C.J. Date
5th International Conference on V.L.D.B. *

1. INLEIDING

In dit artikel volgt een uiteenzetting over het automatiseringsbegrip Concurrency Control. Het doel hiervan is de accountant inzicht te verschaffen over dit technische en veel voorkomende begrip, dat zeker in een online-omgeving van bijzondere invloed is op de betrouwbaarheid van de gegevensverwerking.
Met dit inzicht dient de accountant in staat te zijn gevaren op dit gebied te onderkennen en waar nodig de gespecialiseerde EDP-auditor gericht in te zetten.

Achtereenvolgens worden een aantal problemen gesignaleerd, waarvoor oplossing worden gegeven met vermelding van de daaraan gerelateerde consequenties.
Vervolgens zal worden ingegaan op een situatie, waarin de bestaande oplossingen veelal niet adequaat zullen werken, waardoor aandachtsgebieden voor de EDP-auditor ontstaan.

2. PROBLEMEN TEN GEVOLGE VAN HET GELIJKTIJDIG GEBRUIK VAN RESOURCES

U en bijvoorbeeld uw dochter menen op hetzelfde moment gebruik te moeten maken van een en dezelfde auto (resource).
Indien beiden gelijktijdig de besturing in handen hebben, zal de beslissende T-kruising niet worden genomen zoals eenieder van u dit vooraf voor ogen had.
Mede gezien het geschetste gevaar zal naar alle waarschijnlijkheid vooraf een bepaalde regeling tot stand zijn gebracht voor het gebruik van de auto, al dan niet onder invloed van uw dochter's lieftalligheid danwel uw ouderlijke macht (de dominantie is hierbij arbitrair).

* VLDB = very large data bases

In de automatisering zijn veelal meerdere applicaties gelijktijdig actief.
Indien meer dan een applicatie gebruik maakt van dezelfde resource kunnen zich eveneens problemen (weliswaar van een andere - niet fysieke - orde) voordoen.
Deze problemen kunnen zijn:
- het verliezen van mutaties;
- het foutief herstellen van de database;
- het onjuist verkrijgen van informatie.

Genoemde problemen worden navolgend geïllustreerd.

Het verliezen van mutaties

Figuur 2.1 geeft in de tijd gezien de acties weer van twee applicaties (A en B), die hetzelfde record uit een bestand (database) gelijktijdig muteren.

Figuur 2.1.

Tijd	Applicatie A	Inhoud record	Applicatie B
t0	-	100	-
t1	READ record	100	-
t2	-	100	READ record
t3	100 + 50 = 150	100	-
t4	-	100	100 - 20 = 80
t5	WRITE record	150	-
t6	-	80	WRITE record
t7	-	80	-

Indien de applicaties achtereenvolgens zouden worden uitgevoerd, zou na beëindiging van beiden de inhoud van het record (100 + 50 - 20 =) 130 moeten zijn.
Doordat zowel applicatie A als B vanuit eenzelfde startwaarde gaan muteren zal alleen het laatst weggeschreven resultaat, in dit geval van B gelden. Hierdoor valt de wijziging van applicatie A tussen de wal en het schip.

Het foutief herstellen van de database

Figuur 2.2 geeft in de tijd gezien de acties weer van twee applicaties (A en B), die weliswaar achtereenvolgens hetzelfde record muteren, maar waarbij de eerste applicatie na mutatie door de tweede toch nog invloed uitoefent op de inhoud van het (inmiddels 2x) gemuteerde record.

In dit voorbeeld vindt een database/transaction-rollback (transaction-backout) plaats. Voor een gedetailleerde uitleg hiervan wordt hier volstaan met een verwijzing naar deel 2 van het artikel van R. Bron over Backup, Restart en Recovery (Compact nr. 33, herfst 1983).

Figuur 2.2

Tijd	Applicatie A	Inhoud record	Applicatie B	Log info
t0	-	100	-	
t1	READ record	100	-	
t2	100 + 50 = 150	100	-	
t3	WRITE record	150	-	old: 100 new: 150
t4	-	150	READ record	
t5	-	150	150 - 20 = 130	
t6	-	130	WRITE record	old: 150 new: 130
t7	ROLLBACK	100	-	old: 100 new: 100
t8	-	100	-	

De inhoud van het record zou na de verwerking van beide applicaties (100 + [50 - 50] - 20 =) 80 moeten zijn, omdat applicatie A door middel van een "ROLLBACK" aangeeft zijn mutatie te willen annuleren.
In dit voorbeeld heeft applicatie B, na mutatie en nog voor annulering door applicatie A, hetzelfde record echter al gemuteerd.
Door de uitgevoerde "ROLLBACK" zal de inhoud van het record, zoals deze is gewijzigd door A, worden teruggeplaatst, waardoor de mutatie van applicatie B verloren gaat.

Het onjuist verkrijgen van informatie

Ook bij het eenvoudig opvragen van gegevens kunnen fouten ontstaan ten gevolge van het gelijktijdig gebruik van een en dezelfde resource door meer dan een applicatie.
Figuur 2.3 illustreert dit. In dit voorbeeld leest applicatie A uitsluitend records en telt de inhoud hiervan, terwijl applicatie B tussentijds de door A gelezen en nog niet gelezen records wijzigt.

Figuur 2.3

Tijd	Applicatie A	Records	Applicatie B
t0	-		-
t1	READ record 1	Record 1 = 40	-
t2	0 + 40 = 40		-
t3	READ record 2	Record 2 = 50	-
t4	40 + 50 = 90		-
t5	-	Record 3 = 30	READ record 3
t6	-		record 3 = 30 - 10
t7	-	Record 3 = 20	WRITE record 3
t8	-	Record 1 = 40	READ record 1
t9	-		record 1 = 40 + 10
t10	-	Record 1 = 50	WRITE record 1
t11	READ record 3	Record 3 = 20	-
t12	90 + 20 = 110		-
t13	totaal = 110		-

De waarde van de records 1, 2 en 3 te zamen is 120. Door de tussentijdse verwerking van applicatie B telt applicatie A slechts de waarde 110.
Het bestand zal na beëindiging van beide applicaties desalniettemin juiste informatie bevatten. Uitsluitend de resultaten van applicatie A zijn derhalve foutief.

3. MAATREGELEN TEN BEHOEVE VAN CONCURRENCY CONTROL

Voorafgaande voorbeelden toonden de noodzaak tot adequate, centraal gestelde maatregelen teneinde wederzijdse beïnvloeding van applicaties te voorkomen. In dit hoofdstuk wordt hierop ingegaan.

Indien een applicatie (lees ook proces, programma, transactie) op een bepaald moment als enige gebruik maakt van een bepaalde resource bestaan er geen problemen, zoals geschetst in het voorgaande hoofdstuk. Als dus meerdere applicaties gebruik zouden maken van dezelfde resource, zouden er geen problemen bestaan, indien deze applicaties dit volgtijdelijk (serieel) zouden doen.
De maatregelen ten behoeve van Concurrency Control (Samenwerkingsregeling) zijn er dan ook op gericht ervoor zorg te dragen dat het gebruik van resources serieel plaatsvindt.
Dit wordt bereikt door applicaties op elkaar te laten wachten ten behoeve van het gebruik van een gemeenschappelijk resource. Indien bijvoorbeeld een applicatie aan het Operating System verzoekt om gebruik van een bestand (door middel van een OPEN-instructie), zal het O.S. pas dan de applicatie toestemming geven tot bestandsgebruik, indien geen andere applicatie het gevraagde bestand reeds in gebruik heeft.

Is dit laatste wel het geval, dan zal het O.S. de vragende applicatie laten wachten totdat de reeds gebruikende applicatie beëindigt c.q. door middel van een CLOSE-instructie aangeeft het bestand niet langer meer nodig te hebben.
De genoemde maatregel, die door het O.S. wordt uitgevoerd, kent een (soms onacceptabel) bezwaar, namelijk alle gegevens uit het gealloceerde bestand zijn gedurende een bepaalde tijd voor slechts een applicatie beschikbaar.
Idealer zou zijn, indien de allocatie niet op bestandsniveau maar tenminste op record-niveau zou plaatsvinden.
Neem in herinnering dat het gaat om een samenwerkingsregeling tussen meerdere applicaties voor wat betreft het gelijktijdig gebruik van een in beschouwing genomen resource. Bedenk daarbij dat: hoe kleiner de resource, des te groter zijn beschikbaarheid.
Het verwerken van een geheel bestand duurt immers langer dan de verwerking van een enkel record en indien toch slechts een enkel record wordt verwerkt dan zullen, indien op bestandsniveau wordt gealloceerd, toch ook alle overige records gedurende die (weliswaar geringe) tijd niet beschikbaar zijn.

Door onder meer het gebruik van online-applicaties, waarmee diverse (eind)-gebruikers, met zowel identieke als verschillende bevoegdheden, gelijktijdig gebruik maken van gegevens, die in een en hetzelfde bestand zijn opgenomen (voor de eenvoud spreken wij verder van de database), dient op een lager niveau (kleinere resource) een regeling plaats te vinden. In het algemeen wordt hierbij de samenwerking tussen twee of meerdere applicaties op record-niveau geregeld niet door het O.S. maar door het Data Base Management System (DBMS).

Een applicatie verzoekt aan de beherende software (het DBMS) om het gebruik van een record.
Hierdoor zal de applicatie im- danwel expliciet aan het DBMS verzoeken dit record uitsluitend aan hem ter beschikking te stellen.

Maatregel 1

Indien geen andere applicaties hiervan reeds gebruik maken, zal het DBMS een soort 'lock' plaatsen op het gevraagde record ten behoeve van de verzoekende applicatie. (Het plaatsen van een zogeheten 'lock' betekent in de praktijk dat het DBMS bijhoudt op disk of in het geheugen welke applicatie welk record gebruikt.)
Andere applicaties zullen door de geplaatste 'lock' geen toegang krijgen tot het record, totdat de lock door een im- of expliciet verzoek van de eerste applicatie aan het DBMS wordt opgeheven.
Hiermee wordt het probleem uit figuur 2.1 (het verliezen van mutaties) opgelost; echter nog niet de problemen uit de figuren 2.2 en 2.3 (het foutief herstellen van de database en het onjuist verkrijgen van informatie).

Maatregel 2

Het DBMS zal niet toestaan, dat records door een applicatie worden vrijgegeven ('unlocked'), indien deze applicatie vervolgens nieuwe records (dus automatisch nieuwe locks) zal aanvragen.
Praktisch gezien, zal het DBMS de locks niet verwijderen, indien de applicatie niet uitdrukkelijk te kennen geeft het DBMS geen verzoeken meer te zullen doen. Hierdoor worden ook de problemen uit de figuren 2.2 en 2.3 opgelost c.q. voorkomen.

4. DEAD-LOCK (DEADLY EMBRACEMENT)

De maatregelen uit het voorafgaande hoofdstuk zijn adequaat; in sommige gevallen echter te adequaat.
In dit hoofdstuk wordt het probleem van Dead-lock onder de aandacht gebracht; een situatie waarbij twee of meerdere applicaties onder invloed van het locking-mechanisme elkaars verwerking blokkeren (zie figuur 4.1).

Figuur 4.1

Tijd	Applicatie A	Applicatie B
t0	-	-
t1	READ record 1 (lock record 1 voor A)	-
t2	-	READ record 2 (lock record 2 voor B)
t3	READ record 2 (wacht op einde B)	-
t4	-	READ record 1 (wacht op einde A)
t5	-	-

Achtereenvolgens wordt door toedoen van applicatie A record 1 en door toedoen van applicatie B record 2 gelezen en gelocked, waarna applicatie A op de beëindiging van applicatie B moet wachten teneinde record 2 te kunnen gebruiken en applicatie B op de beëindiging van applicatie A om record 1 te kunnen gebruiken.
Beide applicaties wachten dus op elkaar.
Een nog complexere vorm zal worden aangetroffen indien meer dan twee applicaties op elkaar wachten (bijvoorbeeld A wacht op B, B wacht op C en C wacht op A).

Na constatering van de zogeheten Dead-lock-situatie is het oplossen van het ontstane probleem even simpel als doeltreffend, namelijk: breek de verwerking van een van de betrokken applicaties af.

Indien de applicaties A en B uit figuur 4.1 batch-applicaties zijn, zal veelal de computer-operator (na verloop van tijd) constateren, dat de applicaties niet vorderen in hun verwerking. Op grond van onder meer beschikbare documentatie en/of advies van bijvoorbeeld de data-base-administrator zal hij een van de applicaties 'cancelen'. De keuze van applicatie dient op grond van de beantwoording van de volgende vragen te geschieden:

- hoe ver in verwerkingstijd is de applicatie gevorderd (met andere woorden: hoeveel tijd wordt verloren met het vanaf het begin overnieuw uitvoeren van de applicatie?
- is het eenvoudig om de door de applicatie reeds aangebrachte data-base-wijzigingen terug te draaien tot op de situatie van vóór de aanvang van de applicatie (Rollback-situatie)?
- kan een eventuele herstart van de applicatie eenvoudig plaatsvinden (mede in relatie tot het voorafgaande)?

Deze complexe vragen maken de gedane keuze van de operator in de praktijk wel eens arbitrair.

Indien de applicaties A en B uit figuur 4.1 online-applicaties zijn, zal veelal de beherende software (DBMS/TP-monitor) een op willekeur gebaseerde keuze maken.
Kortom: de oplossing is even gruwelijk als de naam voor het geconstateerde probleem (bij een dodelijke omarming het doden van een van de betrokkenen).

In de praktijk zal het veelal niet mogelijk zijn Dead-lock-situaties volledig te voorkomen. De volgende punten zijn echter wel van invloed op de frequentie, waarmee Dead-locks zich kunnen voordoen:

- de opslag van gegevens (de wijze waarop de benodigde gegevens zijn verdeeld over apparatuur, bestanden, delen van bestanden en records);
- de gebruikte lock-soorten en granulatie (zie hoofdstuk 5);
- het aantal concurrent applicaties (hoe meer concurrent applicaties, des te groter de kans op Dead-locks).

In het algemeen geldt: hoe groter de mate van beschikbaarheid van de resource, des te geringer de kans op Dead-locks tenzij op het allerhoogste niveau locking plaatsvindt, waarbij nagenoeg geen concurrent processing kan plaatsvinden.

De niet of minder in de techniek geïnteresseerde lezer kan vervolgen met hoofdstuk 6. Hoofdstuk 5 geeft slechts een technische verdieping van de maatregel ten behoeve van Concurrency Control.

5. LOCKS: SOORTEN? NIVEAU EN IMPLEMENTATIEPRINCIPES

Soorten

Tot nu toe is van de beperking uitgegaan dat slechts één applicatie een bepaald record gelijktijdig mag gebruiken. Deze beperking is niet altijd noodzakelijk c.q. gewenst. Het lezen zou bijvoorbeeld door meerdere applicaties gelijktijdig mogen plaatsvinden. Hierdoor vindt immers geen onderlinge beïnvloeding plaats.

Zo ook zullen update-applicaties geen hinder ondervinden, indien andere applicaties dezelfde records gelijktijdig lezen. Lezende applicaties zouden het echter wel eens hinderlijk kunnen vinden, indien andere applicaties het record gelijktijdig wijzigen (zie bijvoorbeeld figuur 2.3).
Derhalve bestaan er veelal verschillende soorten locks, waarom door applicaties kan worden verzocht.
De volgende soorten kunnen worden onderkend:

- U-LOCK: de applicatie verzoekt om het wijzigen van records, waarbij niet wordt toegestaan dat andere applicaties het bestand benaderen.
- SUR-LOCK: de applicatie verzoekt om het wijzigen van records, waarbij uitsluitend andere lezende applicaties worden toegestaan, die niet de gewijzigde records benaderen.
- R-LOCK: de applicatie verzoekt om het lezen van records, waarbij uitsluitend andere lezende applicaties in het bestand worden toegestaan.
- SU-LOCK: de applicatie verzoekt om het wijzigen van records, waarbij andere applicaties tot het bestand worden toegestaan, voor zover deze niet gebruik maken van de gewijzigde records.
- SR-LOCK: de applicatie verzoekt om het lezen van records, waarbij andere applicaties worden toegestaan voor zover deze niet de gelezen records wijzigen.

(Voor alle duidelijkheid zij opgemerkt dat met een update-permissie tevens mag worden gelezen en binnen een enkel DBMS niet alle soorten zullen worden ondersteund.)

Uit de opsomming van lock-soorten blijkt dat bepaalde locks met andere locks conflicteren. Dit wordt nader getoond in de matrix van figuur 5.1. De 'C' geeft hierin een conflict aan. Indien een conflict optreedt zal de applicatie, die als laatste om het record (en daarmee om de lock) heeft verzocht, moeten wachten.

De "(c)" geeft pas dan een conflict indien door beide applicaties gebruik wordt gemaakt van een en hetzelfde record.

Figuur 5.1

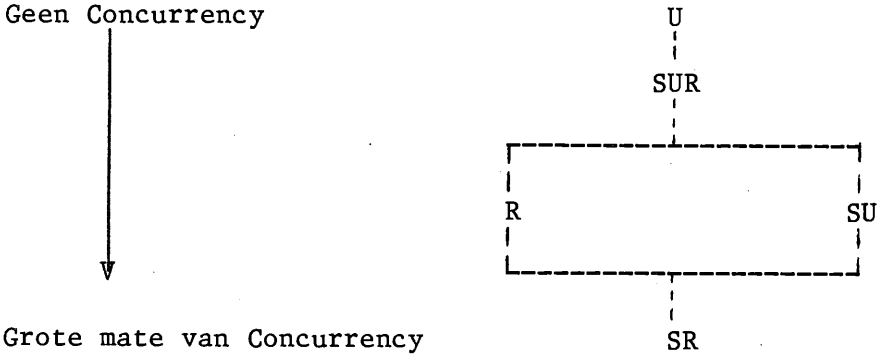
LOCKS	U	R	SUR	SU	SR ← applicatie B
U	C	C	C	C	C
R	C	-	C	C	-
SUR	C	C	C	C	(c)
SU	C	C	C	(c)	(c)
SR	C	-	(c)	(c)	-

↑

applicatie A

De genoemde locks verschillen in de mate, waarin samenwerking (concurrent processing) tussen applicaties mogelijk is. Bij de U-LOCK is dit bijvoorbeeld niet mogelijk; bij de SR-LOCK is meer samenwerking mogelijk.
Figuur 5.2 toont een onderlinge verhouding met betrekking tot samenwerking.

Figuur 5.2



Concurrency niveau

Uit de verhandeling over beschikbaarheid (hoofdstuk 3) bleek dat Concurrency Control geregeld kan worden op verschillende niveaus. De volgende niveaus kunnen worden onderkend:
- apparaatniveau (voorbeeld: het O.S. zal aan slechts één applicatie gelijktijdig een Tape-unit toewijzen);
- bestandsniveau (voorbeeld: het O.S. zal aan slechts één applicatie gelijktijdig een Disk-bestand toewijzen);
- delen van bestandsniveau (voorbeeld: het DBMS zal dit toewijzen; veelal met betrekking tot I/O-blocks);
- recordtypeniveau (voorbeeld: het DBMS zal dit toewijzen);
- recordniveau (voorbeeld: het DBMS zal dit toewijzen);
- delen van recordniveau (de ideale maar helaas weinig aangetroffen toewijzing door het DBMS).

In de praktijk zullen niet alle niveaus worden onderkend binnen een bepaalde beherende software. Op welk niveau in een concrete situatie zal worden gelocked hangt soms af van de applicatie, die om locking verzoekt, en de beperkingen in de mogelijkheden van de beherende software, die de Concurrency Control uitvoert. De applicatie, die echter om een U-LOCK verzoekt, verzoekt daarmee om Concurrency Control op bestandsniveau; de applicatie met een SR-LOCK verzoekt om Concurrency Control op recordniveau.

Implementatieprincipes

Uit het voorafgaande kunnen onder meer de navolgende principes worden afgeleid, die betrekking hebben op de implementatie van Concurrency Control in de beherende software:

- de beherende software kan zonder enig risico op een hoger niveau locken, dan waarom door de applicatie is verzocht (voorbeeld: de applicatie verzoekt om een lock op recordniveau; de software plaatst de lock op bestandsniveau);
- de beherende software kan, zonder enig risico, de locks langer handhaven dan voor de applicatie strikt noodzakelijk is (voorbeeld: de applicatie verzoekt om een bestand; het O.S. alloceert het bestand gedurende de draaitijd van de gehele job in plaats van de tijd van de jobstep, die de applicatie bevat);
- de beherende software kan een verzoek om een lock zonder enige risico behandelen als een verzoek om een zwaardere lock (voorbeeld: de applicatie verzoekt om een SU-LOCK; de software voert daarvoor een U-LOCK uit).

Indien de beherende software op een hoger niveau locking uitvoert, de locks langer handhaaft en zwaardere locks toepast, benadeelt dat de samenwerkingsmogelijkheden en daarmee in een online-omgeving veelal de performance.
Tevens vergroot dit de kans op Dead-locks, door de afname in beschikbaarheid van de resource (zie hoofdstuk 4).

6. AANDACHTSGEBIED VOOR DE EDP AUDITOR

Hoofdstuk 2 bevatte een opsomming van problemen ten gevolge van het gelijktijdig gebruik van resources door meerdere applicaties. In hoofdstuk 3 werden daarvoor oplossingen aangedragen, die echter van nadelige invloed konden zijn op de beschikbaarheid van gegevens.
Door de genoemde oplossingen (maatregelen) op een zo laag mogelijk niveau (onder meer recordniveau) toe te passen, kon toch een acceptabele beschikbaarheid worden verkregen.
In hoofdstuk 4 kwam nog een vervelende situatie naar voren, namelijk Dead-locks, waarvoor tot dusver geen directe oplossingen bestaan. Dit laatste probleem schaadt echter niet de betrouwbaarheid maar meer de snelheid, waarmee een aantal applicaties gelijktijdig kunnen worden verwerkt.

In dit laatste hoofdstuk zal geconstateerd worden, dat ondanks de genoemde maatregelen door toedoen van een aantal factoren de betrouwbaarheid van de gegevensverwerking nadelig kan worden beïnvloed ten gevolge van het gelijktijdig gebruik van resources door meerdere applicaties.
Gelet op dit nog nader toe te lichten feit, verdient deze problematiek dan ook de aandacht van de EDP-auditor.

De effectiviteit van de maatregelen ten behoeve van Concurrency Control is in het algemeen afhankelijk van:
- de beherende software (voorbeeld: het O.S. en het DBMS);
- de applicaties, die verzoeken om het gebruik en het locken van bestanden/records;
- de automatiseringsorganisatie, waarin enerzijds de beherende software wordt geïnstalleerd, ter beschikking wordt gesteld en onderhouden; anderzijds de applicaties worden ontwikkeld en uitgevoerd.

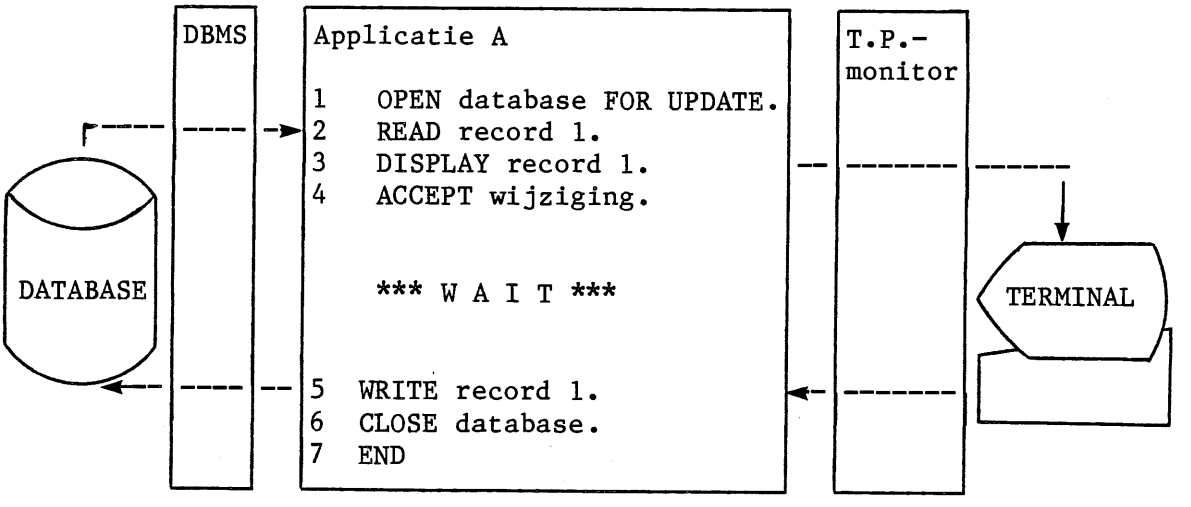
Beherende software

De beherende software is veelal standaardprogrammatuur van een hard/software-leverancier. Als gevolg daarvan zullen eventueel noodzakelijke aanbevelingen voor wat betreft de door de EDP-auditor geconstateerde tekortkomingen terzake niet of nauwelijks invloed hebben op de inhoudelijkheid van deze programmatuur; althans niet op afzienbare termijn.

Applicaties

Veelal wordt Concurrency Control door de beherende software (al dan niet op grond van installatie-opties) standaard toegepast. Applicaties hebben op de effectiviteit daarvan nauwelijks invloed. Figuur 6.1 toont een voorbeeld, waarin een online-applicatie via het DBMS gegevens gebruikt uit een database. In dit voorbeeld wordt uitgegaan van het adequaat locken door het DBMS op recordniveau.

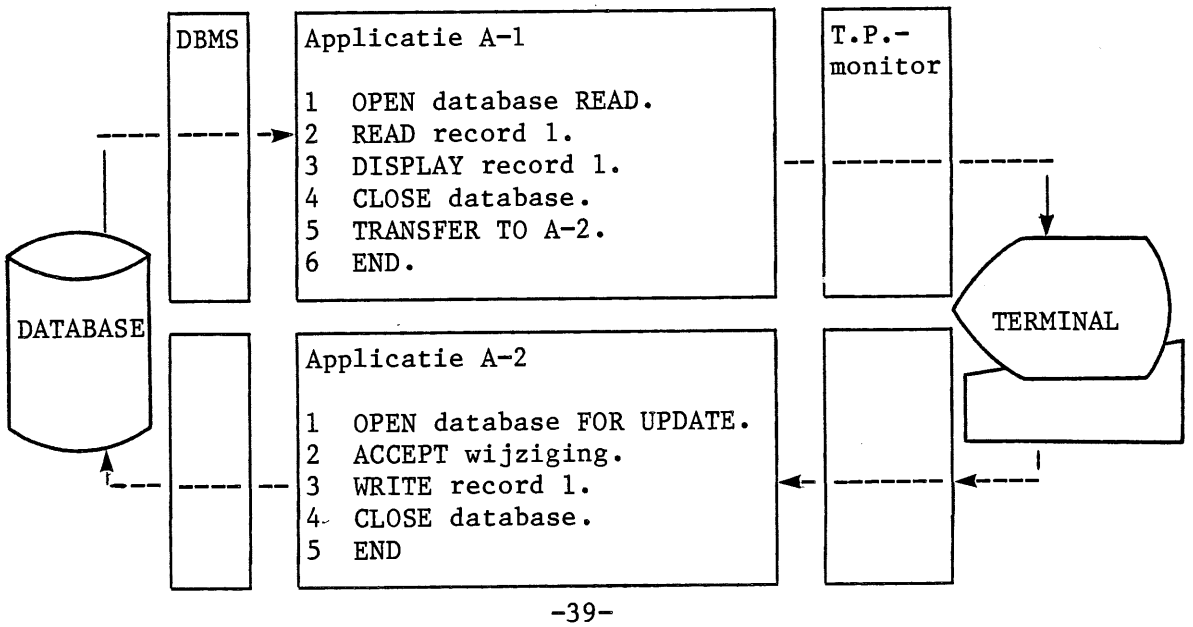
Figuur 6.1



Instructie 1 verzoekt het DBMS om de database te lezen en te wijzigen. Op grond hiervan zal het DBMS alle records, die zullen worden gelezen en/of gewijzigd, locken totdat applicatie A te kennen geeft geen records meer te zullen gebruiken. Instructie 2 verzoekt aan het DBMS om record 1. Het DBMS zal het record, indien niet reeds gelocked, aan de applicatie ter beschikking stellen en ten behoeve hiervan locken, zodat geen andere applicaties hetzelfde record kunnen gebruiken.
Instructie 3 respectievelijk 4 maakt het gelezen record op de gebruikersterminal zichtbaar en verzoekt om wijziging.
Totdat de gebruiker heeft geantwoord (bijvoorbeeld na de koffiepauze) blijft de applicatie in het geheugen van de computer wachten en het gelezen record gelocked.
Na beantwoording wijzigt instructie 5 het record in de database, waarna instructie 6 aan het DBMS te kennen geeft geen verdere records te zullen gebruiken. Het DBMS zal na deze instructie ook geen verzoek van deze applicatie meer in behandeling nemen, tenzij zo'n verzoek wordt vooraf gegaan door een instructie zoals instructie 1, waarmee de applicatie aangeeft een nieuwe transactie (in dit voorbeeld het muteren van een database-record) te willen verwerken.
Het DBMS zal op grond van instructie 6 alle tot dan toe ten behoeve van deze applicatie geplaatste locks opheffen, waarmee de gebruikte records vrijkomen voor andere applicaties.

De opzet van applicatie A uit figuur 6.1 kent een groot bezwaar, namelijk het onnodig lang alloceren van geheugenruimte en records door het wachten op een gebruikersinteractie (wederom een beschikbaarheidsprobleem).
Derhalve zal veelal voor een andere opzet van applicaties worden gekozen, waardoor de beschikbaarheid alsmede helaas de problemen ten aanzien van Concurrency Control toenemen. Figuur 6.2 geeft de veranderde opzet weer.

Figuur 6.2



Op het moment dat het gelezen record op de terminal is zichtbaar gemaakt, eindigt applicatie A-1, waardoor de geheugenruimte vrijkomt en de voor applicatie A-1 geplaatste locks worden opgeheven door toedoen van instructie 4. Applicatie A-2 zal (automatisch) door de T.P.monitor worden opgestart, indien de gebruiker de door applicatie A-1 gestelde vraag heeft beantwoord.
Dit betekent evenwel dat, nadat applicatie A-1 is beëindigd en nog voordat applicatie A-2 record 1 heeft gewijzigd (in de tijd dat de gebruiker dus antwoordt), het bewuste record door andere applicaties kan worden gewijzigd.
Deze situatie kan leiden tot het verliezen van mutaties (zie figuur 2.1 in hoofdstuk 2).
Dus ondanks de veelal adequate maatregelen, die geboden worden door de beherende software, kunnen onder invloed van de opzet van applicaties toch nog problemen ontstaan voor wat betreft het gelijktijdig gebruiken van resources door meerdere applicaties.
De in figuur 6.2 getoonde opzet van applicaties zal in de praktijk veel worden aangetroffen, waardoor de maatregelen ten behoeve van Concurrency Control niet effectief zullen zijn.

Derhalve dient de programmeur onder de gegeven opzet van de applicaties hierin speciale voorzieningen op te nemen, waardoor tenminste nog geconstateerd kan worden dat tussentijds records zijn gewijzigd.
In het voorbeeld uit figuur 6.2 zou hij het gelezen record vanuit applicatie A-1 in het geheugen kunnen doorgeven aan applicatie A-2, die nog voor het wijzigen van het record in de database nogmaals dit zelfde record zou moeten lezen en vergelijken met het record van applicatie A-1. Indien de records verschillen dient hij de wijziging niet in de database aan te brengen.
Bij de beoordeling van het technisch ontwerp en de bouw van een informatiesysteem dient hieraan door de EDP-auditor aandacht te worden besteed, teneinde vast te stellen dat voornoemde voorzieningen zijn danwel worden aangebracht.

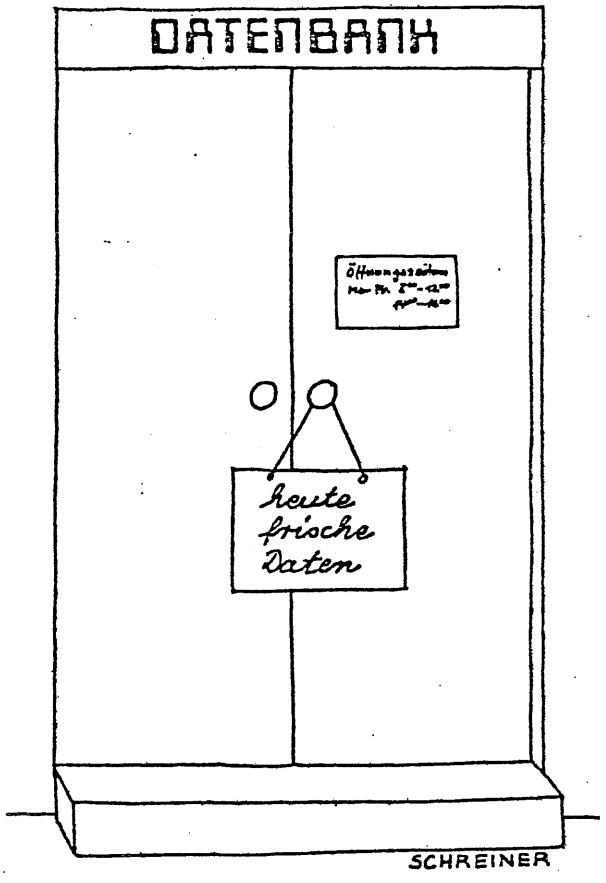
Automatiseringsorganisatie

In het algemeen geldt dat bij tekortkomingen in de mogelijkheden van de beherende software ten aanzien van Concurrency Control door de automatiseringsorganisatie (afdeling Produktie waaronder Werkvoorbereiding en/of Operating) scheduling van applicaties dient plaats te vinden.
Dit houdt in dat voorkomen moet worden dat bepaalde applicaties gelijktijdig worden uitgevoerd. In de gemiddelde automatiseringsorganisatie zal dit in de praktijk niet of nauwelijks mogelijk zijn; zeker niet indien online-verwerking en/of Remote Job Entry (RJE= het op afstand aanbieden van job's) plaatsvindt.

Voornoemde maatregelen, die door de programmeurs moeten worden getroffen in de applicaties, dienen te zijn opgenomen in de ontwikkelingsvoorschriften. De naleving van de voorschriften, gericht op Concurrency Control, dient integraal danwel bij wijze van deelwaarnemingen door bijvoorbeeld de Database-administrator te worden vastgesteld aan de hand van de applicatie-listings.
Door middel van het testen van applicaties komen eventuele tekortkomingen op dit gebied nauwelijks tot uiting.

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

Das Allerletzte



winter 1983/lente 1984

DE MICRO EN DE CONTROLERENDE ACCOUNTANT

door L.N.M. Straathof

In dit artikel worden twee toepassingsgebieden onderscheiden:
- De micro in gebruik bij de cliënt als hulpmiddel bij de bestuurlijke elektronische informatievoorziening (BEIV),
- De micro in gebruik bij de accountant als controlegereedschap.

De vraag wordt behandeld: Wat is de invloed van de micro op de controleplan van de accountant. Dit zowel naar de aard als naar de omvang van de werkzaamheden.

De indeling van dit artikel is als volgt:

1. Inleiding

De ontwikkelingen op het gebied van microcomputers zijn de afgelopen jaren relatief snel gegaan. Werd de microcomputer in eerste instantie voornamelijk gebruikt in de hobbysfeer (spelletjes), nu zien we dat deze steeds meer wordt gebruikt in commerciële toepassingen.
IBM bijvoorbeeld heeft recent een pakket ontwikkeld dat de grootboekadministratie verzorgt met behulp van een personal computer (P.C.), dat wil zeggen een uitgebouwde microcomputer, die meer mogelijkheden biedt dan de hobby-computer.

De verwachting lijkt gerechtvaardigd, dat vooral bij "kleine" organisaties de P.C. steeds meer zal worden gebruikt in zowel de bedrijfsvoering als de administratieve gegevensverwerking.
Bij de laatste kan naast de voornoemde grootboekadministratie worden gedacht aan:
- vastleggen van de gegevens omtrent de primaire bedrijfsprocessen (inkopen, produktie, verkopen e.d.);
- gebruik van spread sheet calculators (Visicalc, Multiplan) voor planningdoeleinden in de ruime zin des woords;
- agendering van afspraken;
- tekstverwerking.

In dit artikel wordt ingegaan op de invloed van de microcomputers op de accountantscontrole, ingeval zij gebruikt worden voor administratieve toepassingen.
Hierbij wordt antwoord gegeven op de vraag in hoeverre de micro, en met name de controles in het besturingssysteem en de toepassingsprogrammatuur, object van onderzoek moet zijn voor de accountant.

Verder wordt aandacht geschonken aan de mogelijkheden die een microcomputer kan bieden als hulpmiddel in de accountantscontrole (auditmicro).
Onder accountantscontrole wordt in dit artikel verstaan: de controle die resulteert in een verklaring bij de jaarrekening.

Functioneel is er geen verschil tussen een microcomputer, een minicomputer en een mainframe. Alle drie kunnen worden gebruikt voor procesbesturing en gegevensverwerking.

Ten opzichte van de minicomputer en de mainframe:
- is de micro kleiner in omvang;
- is de aanschaffingsprijs van de micro, afhankelijk van de configuratie aanzienlijk lager;
- heeft de micro over het algemeen een geringere geheugen- en verwerkingscapaciteit.

De microcomputer bestaat veelal uit de volgende componenten:
- toetsenbord;
- beeldscherm;
- centrale verwerkingseenheid (C.V.E.);
- intern geheugen;
- eenheden voor externe geheugenopslag (diskette, schijf en/of cassette);
- printer;
- diverse poorten voor aansluitingen op andere hardware en datacommunicatielijnen.

2. De functie van de micro als hulpmiddel voor de BEIV

In het kader van de jaarrekeningcontrole beoordeelt de accountant minstens globaal de opzet van de (administratieve) organisatie en de daarin opgenomen maatregelen van interne controle.

De invloed van een microcomputer op de interne controle wordt voor de accountant bepaald door de functies die een microcomputer vervult in het gegevensverwerkingsproces, dat resulteert in een jaarrekening.

Hierbij kan het volgende onderscheid worden gemaakt:
1. Een microcomputer die geheel zelfstandig (stand-alone) bepaalde gegevens verwerkt (paragraaf 2.1).
2. Een microcomputer die als decentrale intelligente terminal is opgenomen in een netwerk (paragraaf 2.2).
   Behalve dat de micro eigen bestanden bijwerkt of raadpleegt, kunnen gegevens worden ontvangen en gestuurd van respectievelijk naar andere computersystemen.
3. Er is wel of geen combinatie van administratieve functies en werkstationfuncties zoals tekstverwerking.

Het gebruik van microcomputers leidt veelal tot kleinschalige automatisering.

Ten opzichte van een niet geautomatiseerde gegevensverwerking heeft met name kleinschalige automatisering over het algemeen de volgende gevolgen voor de interne controle:
1. De traditionele functiescheiding tussen beschikken, bewaren en registreren kan worden aangetast. In een kleinschalige omgeving kunnen moeilijk elders in de organisatie compenserende maatregelen worden ingebouwd.
2. De gegevens worden vastgelegd op machinaal leesbare gegevensdragers in een niet voor de mens leesbare vorm. De greep van de gebruikers op "hun" gegevensverzamelingen kan dan ook problemen opleveren.
3. Programmeerbare beslissingen worden opgenomen in computerprogramma's. Dat roept vragen op betreffende de kwaliteit en de werking van de programma's.
4. Meervoudige vastlegging van dezelfde gegevens wordt zo veel mogelijk vermeden (integratie).
5. De neiging bestaat om - gelet op de beperkte printcapaciteit - minder gegevens af te drukken op papier. Hierdoor bestaat het risico dat de audit-trail niet volledig is.

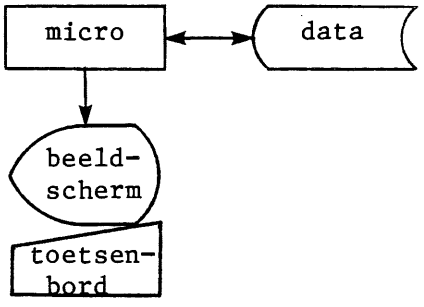
Verder heeft de inschakeling van meerdere microcomputers tot gevolg dat de gegevensverwerking wordt gespreid.
De risico's verbonden met deze spreiding zijn beschreven in paragraaf 2.3.

Voor een juist begrip van het navolgende gaan we ervan uit dat de microcomputer(s) wordt (worden) gebruikt voor de verwerking van financiële mutaties en dat de accountantscontrole systeemgericht is. Het zal blijken dat deze aanpak niet altijd toereikend is.

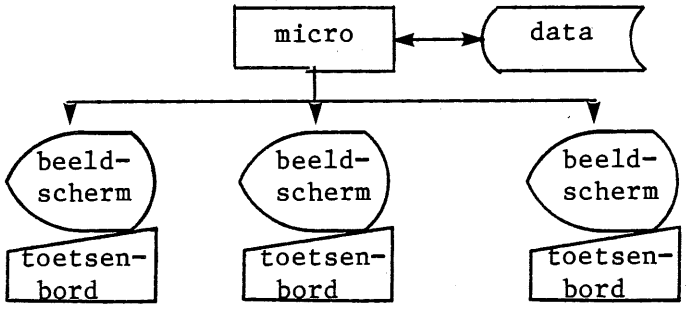
2.1 De micro als stand-alone computer

Wanneer een microcomputer niet is verbonden met een andere (centrale) computer en zelfstandig gegevens verwerkt, wordt gesproken van stand-alone verwerking.
Hierbij kan onderscheid worden gemaakt tussen:
- single-using;
- multi-using.

Bij single-using kan de micro slechts één gebruiker tegelijk bedienen, terwijl bij multi-using gelijktijdig meerdere gebruikers kunnen worden bediend.
Schematisch is dit weergegeven in de figuren 1 en 2.



Figuur 1. Micro als stand-alone computer (single-using).



Figuur 2. Micro als stand-alone computer (multi-using).

Het onderscheid tussen single-using en multi-using is van belang met het oog op een betrouwbare (juiste, volledige en geautoriseerde) gegevensverwerking.
Bij single-using kan, indien voor opslag van programma's en gegevens uitsluitend gebruik wordt gemaakt van verwijderbare gegevensdragers (bijvoorbeeld floppy disks), door middel van handmatige procedures worden geregeld dat elke gebruiker slechts toegang krijgt tot zijn/haar bestanden. Immers, buiten produktie-uren kunnen deze bestanden en de benodigde programmatuur worden bewaard in afgesloten ruimten.
Is bij single-using de toegangsbeveiliging althans formeel eenvoudig te regelen, bij multi-using wordt het moeilijker. Zodra meerdere gebruikers "gelijktijdig" worden bediend door de micro zijn de betreffende bestanden van de gebruikers "gelijktijdig" toegankelijk voor de computer. Dit brengt het risico met zich dat gebruikers ongeautoriseerd toegang krijgen tot bestanden van een ander. Overigens kan het besturingssysteem zorg dragen voor een redelijke beveiliging.

Rond microcomputers, die stand-alone worden gebruikt in een kleine organisatie, ontbreekt veelal een toereikende automatiseringsorganisatie vooral ten gevolge van het feit dat de traditionele functiescheidingen niet mogelijk zijn. Bovendien is het relatief eenvoudig om bij multi-using een toegangsbeveiligingssysteem te doorbreken.

Daarnaast kunnen operationele systemen, indien geprogrammeerd in een interpreter-taal (bijvoorbeeld BASIC), door de gebruiker "gemakkelijk" worden gewijzigd zonder dat dit achteraf kan worden vastgesteld.

Wel kan de microcomputer een sterke vooruitgang betekenen in de zelfcontrole van de functionaris. Hiermede kan hij zijn functie beter uitoefenen, hetgeen de gehele organisatie ten goede zal komen.

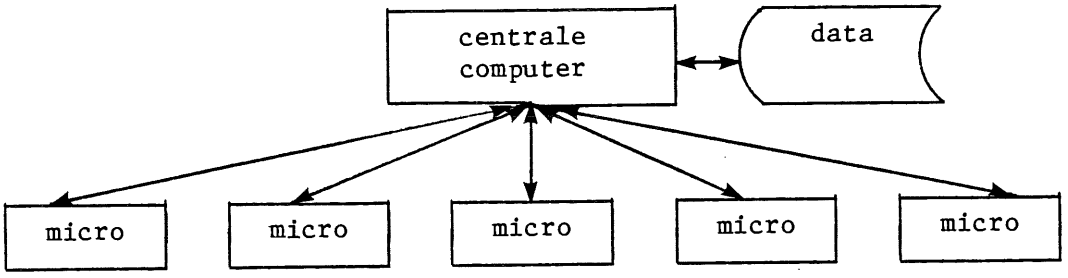
Gezien de hiervoor beschreven problematiek is het zowel voor de gebruiker als voor de accountant van belang dat voldoende overzichten worden geproduceerd die inzicht geven in de opeenvolgende fasen van het gegevensverwerkingsproces (audit-trail). De nadruk zal immers veelal liggen op de controleerbaarheid van de cijfers met mogelijkheid tot een verantwoorde analyse en cijferbeoordeling.

De accountant zal in een organisatie, waarin micro's op voornoemde wijze worden gebruikt, volstaan met een globaal oordeel over de organisatie en het functioneren daarvan, door middel van het invullen van korte evaluatievragenlijsten op basis van interviews, inzien van documentatie alsmede notities gemaakt bij de controle van de eindcijfers van een bepaalde periode waarover de controle zich uitstrekt.
Het waarnemen of de voorgeschreven organisatie altijd goed heeft gefunctioneerd zal evenwel niet mogelijk zijn. Zie het artikel van drs. J.E. Huizenga in Compact zomer 1983, nummer 32, pagina 21 e.v.

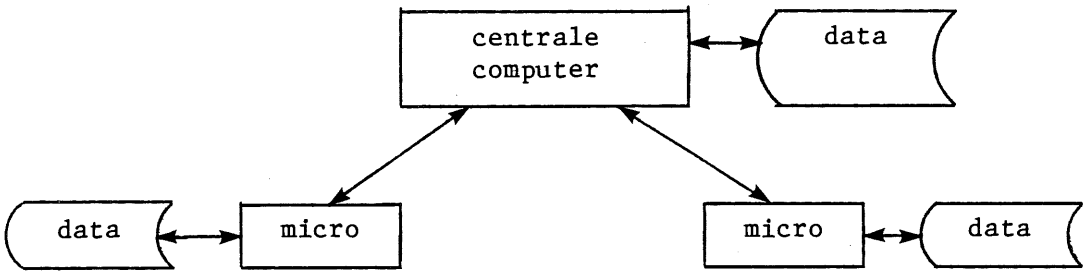
2.2 Microcomputer als onderdeel van een computernetwerk

Ruim 10 jaar bestaan reeds netwerken waarvan ook micro's deel uitmaken en waarin gegevens centraal en/of decentraal worden verwerkt en opgeslagen.
Schematisch is dit weergegeven in de figuren 3, 4 en 5.
In figuur 5 is een model van decentrale gegevensverwerking en -opslag weergegeven met alleen microcomputers.
Een praktische toepassing van dit model komt reeds voor in de vorm van een aantal microcomputers, welke door één kabel zijn verbonden en met een hoge snelheid over een beperkte afstand (veelal binnen één gebouw) gegevens kunnen uitwisselen, een zogenaamde Local Area Network. Verdere realisaties ervan zullen in de toekomst mogelijk zijn gezien de snelle technische ontwikkelingen op dit gebied. Intussen is ook aansluiting op het openbare Datanet 1 mogelijk.

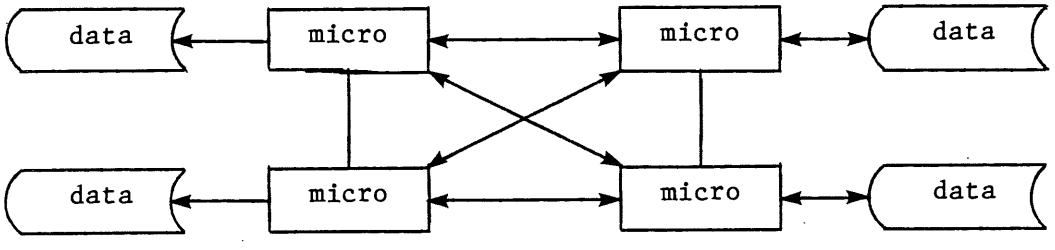
Een netwerk verbindt meerdere intelligente terminals of micro-, minidan wel mainframe-computers met een centrale computer en/of onderling. Als terminal kan een microcomputer worden gebruikt. Vanwege de aanwezigheid van programmatuur op de decentrale punten kunnen gegevens decentraal worden verwerkt en opgeslagen. De hierop betrekking hebbende bestanden kunnen door één of meerdere gebruikers (per locatie of op meerdere locaties) worden gemuteerd en gelezen. Indien verschillende bedrijfsfuncties gebruik maken van dezelfde gegevensverzameling spreekt men wel van data-sharing.
De hiermee, uit hoofde van interne controle, verband houdende problematiek bestond reeds vóór het gebruik van microcomputers als intelligente terminal en levert geen nieuwe problemen voor de accountantscontrole.



Figuur 3. Centrale gegevensverwerking en -opslag. Inquiry en invoer op decentraal niveau via microcomputers.
Er kan sprake zijn van data-sharing.



Figuur 4. Gespreide (centrale en decentrale) gegevensverwerking en -opslag.
Er kan sprake zijn van data-sharing.



Figuur 5. Decentrale gegevensverwerking en -opslag met mogelijk data-sharing via het netwerk.

Deze problematiek betreft namelijk het risico dat ongeautoriseerde toegang wordt verkregen tot de gegevens.

Ervan uitgaande dat de functiescheiding binnen de gebruikersorganisatie uit oogpunt van interne controle toereikend is zal de accountant nagaan of deze is gehandhaafd in het geautomatiseerde traject om zo vast te stellen of het voornoemde risico aanwezig is.
Hierbij zal de accountant, naast het algemeen onderzoek ter zake van passwords, gebruikersidentificaties etc. zijn aandacht richten op de volgende relaties:

1. Welke gebruikers vervullen welke functie?
2. Tot welke programma's hebben deze functies toegang?
3. Tot welke bestanden (data) hebben deze programma's toegang?
4. Welke activiteiten kunnen deze programma's met de gegevens verrichten (toevoegen, verwijderen, wijzigen of lezen)?

Intern is het noodzakelijk naar vermogen te waarborgen dat de gegevens slechts op een geautoriseerde wijze worden gebruikt.
Hiertoe dient - al naar gelang de situatie - een aangepast toegangsbeveiligingssysteem te worden ingevoerd.
Bij een centrale computer zonder terminals is dit eenvoudiger realiseerbaar dan met aangekoppelde micro's. Temeer daar aangekoppelde microcomputers geprogrammeerd zouden kunnen worden om op ontoelaatbare wijze in het systeem in te breken.
Echter ook een organisatie met beveiligde stand-alone micro's is niet geheel gevaarloos.
Weliswaar kunnen de stand-alone micro's niet de centrale computer benaderen maar wel de uit te wisselen diskettes beschrijven, kopiëren of verminken.
Hiervoor werd in de boekbespreking in Compact nummer 26 (pag. 30) reeds gewaarschuwd.
Van gebruikers moet daarom worden verwacht dat maatregelen ter bescherming van data worden getroffen en nageleefd.

Een extra complicatie vormt de omstandigheid dat de microcomputers gebouwd zijn voor functionarissen die "gebruikersvriendelijkheid van de micro" als voorwaarde stellen. Deze eigenschap zou de ongewenste bijwerking kunnen hebben van verminderde controle. Dit behoeft echter niet steeds het geval te zijn; denk aan menu gestuurde toepassingen, waardoor de gebruiker op verantwoorde wijze gebruik kan maken van de micro.

In het kader van de jaarrekeningcontrole beoordeelt de accountant de opzet van de interne controlemaatregelen. Afhankelijk van de kwaliteit ervan stelt hij zijn controleplan samen. Als onderdeel hiervan zal hij de goede werking van de interne controle toetsen.
De accountant kan daarbij worden geconfronteerd met leemten in de interne controle, zoals mogelijkheden tot ongeautoriseerde toegang tot gegevens.
Het management is de eerst verantwoordelijke; zij heeft tot taak om deze leemten (en fraudemogelijkheden) naar vermogen af te grendelen.

De accountant zal ten minste nagaan of aan minimumeisen van interne controle is voldaan en het management blijk geeft van de aandacht voor frauderisico's doordat op de meest kritische punten zo nodig tegenmaatregelen zijn aangetroffen.
Hij zal zich bij gebleken leemten - welke waarschijnlijker zijn dan bij een centrale computer met toereikende functiescheidingen in de automatiseringsorganisatie - meer moeten bezighouden met de controle van het cijfermateriaal dat wil zeggen met de door het systeem, ook door de micro's, opgeleverde overzichten. Dit op een zodanige wijze dat een fraude/omissie die het beeld van de jaarrekening zou kunnen verstoren niet onopgemerkt blijft.
Voor een meer moderne aanpak verwijzen wij u naar hoofdstuk 3.

2.3 **Specifieke risico's verbonden aan het microgebruik bij uitsluitend decentrale aanwending**

De accountant zal zijn aandacht richten op de functie die de micro vervult bij decentrale aanwending en de interne beheersbaarheid van die functie.
Dit zowel terzake van de bewaking van het gebruik van de micro's zelf als de beveiliging van het gegevenstransport via verbindingslijnen.
Het geheel is heden ten dage uiterst urgent. Een adequaat beveiligingsbeleid is voorwaarde. Wij komen hier in Compact nader op terug.
Voorbeelden van risico's die veelal zijn verbonden aan het genoemde gebruik van micro's zijn:

1. Kans op wildgroei gepaard gaande met slechte documentatie van de ontwikkelde systemen.
2. Het ontbreken van toereikende maatregelen gericht op het handhaven van de permanente juistheid en volledigheid van bestanden die voor meerdere functies worden gebruikt.
3. Geen adequate back-up procedures van bestanden en programmatuur. Zodra de gebruiker op basis van ervaring constateert dat dergelijke maatregelen toch eigenlijk niet nodig lijken te zijn, zal de neiging toenemen om hieraan minder aandacht te schenken.
4. Het afwijken van de inhoud van dezelfde bestanden die op verschillende decentrale punten worden gemuteerd en geraadpleegd. Dit risico, asynchroniteit, zal vooral toenemen wanneer het data-beheer niet goed is geregeld.

Zowel uit hoofde van de controle- als de adviesfunctie zal de accountant nagaan of intern adequate maatregelen zijn getroffen om de voornoemde leemten te beperken.

3. Controle door middel van de microcomputer

De accountantscontrole heeft als doel vast te stellen of de jaarrekening een getrouw beeld geeft van de grootte en de samenstelling van het vermogen en het resultaat.

Deze doelstelling dient zo efficiënt mogelijk te worden gerealiseerd. Vandaar dat reeds enige jaren in de accountantscontrole gebruik wordt gemaakt van controleprogrammatuur, ook wel audit-software genoemd. Deze programmatuur wordt gedraaid op de computer van de accountant of op die van de cliënt, of op die van derden.

In dit verband verwijzen wij naar de in het Handboek Accountancy opgenomen publicaties van de hand van A.H.C. Koedijk en A.W. Neisingh, waarin naast een uitputtende beschrijving van de mogelijkheden van het gebruik van de computer in de accountantscontrole aandacht wordt besteed aan de onafhankelijkheid van de accountant bij gebruik van de verschillende technieken (blz. 3660 tot en met 3664).
Bij deze controle-aanpak wordt gebruik gemaakt van audit-pakketten die een algemene toepasbaarheid hebben en van specifiek ontwikkelde programmatuur.

Bij het gebruiken van dergelijke controleprogrammatuur worden onder andere de volgende nadelen onderkend:
1. Het duurt, afhankelijk van de omvang van de toepassing, relatief lang voordat deze operationeel is.
2. Het ontwikkelen en wijzigen van dergelijke toepassingen kan niet (gemakkelijk) door de gebruiker (controlerend accountant) geschieden; de inschakeling van automatiseringsdeskundigen is noodzakelijk.
3. Het bestandsonderzoek zoals dat nu in veel gevallen plaatsvindt, kost vooral bij kleinere huishoudingen relatief veel ten opzichte van de totale controlekosten.

Naar aanleiding hiervan en de ontwikkelingen op het gebied van de microcomputer, waarvan de verplaatsbaarheid een belangrijk aspect vormt, is onderzocht in hoeverre het gebruik van een micro in de accountantscontrole (audit-micro) een oplossing kan bieden.
Gebleken is dat de audit-micro toepassingsmogelijkheden heeft, maar dat een aantal probleempunten moeten worden opgelost voordat een gebruik op grotere schaal mogelijk wordt.

3.1 Toepassingsmogelijkheden audit-micro

De audit-micro kan als volgt worden gebruikt in de accountantscontrole:
1. Het plannen, voorbereiden, registreren en begeleiden van accountantswerkzaamheden.
2. Het verrichten van bestandsonderzoeken.
3. Het gebruik van de micro als tekstverwerker, voor bijvoorbeeld de vervaardiging van dossierstukken ("elektronisch dossier") en rapporten.

4. Het langs geautomatiseerde weg in kaart brengen van de administratieve organisatie (PRISMA, Administratieve Procedure-Schema's).
5. Het opstellen en gebruiken van (financiële) modellen met behulp van spread sheet calculators (Multiplan, Visicalc).
   Voorbeelden hiervan zijn:
   - consolidatiemodel;
   - planningmodel.
6. Cijferbeoordeling.

De verwachting is dat een belangrijk toepassingsgebied van de audit-micro zal liggen op het gebied van bestandsonderzoeken. Hierop zal verder worden ingegaan in dit artikel.
De bedoelde bestandsonderzoeken hebben betrekking op bestanden die door een computersysteem van de cliënt zijn aangemaakt.
De te onderzoeken gegevens kunnen als volgt worden verkregen:
1. Overdracht van gegevens door middel van diskette-uitwisseling. Een door het andere computersysteem, eventueel een microcomputer, aangemaakte diskette wordt gelezen door de audit-micro.
2. Uitwisseling van gegevens met behulp van een directe koppeling. De microcomputer wordt ter plaatse gekoppeld aan het andere computersysteem.
3. Een koppeling, lokaal c.q. op afstand, met behulp van huislijnen, kieslijnen of openbare netwerken, met hetzelfde doel.

Door het inzetten van micro's worden de volgende voordelen nagestreefd ten opzichte van het gebruik van audit-programmatuur, die wordt gedraaid op een grotere computer (op het accountantskantoor of bij de cliënt):
1. Vermindering van de kosten van de controle.
   Bij het bestaande gebruik van audit-software is het noodzakelijk dat voor elke controle-opdracht programmatuur moet worden ontwikkeld die afgestemd is op de specifieke situatie. Hierbij kan voor een groot deel gebruik gemaakt worden van generatoren (Culprit/Cars) voor de standaardwerkzaamheden. Met behulp hiervan kan met verbindende programmatuur alsmede met de afzonderlijk geschreven specifieke programmadelen de gevraagde audit-software worden "gecomponeerd". Hiervoor is het tot dusverre nodig dat uit hoofde van doelmatigheid en vakkennis programmeurs worden ingeschakeld.
   De ontwikkeling van de audit-micro maakt het mogelijk dat meer dan voorheen algemeen toepasbare programmatuur wordt ontwikkeld, die zonder tussenkomst van programmeurs, in een dialoog, ondersteund door keuzemenu's met een vaste indeling en toelichtingen op zogenaamde help-schermen, wordt afgestemd op een specifieke situatie. Hiervoor is wel een omvangrijk audit-softwarepakket noodzakelijk. Echter de geheugencapaciteit van de jongste generatie micro's is voldoende (uitbreidbaar).

2. De controleprogrammatuur alsmede de gekozen variabelen behoeven niet bekend te worden bij de gecontroleerde, waardoor het bestandsonderzoek onafhankelijk van de gecontroleerde kan worden uitgevoerd.
3. De accountant maakt met de audit-micro bijna geen gebruik van de processorcapaciteit van de computer van de klant wanneer over diens diskettes kan worden beschikt of de gegevens door middel van data transmissie kunnen worden overgezonden.

Het blijft echter geboden dat de accountant de voorgeschreven benaderingsregels van het systeem van de cliënt in acht neemt. Alhoewel de accountant uit hoofde van zijn functie toegang zal hebben tot alle administratieve processen, dient het bedrijf zijn regels te blijven hanteren ook ten opzichte van de accountants. In het kader van de komende privacy-wetgeving zullen extra maatregelen wellicht nodig zijn als de accountant ook op het gebied van privacy-gevoelige gegevens bestandsonderzoeken moet doen. Te allen tijde zal de accountant leesbevoegdheid moeten hebben.

Ter wille van een doelmatige aanpak van het bestandsonderzoek kan het noodzakelijk zijn, na het voorbereiden van het bestandsonderzoek met behulp van de audit-micro, de verwerking op de grotere cliëntcomputer te laten geschieden. Dit hangt sterk samen met het object van controle. Een dergelijk actie kan geregeld worden door de AC-accountant die deel uitmaakt van het controleteam, uiteraard in overleg met de behandeld vennoot, die beslist of de risico's voor aantasting van de onafhankelijkheid aanvaardbaar zijn.

Voordat de audit-micro operationeel kan worden dienen een aantal problemen te worden opgelost, die gedeeltelijk technisch van aard zijn. Diskettes, die door het ene computersysteem zijn aangemaakt, zijn niet altijd (goed) leesbaar voor een ander systeem (diskette-incompatibiliteit). Dit probleem is op te lossen door het inzetten van aparte hard- en software; het zogenaamde diskette-conversiehulpmiddel. Verder worden problemen onderkend bij de computer-interface. Hieronder wordt de communicatie verstaan tussen de audit-micro en het computersysteem van de gecontroleerde door middel van de directe koppeling of de koppeling op afstand. Daarbij treden ook organisatorische problemen op.

3.2 Op te lossen problemen bij de computer-interface

De problemen bij de computer-interface hebben vooral betrekking op:
1. de communicatieverbinding;
2. de toegangsbeveiliging;
3. de verbinding met de "computerhuishouding" van de cliënt.

Ad 1. De communicatieverbinding

De wijze waarop bestanden van de computer van de gecontroleerde naar een audit-micro kunnen worden overgestuurd is afhankelijk van de data-communicatiemogelijkheden van de computer en de audit-micro alsmede van de mate waarin deze mogelijkheden op elkaar zijn afgestemd.

Een accountantskantoor heeft over het algemeen te maken met verschillende merken en typen computers bij cliënten. Dit betekent onder meer dat rekening moet worden gehouden met verschillende protocollen. De gebruiker van de audit-micro, zijnde de accountant in de algemene controle, mag echter niet worden geconfronteerd met deze specifieke automatiseringsproblematiek en moet zonder problemen zijn micro kunnen aansluiten op verschillende computers.
Om dit te realiseren dient een zodanige communicatieverbinding te worden ontwikkeld, dat de betreffende protocollen verwerkt kunnen worden.

Ad 2. De toegangsbeveiliging

Met behulp van de audit-micro kan de accountant na directe koppeling of koppeling op afstand toegang krijgen tot gegevens van de cliënt. Het zal de lezer duidelijk zijn dat door de cliënt zodanige maatregelen dienen te worden getroffen dat de accountant gegevens alleen kan lezen.

Ad 3. De verbinding met de "computerhuishouding" van de cliënt

Uit de voorgaande alinea's blijkt dat voor het verkrijgen van toegang tot files van cliënten hunnerzijds hardware- en/of software-voorzieningen vereist zullen zijn. De door cliënten in gang te zetten procedures zullen tenminste dienen te leiden tot een tijdelijk erkenning van de audit-micro als randapparaat. Afhankelijk van de constellatie bij de cliënt zal een fysieke en/of een logische herkenning van dat apparaat en de bevoegde gebruiker mogelijk dienen te worden gemaakt.

3.3 **Overige aandachtspunten bij invoering audit-micro**

Naast de grotendeels reeds opgeloste problemen bij diskette-uitwisseling (diskette-incompatibiliteit) en de problemen inzake de computer-interface indien gebruik wordt gemaakt van een directe koppeling of een koppeling op afstand, moeten voorafgaande aan de invoering van een draagbare audit-micro beslissingen worden genomen ter zake van:

- de microcomputer;
- de systeemprogrammatuur;
- de programmeertaal voor de ontwikkeling van de toepassingsprogrammatuur.

De facetten betrouwbaarheid en gebruikersvriendelijkheid spelen bij de besluitvorming een belangrijke rol.

Om een betrouwbare gegevensverwerking te waarborgen dient de werking van het programma, voorafgaande aan de invoering ervan, te worden getest.
Tevens dient voldoende documentatie te worden opgebouwd om onder andere goed onderhoud mogelijk te maken.

De audit-micro is primair bestemd voor accountants die werkzaam zijn in de algemene controle.
Hun kennis moet toereikend zijn om:
- te beoordelen of de documentatie van de cliënt een effectief gebruik van de micro mogelijk maakt;
- te bepalen dat een geautomatiseerd bestandsonderzoek doelmatig zal zijn (bepaling break even point);
- een test-run uit te voeren;
- bij moeilijkheden te onderkennen of het probleem moet worden voorgelegd aan de cliënt of aan een trouble-shooter in het eigen kantoor.

Om het gebruik van de audit-micro gebruikersvriendelijk te maken kan aan de volgende punten worden gedacht:
1. Het hanteren van een zodanige menustructuur van schermbeelden dat de gebruiker in staat wordt gesteld om achter zijn beeldscherm, op relatief eenvoudige wijze, zijn eigen toepassing te definiëren.
   Aspecten hierbij zijn:
   - vraag- en antwoordspel;
   - duidelijkheid;
   - geen verrassingen;
   - correctiemogelijkheid.
2. Het in de voornoemde structuur opnemen van een faciliteit die de gebruiker in staat kan stellen om uit mogelijke problemen te komen (helpfunctie).
3. Het vermelden van een indicatie van de foutoorzaak bij foutboodschappen.
4. Toereikende documentatie (gebruikershandleiding).
5. Goede responsetijden.
6. Ergonomie (bijvoorbeeld indeling beeldscherm).
7. Het gebruik van vragenlijsten om bij elke cliënt te komen tot toereikende beveiligingsmaatregelen indien de audit-micro wordt ingeschakeld.

'I've got my briefcase terminal, briefcase microfiche reader, briefcase dictating machine and briefcase photo-copier, but I've forgotten my briefcase!'

4. Samenvatting

Om de invloed van de micro op de controleplan van de accountant (aard en omvang van controlewerkzaamheden) vast te stellen zal de accountant op de eerste plaats dienen te kijken naar de functie die een microcomputer vervult in de te controleren huishouding en vervolgens moeten vaststellen of het samenstel van interne controlemaatregelen rond deze functie toereikend is.

Hierbij zal hij worden geconfronteerd met de gevolgen van decentralisatie van de automatisering voor de betrouwbaarheid van de gegevensverwerking en voor de beveiliging tegen verlies, diefstal of vermin-king van gegevens.

Het gebruik van microcomputers, zowel in een computernetwerk als stand-alone, gaat veelal gepaard met een automatiseringsorganisatie rond deze computers, die op het punt van interne controle niet toereikend is voornamelijk wegens het ontbreken van goede functiescheidingen.

Het gebruik van deze computers brengt voorts het risico met zich mee dat:
- toegangsbeveiligingssystemen op relatief eenvoudige wijze worden doorbroken;
- operationele systemen door de gebruiker makkelijk worden gewijzigd, zonder dat dit sporen nalaat.

Geprogrammeerde controles hebben voor de accountant dan ook maar een beperkte betekenis; hij kan immers onvoldoende zekerheid krijgen of deze controles gedurende de gehele controleperiode goed hebben gewerkt.
Daar de betrouwbaarheid van een informatiesysteem wordt bepaald door een combinatie van geprogrammeerde controles en gebruikerscontroles zal de accountant nagaan of deze laatste voldoende compensatie opleveren voor de genoemde onzekerheid.
Indien dit niet het geval is zal hij meer de nadruk leggen op een gegevensgerichte controlebenadering.
Overigens kunnen hierbij ook andere overwegingen een rol spelen, zoals bijvoorbeeld kostenoverwegingen.
Tevens zal de mogelijkheid tot gebruik van controleprogrammatuur hierbij een rol spelen.

De microcomputer biedt ruime mogelijkheden als hulpmiddel bij de accountantscontrole (audit-micro).
Hierbij kan de audit-micro stand-alone worden gebruikt alsmede gekoppeld aan de computer van de gecontroleerde.
Bij deze laatste gebruiksmogelijkheid dient rekening te worden gehouden met problemen op het gebied van de computer-interface.
Het gebruik van de audit-micro stelt voorts eisen op het gebied van betrouwbaarheid en gebruikersvriendelijkheid.

Geraadpleegde literatuur

1. Audit-micro.
   De datacommunicatieverbinding en de keuze van een programmeertaal.
   Stageverslag H. Spape.
2. De audit-micro
   "Een gebruikersvriendelijke user-interface".
   Stageverslag P. Salemans.
3. Edpacs, november 1981.
4. Edpacs, oktober 1983.
5. Microcomputers en financiële modelling.
   G. Horlings, R.A.
   Accountant, april 1983.
6. Microcomputers: mogelijkheden en beperkingen.
   Prof. W. Hartman, R.A.
   Accountant, december 1982.
7. The impact of the microcomputer.
   By Robert A. Fogler, MBA, CPA, FLMI, CLU.
   The internal auditor/April 1983.
8. Audit considerations in distributed processing systems.
   James V. Hansen, Brigham Young University.
   Communications of the ACM, August 1983.
9. Artikelenserie van R.H. Healey, Thorne Riddell.
   De microcomputer in de accountantscontrole.
   - A science fiction trip into auditing.
     Compact 30, winter 1982/1983.
   - Current developments for future thinking.
     Compact 31, lente 1983.
   - Down to earth again, KMG potential.
     Compact 32, zomer 1983.
10. How cheap computers are affecting external audit.
    William List, CA, MBCS.
    The Accountant's Magazine, February 1983.
11. Geautomatiseerde audit technieken door J. Achterberg RA en drs. G.L. Sijtsma maandblad Informatie september 1983. Samengevat in Compact herfst 1983, nummer 33 bladzijde 62 tot en met 66.
12. Het gebruik van de computer in de accountantscontrole:
    deel I Het onderzoek van gegevensverzamelingen (3651 ev), december 1979.
    deel II Technieken ten behoeve van beoordeling van organisatorische maatregelen (3669 ev), november 1981.
    Handboek Accountancy door A.H.C. Koedijk en A.W. Neisingh.
13. Onderzoek naar de werking interne controle mogelijk?
    Compact 32, zomer 1983 drs. J.E. Huizenga

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

OPLEIDING RISK-MANAGER

Dit artikel is geschreven door de heren F.H. Horbeek en H.A. Huyskens van de Rabo-bank.
De heer Horbeek (hoofd beveiliging van de Rabo-bank) is lid van de werkgroep die een leerprogramma heeft opgesteld voor de opleiding tot Risk-manager.

Inleiding

Risk-management of risicobeheer. Het zijn termen, die de laatste jaren steeds vaker worden gebruikt door een steeds groter wordende groep mensen in een groeiend aantal situaties.
Het is de vraag of een ieder zich bewust is welke lading nu precies door de Risk-managementvlag wordt gedekt, doch één ding is duidelijk:

er is een einde in zicht van een periode, waarin vanuit een verzuilde optiek de risico's, die een organisatie bedreigen, te lijf worden gegaan.
Niet langer wordt genoegen genomen met een monopolistische benadering van risico's, waarbij de verzekeringsadviseur, de veiligheidskundige, de beveiligingsman en ... de ondernemer, allen vanuit hun eigen denkraam, tegen specifieke situaties aankijken.

Wat is dan Risk-management?
Uit de vele definities hebben wij de volgende gekozen:

> "Het geheel van systemen en subsystemen, dat tot doel heeft de risico's, die een organisatie bedreigen, op economische wijze zo volledig en systematisch mogelijk te beheersen."

Met name de term "het geheel" geeft aan, waar het in dit kader om gaat.
Risk-management wil een samenhangend systeem zijn, waarvan de diverse disciplines deel uitmaken, met aandacht voor hun onderlinge relaties en afhankelijkheden.
Het moge duidelijk zijn, dat er binnen een organisatie nauwelijks beslissingen kunnen worden genomen, die niet van invloed zijn op meerdere gebieden van Risk-management.
Investering in een gebouw is op zich al een ondernemersrisico, maar heeft ook zijn weerslag op brandpreventie en repressie, beveiliging, verzekering en veiligheid.
Indien de diverse aspecten uit bovenstaand voorbeeld los van elkaar worden benaderd, dan is de kans, dat aandachtsgebieden overlappend worden behandeld, levensgroot aanwezig. Het moge bovendien duidelijk zijn, dat deze benadering overbodige financiële consequenties met zich mee kan brengen.

Noot

Een ander gevolg zou kunnen zijn, dat er hiaten ontstaan in het geheel van de beheersingsmaatregelen, waardoor risico's niet of niet op de juiste wijze worden beheerst. De financiële en/of menselijke gevolgen laten zich slechts raden.

Oog hebben voor dit gegeven wil zeggen: kiezen voor Risk-management als bedoeld in vorenstaande definitie.
Risk-management is echter meer dan alleen maar een systeem: het is ook een manier van denken. Immers, de verantwoordelijkheid voor het voortbestaan en goed functioneren van een organisatie en dus ook het beheersen van risico's in een organisatie berust bij alle medewerkers.

Vandaar, dat Risk-management als manier van denken een geïntegreerd deel dient uit te maken van de totale bedrijfscultuur in een onderneming.

Wellicht ten overvloede zij vermeld, dat Risk-management geen doel op zich is, maar dienstbaar dient te zijn aan de doelstelling van de organisatie. Anders gezegd: Risk-management is een aspect van ondernemen.

Het ontwikkelen en uitbouwen van een dergelijk systeem en de "opvoeding" van alle medewerkers in een organisatie in die richting vereist de nodige kennis en vaardigheden.

Ofschoon zowel in het bedrijfsleven als bij de overheid diverse functionarissen werkzaam zijn op het gebied van - delen van het - Risk-management, ontbreekt het aan een opleiding, die alle facetten van Risk-management omvat.

In de huidige situatie bestaat derhalve duidelijk het gevaar voor een eenzijdige benadering van de diverse aandachtsvelden binnen de Risk-management problematiek.

Dit gevaar zal in de komende decennia alleen maar toenemen.
Enige oorzaken hiervan zijn:
- groeiende complexiteit van het bedrijfsgebeuren;
- uitbreiding van geautomatiseerde procesbesturing en gegevensverwerking; en
- ontwikkelingen op communicatiegebied (bijvoorbeeld satelliet).

Er bestaat derhalve behoefte aan een opleiding tot Risk-manager, die alle aspecten van Risk-management omvat.

Vanuit deze behoefte is door vertegenwoordigers van de Sectie Beveiliging van het N.G.I. (Nederlands Genootschap voor Informatica) en het V.B.B. (Nederlandse vereniging voor Bedrijfsbeveiliging) een werkgroep opgericht, die zich als taak heeft gesteld een opleiding tot Risk-manager gestalte te geven.

De werkgroep heeft inmiddels een concept-leerprogramma het licht doen zien.

Uitgangspunten

Zonder volledigheid in haar eerste rapportage te willen claimen, is de werkgroep uitgegaan van de volgende basisvragen:
1. Wat is de doelstelling van de opleiding?
2. Voor wie is de opleiding bestemd?
3. Hoe moet de opleiding worden opgebouwd (inhoudelijk en organisatorisch)?
4. Hoe past een voorstel binnen het totale veld van onderwijs in Nederland?

Ad 1. Doelstelling

In wezen vloeit de doelstelling (hier niet in zuiver onderwijskundige zin gebruikt) voort uit de benaming van de opleiding.

Op de eerste plaats beoogt zij op te leiden tot risk manager, een functionaris op managementniveau, belast met beleidsadvisering op het gebied van Risicobeheersing.

Op de tweede plaats beoogt zij op te leiden tot manager, teneinde buiten het specifieke terrein van Risk-management te kunnen fungeren op leidinggevend niveau. Dit betekent dat de opleiding zich op een aantal onderdelen niet alleen in de diepte, doch ook in de breedte zal dienen te begeven.

De operationalisering van deze doelstellingen in termen van kennis, vaardigheden en attitudes (ook wel: meetbaar eindgedrag), zal een volgende - niet geringe - stap moeten zijn. Als uitgangspunt hiervoor zou de proeve van leerstof kunnen dienen, die de werkgroep in haar rapport heeft neergelegd (zie blz. 20 van het rapport).

Ad 2. Doelgroepen

De groepen op wie de opleidingsactiviteiten gericht worden, zijn de volgende:
- de groep die op managementniveau betrokken is (zal worden) bij beleidsaangelegenheden op het gebied van Risk-management;
- de groep die naast beleidsmatige betrokkenheid op middelbaar en hoger niveau belast is (zal worden) met uitvoering van specifieke taken op het gebied van Risk-management.

De opleiding zal derhalve dusdanig flexibel moeten zijn, dat zij gevolgd kan worden door:
- "leken" op het gebied van Risk-management, die al op management niveau werkzaam zijn;
- functionarissen werkzaam op (delen van) het gebied van Risk-management;
- anderen (waaronder schoolverlaters) (zie ook ad 3).

Ad 3. De opleiding

Bij de opzet van een opleiding gaat de werkgroep uit van een modulaire opbouw, waarbij iedere module een afgebakend onderdeel van de opleiding omvat.
De keuze voor deze opzet is ingegeven door een aantal gedachten:
- Het moet mogelijk zijn (gedeelten van) bepaalde modules te volgen zonder dat het behalen van een einddiploma nagestreefd wordt (specialisatie in de werkkring).
- Afhankelijk van opleiding en/of ervaring kan voor modules vrijstelling worden gegeven.
- De opbouw geeft de mogelijkheid om per module aansluiting te zoeken bij bestaande opleidingsinstituten.
- Omdat het met goed gevolg afsluiten van een aantal modules recht geeft op het diploma Risk-manager, kan reeds tijdens de opleiding worden gespecialiseerd.

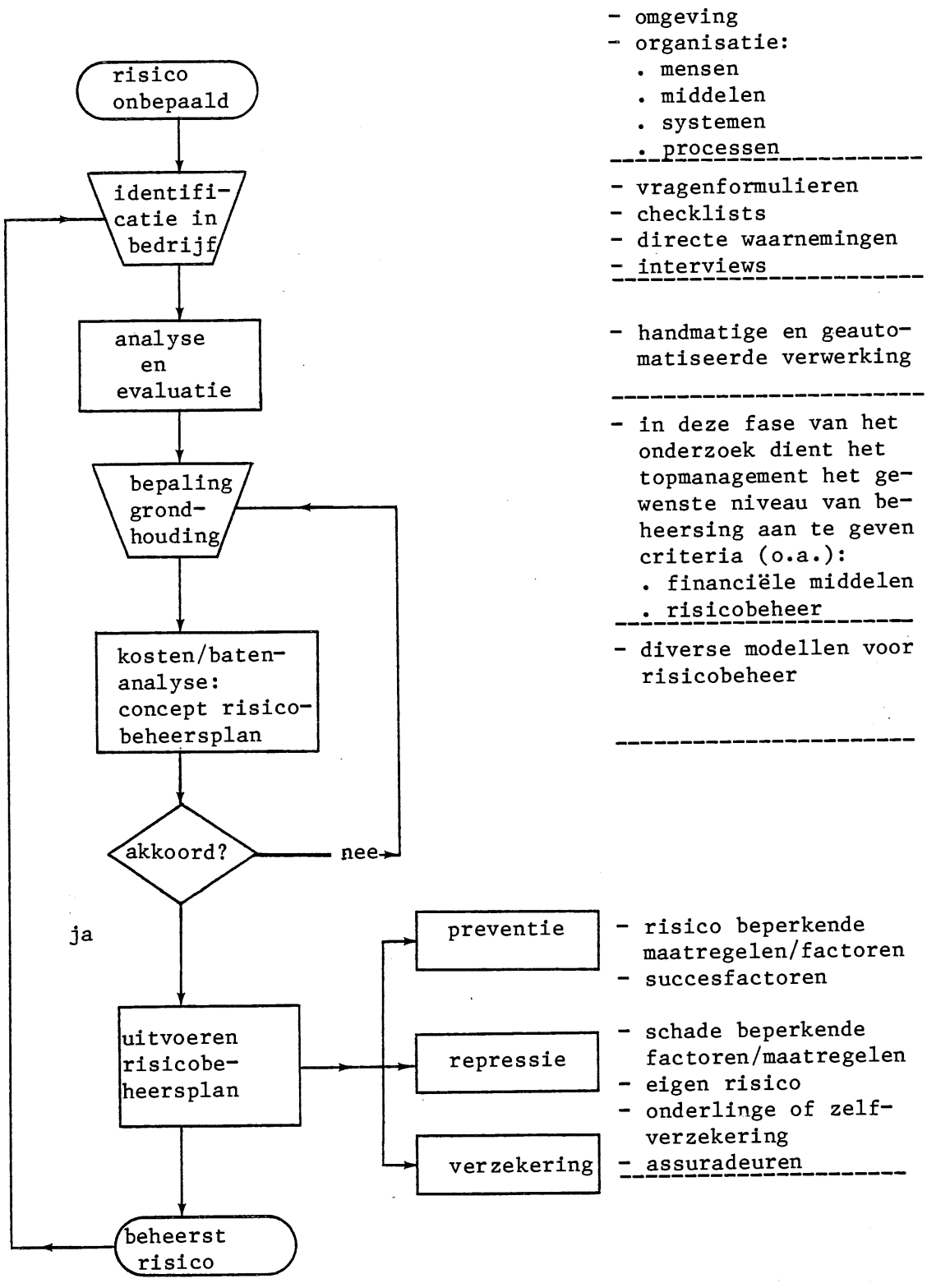
In haar rapportage gaat de werkgroep in principe uit van de volgende modules:

1. Risk-management techniek. Dit onderwerp maakt een geïntegreerd onderdeel van de overige modules uit. Deze module is de belangrijkste binnen de opleiding, omdat het hierbij gaat om de filosofie en (zie figuur 1) techniek van Risk-management als kern, waaromheen de overige modules zijn gegroepeerd.

2. Bedrijfskunde. Dit onderdeel kan beschouwd worden als een algemeen vormende module voor de manager en als vak met diverse aspecten die van belang zijn voor Risk-management.

3. Administratieve organisatie. Hierbij hebben met name de aspecten van interne controle een nauwe band met Risk-management.

4. Recht. De Risk-manager zal binnen zijn vakgebied veelvuldig contact onderhouden met juridisch geschoolde functionarissen. Bovendien hebben een aantal wettelijke voorschriften consequenties voor de taakuitoefening van de Risk-manager (privacy wetgeving, Wet op de Weerkorpsen, Wet Arbeidsomstandigheden).



Figuur 1. Risk-managementorganisatie als proces.

5. Informatica. De ontwikkelingen op dit gebied, alsmede het feit dat de afhankelijkheid van geautomatiseerde systemen steeds toeneemt, maken de keuze voor deze module evident. Bovendien is de informatica een onmisbaar hulpmiddel bij de Risk-managementtechniek.

6. Techniek. Een Risk-manager dient in staat te zijn om risico's, die technisch van aard zijn, te onderkennen en door te spelen naar deskundigen. In deze module wordt onder meer gedacht aan bouwkunde, elektronika, fysika en analyse van technische bedrijfsprocessen.

Vooralsnog wordt gedacht aan een 4-jarige opleiding. De opleiding voor een Risk-manager met als specialisatie Informatica zou er in schemavorm als volgt uit kunnen zien (de gebruikte termen zijn illustratief).

jaar		Risk man.	Bedrijfs-kunde	Adm. org.	Recht	Infor-matica	Techniek
4	doctoraal	X	X			X	
3		X	X			X	X
2	kandidaats	X	X	X	X	X	X
1	propadeuse	X	X	X	X	X	X

Ad 4. Inpassing in het onderwijssysteem

Het plan van de werkgroep is ambitieus, nochtans moeten nog wel vragen worden beantwoord en talloze problemen opgelost.
Een daarvan is wel de inpassing van de opleiding in het onderwijssysteem in Nederland. De werkgroep pleit ervoor zo veel mogelijk aansluiting te zoeken bij bestaande opleidingen. Hierbij kan gedacht worden aan H.E.A.O., H.I.O., H.T.S., universiteiten en hogescholen.

Om het plan verder naar volwassenheid te voeren zal nog moeten worden nagedacht over:
- begingedrag (opleiding en ervaring);
- evaluatiemomenten/-techniek;
- niveau van eindgedrag;
- dagopleiding of part-time opleiding;
- rechtspositie van de student;
- kosten;
- waardering van de opleiding;
- formuleren van leerdoelen (zie ook ad 1);
- ontwikkelingsplanning.

Voorwaar nog een hele kluif, die echter naar onze mening alle steun waard is, omdat de opleiding streeft naar een ontwikkeling van Risk-management in de breedte, een ontwikkeling, die wij al eerder in de inleiding van dit stuk hebben beschreven.

Voor nadere informatie over het leerprogramma kunt u zich wenden tot de secretaris van de redactie van Compact:
H.J.M.v.d. Wielen (telefoon 020 546 1394).

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

REACTIE VAN LEZERS

Onderwerp Password-protectie in Compact herfst 1983 pagina's 19 en volgende, nummer 33 10e jaargang

Geachte schrijver,
Uw artikel heb ik met aandacht gelezen. Het is een indrukwekkende lijst van elkaar aanvullende beveiligingsmaatregelen. Bovendien bijeengebracht in een kort bestek.

Met deze kennis gewapend neem ik het standaard controleprogramma van cliënt X ter hand.
Mijn opdracht luidt:
- beoordeel de interne controlemaatregelen;
- toets deze op hun bestaan en werking;
- pas een cijferbeoordeling toe met aanvullende steekproef naar de massa, opdat een fraude, veroorzaakt door een omissie, die het beeld van de jaarrekening beïnvloedt door mij kan worden getraceerd.

Vraag: Welke opeenvolgende stappen moeten we aanhouden om een goed gebruik van passwords te constateren, ook in het computercentrum.
Neem aan dat alle overige interne en externe controlemaatregelen adequaat zijn genomen en ook adequaat werken.
H.J.M. van der Wielen

Antwoord van de schrijver
Mijn artikel uit de vorige editie van Compact zou meer volledig en toepasbaar zijn met het antwoord op de door u gestelde vraag.
Vandaar dat ik deze kans gaarne benut voor het completeren van voornoemd artikel.

In het algemeen kan worden gesteld dat de controle op de naleving van maatregelen ten aanzien van password-protectie ten nauwste bepaald wordt door de mogelijkheden, die worden geboden door de password-protectie-software. Veelal zullen wij daardoor voor beperkingen worden gesteld.
Een en ander betekent dat de accountant (EDP-auditor) op de eerste plaats bekend dient te zijn met de mogelijkheden en onmogelijkheden van deze software. Hij zal, zonder de software op dit punt ter discussie te stellen, niet meer kunnen verlangen dan datgene, dat door deze software kan worden geboden.
Het kan overigens voorkomen dat installatie-opties invloed uitoefenen op de toepassing van password-protectie, waardoor deze opties object van controle dienen te zijn. In mijn vorige artikel werd hiervan geabstraheerd, zodat ik hier nu niet verder op zal ingaan.
Aan de hand van de punten, genoemd in de hoofdstukken 4 tot en met 7 van het artikel, zal ik mogelijkheden aandragen voor genoemde controle.

Hoofdstuk 4. Effectiviteit passwords

Indien de accountant kan beschikken over een betrouwbare lijst van bij de cliënt in gebruik zijnde passwords met vermelding van de desbetreffende gebruikers en vervolgens een periode later de beschikking kan krijgen over een nieuwe lijst, kan hij de volgende controles verrichten:

- stel vast dat de passwords per gebruiker gewijzigd zijn;
- beoordeel de passwords op willekeurigheid (geen verklaarbare passwords, die andere gebruikers zouden kunnen kennen).

Het verkrijgen van de genoemde lijst is (hoe prettig ook voor onze controle) op zichzelf een vervelende situatie, omdat wellicht ook anderen deze lijst zouden kunnen verkrijgen. Dit zou betekenen, dat wij moeten vaststellen, of anderen deze lijst niet kunnen vervaardigen.
Over de betrouwbaarheid van de verkregen lijst alsmede de effectiviteit van de password-protectie kan onder meer door testen een indruk worden opgedaan.
Indien wij niet over deze lijst kunnen beschikken, blijven er geen andere controlemaatregelen over om voornoemde controle uit te voeren, anders dan datgene dat bij toeval kan worden vastgesteld.
Het kan voorkomen dat de cliënt zo'n lijst niet aan de accountant ter beschikking wil stellen; om begrijpelijke redenen overigens. In deze situatie valt slechts te constateren, dat bij de cliënt voorzichtigheid wordt betracht, hetgeen wij (in beperkte mate) zullen moeten toejuichen.

Op de diverse werklocaties bij de cliënt zou de accountant een indruk kunnen opdoen over het geheim houden van passwords (geen stickers met passwords op de terminals, etc.).

Hoofdstuk 5. Gebruik passwords

In het algemeen gelden de paraplumaatregelen, die onder meer betrekking dienen te hebben op bestands- en programmatuurbeveiliging. De beoordeling van deze maatregelen is ook in dit verband van belang voor het geheim houden van passwords. De bestanden, waarop de passwords zijn opgeslagen alsmede de desbetreffende software dient beveiligd te zijn tegen ongeautoriseerde toegang.

Indien een overschreden aantal pogingen tot het intoetsen van passwords wordt gelogd en vervolgens geprint, dient hiermee door de organisatie wel iets (liefst zo snel mogelijk) te worden gedaan. Dit betekent dat de accountant geïnteresseerd dient te zijn in de naleving van de procedure, die erop gericht is actie te ondernemen indien overtredingen zich voordoen.

Hoofdstuk 6. Aanvullende maatregelen

In een bezoek bij de cliënt kan de accountant vaststellen of terminals, die onbewaakt worden achtergelaten ook inderdaad zijn uitgezet (dit niet alleen uit energiebesparing).
Bij sommige software is een fysieke beveiliging van de terminal zelfs van belang. Dit betekent dat de accountant hieraan aandacht dient te schenken bij een bezoek aan de cliënt.

Hoofdstuk 7. Uitgifte passwords en beheer beveiligingsprogrammatuur

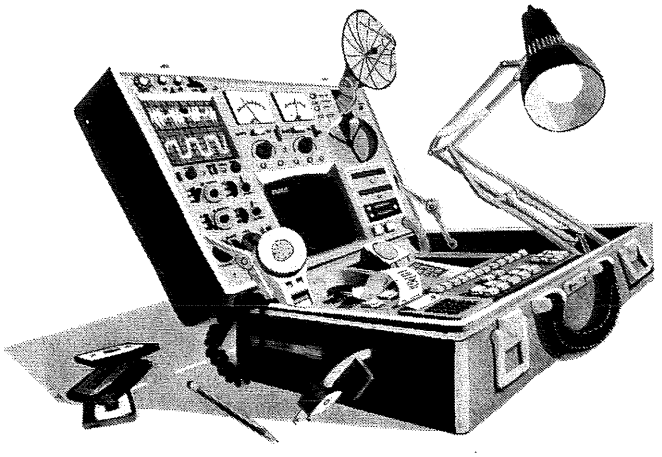
De procedure voor het verkrijgen van een gebruikersidentificatie en initieel password dient te worden beoordeeld.
De naleving dient periodiek gecontroleerd te worden. Veelal vindt in deze procedure een vastlegging/formulierenstroom plaats.
Dit zelfde geldt voor de procedure voor het herkrijgen van een vergeten password.
Voorts kan de eerdergenoemde lijst van gebruikers met passwords worden gebruikt in combinatie met overplaatsingsgegevens en informatie betreffende personeelsleden, die de organisatie hebben verlaten. Deze laatste groep dient niet meer op de meest recente lijst voor te komen. Bij de eerste groep van personeelsleden kan worden beoordeeld of voor hen nog wel toegang tot de computer noodzakelijk is. Zo niet, dan dienen ook zij evenals de ex-personeelsleden niet meer op die lijst voor te komen.

Zoals reeds genoemd in de controlemaatregelen onder hoofdstuk 5, dient de software, die password-protectie biedt, tegen ongeautoriseerde toegang te worden beschermd.

Uit het voornoemde dient duidelijk te zijn, dat:
- een en ander bijzonder afhankelijk is van de password-protectie-software;
- de accountant in dit verband een specialist dient te zijn op het gebied van voornoemde software en password-protectie.

Nochtans is het goed, dat de controlerend accountant weet of tenminste begrijpt waarom en wanneer een EDP-auditor bepaalde punten wel of niet onderzoekt, danwel dient te onderzoeken.
A. van der Drift.

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



winter 1983/lente 1984

DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE

door H. Veenman

Nieuws van het audit micro front

Het KKC Audit Pakket
De afgelopen maanden is door het AC Micro Team hard gewerkt aan de realisatie van het KKC Audit Pakket. Met behulp van dit pakket, dat reeds een zestal maanden in eenvoudige vorm op de ALTOS-computer beschikbaar is in Deventer en in Amsterdam, wordt het de algemene accountant mogelijk gemaakt, zelf gegevens van zijn cliënten aan een bestandsonderzoek te onderwerpen. Verwacht wordt dat dit pakket in het voorjaar van 1984 op de IBM PC en op de microcomputers, die daarmee uitwisselbaar zijn, beschikbaar komt.
In die zelfde periode zal programmatuur beschikbaar komen, waarmee het mogelijk is om verschillende soorten diskettes te kunnen verwerken (zie ook deze rubriek in Compact, herfst 1983).

Microcomputers in de praktijk
Het afgelopen halfjaar is het aantal microcomputers op onze kantoren sterk gestegen. Dat dit in het begin behalve een groot aantal voordelen ook wat problemen gaf, mag blijken uit het volgende.
In de maanden december 1983 en januari en februari 1984 werden een aantal microcomputers aangeschaft; deels ten behoeve van controlewerkzaamheden van een aantal werkeenheden, deels voor gebruik door de AC voor het ontwikkelen van programma's op deze micro's en niet op de laatste plaats als hulpmiddel bij het uitvoeren van administratieve zaken.
Toen de eerste paar machines door de leverancier waren bezorgd en door ons aan de betreffende instantie waren afgeleverd, bleek al spoedig, dat niet alleen auto's maar ook microcomputers kinderziektes kunnen vertonen. De ene na de andere machine kwam terug met een zelfde klacht: een van de diskettestations reageerde soms niet, wanneer gegevens op de diskette gelezen of geschreven moesten worden.

Gevolg was: leverancier gebeld, deze komt de defecte apparaten ophalen, probeert van alles, brengt ze weer terug, wij geven ze weer uit aan de gebruikers, en deze brengt ze per omgaande retour daar de fout nog steeds zo nu en dan optreedt. Ondertussen worden nog steeds nieuwe micro's besteld en afgeleverd, die na een aantal dagen het zelfde euvel vertonen.
Na een aantal weken van groeiende ontevredenheid bij de gebruiker, het AC Micro Team en de leverancier werd de knoop doorgehakt en door de leverancier rechtstreeks contact gezocht met de fabrikant. De week daarop heeft een aantal hoog aangeschreven technici van de fabrikant enkele dagen en nachten gewerkt aan een aantal van onze defecte machines, waarna de volgende conclusie kon worden getrokken: de oorzaak van het defect lag in het gebruik van een verkeerd smeermiddel, waarmee de diskettestations geruisloos zouden moeten werken en tevens in het "vergeten" van een aardeverbinding in de omgeving van het diskettestation.
Deze omissie werd na dit onderzoek dermate regelmatig aangetroffen, dat momenteel gedacht wordt aan een opzettelijke actie van diegenen, die bij de produktie van de diskettestations betrokken zijn.
Gelukkig kan ik melden dat ook aan dit verhaal een happy-end verbonden is; de fout is gelokaliseerd en wordt, indien deze nogmaals bij een machine wordt aangetroffen, door de leverancier verholpen voordat het apparaat wordt afgeleverd.
Door het AC Micro Team wordt iedere micro een aantal dagen getest, voordat ze wordt doorgegeven aan de betreffende gebruiker, zodat de kans op initiële storingen bij gebruikers is verkleind.
Kortom, we hebben er allemaal wat van geleerd, en een ding weten we zeker: EEN COMPUTER IS OOK MAAR EEN ...

Marktontwikkelingen

***Voor diegenen, die de aanschaf van een IBM PC voor (semi)privé-doeleinden financieel iets te ver gaat, heeft IBM de PC Junior geannonceerd. Deze PC Junior, een kleine uitgave van de IBM PC, kost ongeveer de helft en is duidelijk meer gericht op de home computermarkt. Ze kan worden aangesloten op een televisietoestel en voorzien worden van joysticks, waardoor ze ook voor de minder serieuze gebruiker geschikt is gemaakt. Maar een niet minder belangrijk aspect is dat de gegevens, welke op de Junior zijn ingetikt zonder meer kunnen worden gelezen door de "grote" IBM PC, en omgekeerd, zodat een scala van serieuze toepassingen kan worden bedacht.

***Na de geboorte van de IBM PC is de markt het afgelopen jaar overspoeld met computers van andere leveranciers, die allemaal min of meer uitwisselbaar met de IBM PC waren, en bovendien een aantal voordelen hadden boven de IBM PC, zodat het voor de gebruiker aantrekkelijk werd om een dergelijke "look alike" aan te schaffen in plaats van de IBM zelf. De twee belangrijkste voordelen waren wel de prijs en de draagbaarheid van het apparaat.

Ten aanzien van het eerste aspect heeft IBM onlangs een stevige klap uitgedeeld aan haar concurrenten, door de prijzen van de IBM PC-artikelen (fors) te verlagen; maar ook voor wat betreft de draagbaarheid ziet het er naar uit dat IBM terrein probeert te winnen, door kort geleden de IBM Portable Computer te annonceren: de draagbare uitvoering van de IBM PC. Er is nog weinig over bekend, maar we zullen trachten u via Compact op de hoogte te houden.

Tot slot volgt hieronder een artikel uit De Automatisering Gids van 29 februari 1984, dat handelt over de ontwikkeling van de gegevensdragers in de laatste decennia en de mogelijkheden ervan in het heden en de nabije toekomst. De redactie van de AG heeft welwillend toegestaan het artikel over te nemen. Het copyright blijft bij deze uitgever berusten.

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

Jointventures Philips en CDC klaar met prototype optisch geheugen

Grens bij magnetische opslagtechnieken voorlopig niet in zicht

De informatiedichtheid van magnetische informatie-opslagmedia neemt voortdurend toe. Daarnaast wordt gezocht naar alternatieve methoden om informatie voor langere of kortere tijd op te slaan. Een van die methoden is de optische en dit jaar zijn een aantal nieuwe produkten op dit terrein te verwachten.

De onder computergebruikers nog steeds meest wijd verbreide methode om informatie te bewaren is al zo'n dertig jaar de magnetische. Weliswaar is de magnetische methode om informatie vast te leggen op deelgebieden verdrongen, als werkgeheugen wordt bijvoorbeeld al lang geen gebruik meer gemaakt van het ringkerngeheugen, in zijn algemeenheid is de band, de schijf en de floppy disc, ieder in een bepaald deelgebied, *het* medium.
Nu heeft de ontwikkeling van magnetische media sedert de introductie van IBM's magneetbandeenheid 726 in 1952 niet bepaald stil gestaan. Schreef en las de 726 indertijd niet meer dan 32 tekens per mm, de meeste magneetbandgeheugens bevatten nu zo'n 246 tekens per millimeter. Men spreekt bij dergelijke systemen overigens liever van bits per inch. De ontwikkeling in bits per inch ging van 225 naar 6250.
De belangrijkste oorzaak van de informatieverdichting bij magnetische media is het in de loop der jaren allengs verbeteren van de registratielaag. Werd aanvankelijk gewerkt

Magneetband wordt op brede rollen geproduceerd, waarna tot op de honderdste millimeter nauwkeurig de band op de juiste breedte wordt afgesneden.

met eenvoudig ijzeroxide dat met behulp van lak op een drager was aangebracht, tegenwoordig vinden nieuwe materialen als chroomdioxide veel toepassing en hebben veel leveranciers eigen recepten om tot een betere registratielaag te komen. Het maximaal aantal fluxveranderingen per inch (dat is de maat voor natuurkundigen om het mogelijke aantal bits per inch aan te geven) is in theorie 40.000 bij chroomdioxide. Dat is een viervoud van de huidige mogelijkheden.

Magneetband

Was de eerste drager van magnetische informatie de magneetband, dit medium had een nadeel. Omdat de band zich op een spoel bevindt dient men, ten einde bepaalde informatie op de band te kunnen vinden, steeds de band heen en weer te spoelen tot de juiste plek voor de leesschrijfkoppen is terecht gekomen. Met dat spoelen gaat veel tijd verloren en de magneetband vindt dan ook hoofdzakelijk nog toepassing als medium wanneer de te bewaren informatie niet al te vaak nodig is en wanneer de gehele band in één keer kan worden ingelezen. Veelal wordt op magneetband een historisch overzicht van de werkzaamheden van de computer bijgehouden.

Voor het opslaan van grote gegevensbestanden waarvan informatie veelvuldig gebruikt dient te worden vond het schijvengeheugen ingang. Bij de magnetische schijf werd vroeger een ijzeren en tegenwoordig een aluminium ronde plaat voorzien van een registratielaag van hetzelfde materiaal als op de band gebruikt werd. De informatie op een schijf is veel sneller toegankelijk dan op magneetband.

Schijvengeheugen

Het principe berust erop dat het magnetisch gevoelige gedeelte van de schijf een groot aantal 'sporen' kent. Deze sporen zijn als steeds groter wordende cirkels vanaf de as op de schijf aanwezig. Er zijn twee typen van apparaten om de schijf van informatie te voorzien. Per spoor kan er een lees/schrijfkop worden gemonteerd op de juiste plaats boven de schijf (de dure oplossing; meestal aangeduid als 'fixed head') of er kan een enkele beweegbare kop boven de schijf worden gemonteerd. Aan de hand van het adress kan dan het juiste spoor worden gelezen of beschreven. Het adress bevat vaak ook nog een aanwijzing over de juiste plaats op het spoor waarop bepaalde gegevens (data) dienen te komen of kunnen worden gevonden.

Nu is voor het overbrengen van magnetische informatie beweging nodig. Het zeer kleine magneetveldje dat een bit informatie bevat wekt door de beweging een elektrisch stroompje op in de leeskop. De schijf staat daarom niet stil maar draait met een tempo van meestal 1500 omwentelingen per minuut rond. Omdat de snelheid aan de buitenkant van de schijf uiteraard groter is dan vlak bij de as en de schijveneenheid geen mogelijkheden kent om de tijdsduur van iedere bit informatie afhankelijk van het spoor te doen veranderen zal de informatie op de schijf in de nabijheid van de as dichter op elkaar staan dan aan de buitenkant. De hoeveelheid informatie die een schijf kan bevatten wordt dan ook bepaald door de lengte van het spoor het dichtst bij de as en de 'gevoeligheid' van de registratielaag.

Bij de schijvensystemen kost het opzoeken van de benodigde plaats op de schijf nog altijd veel tijd naar computerbegrippen (afhankelijk van het schijftoerental en van het feit of vaste dan wel beweegbare lees/schrijfkoppen zijn toegepast tot enkele tientallen millisekonden), maar wel veel minder dan bij de magneetband. Er zijn in de loop der jaren ook allerlei technieken ontwikkeld om ondanks de enorme aantallen gegevens die een computer nodig kan hebben de opzoektijd zo gering mogelijk te maken. Zo worden bij grote systemen doorgaans meerdere schijven op één as gemonteerd, zodat de beheerder van het gegevensbestand de informatie dusdanig over de verschillende schijven kan verdelen dat steeds zo min mogelijk bewegingen van de lees/schrijfkoppen noodzakelijk zijn. Iedere schijf heeft bij dit soort systemen uiteraard een eigen lees/schrijf inrichting, maar deze zijn meestal ook op één arm gemonteerd en slechts tegelijk te verplaatsen. De schijven zijn vaak aan twee zijden van een registratielaag voorzien waardoor er per schijf twee maal zoveel informatie dan in het geval van een enkelzijdige bruikbaarheid kan worden opgetekend.

De ontwikkeling van schijvengeheugens is gelijk opgegaan met de ontwikkeling van het registratiemateriaal. Verbeteringen van de schijveneenheden zijn voornamelijk te vinden in de vergroting van de opslagcapaciteit per eenheid en niet in een verkorting van de toegangstijd. De grenzen worden daarbij voortdurend verlegd. Het neusje van de zalm op dit moment is de 3380 schijveneenheid van IBM die maar liefts 2,52 Gigabyte aan informatie kan bevatten, verdeeld over een tiental schijven.

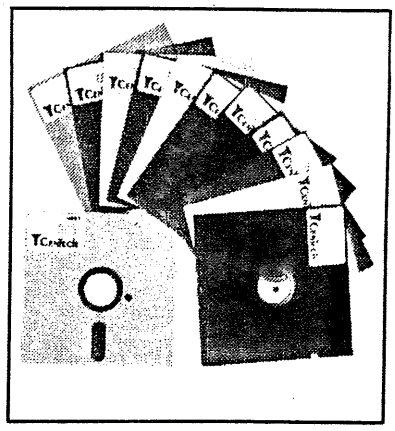
Sinds jaar en dag is IBM al koploper op het gebied van de grote schijveneenheden, waarbij collega's de markt, de plug compatible manufacturers, steeds geruime tijd nodig hebben om IBM te achterhalen. Zo introduceerde IBM haar 3380 al in 1982 en leverde zij er in 1983 al vele duizenden uit. De concurrenten moeten veelal nog beginnen met het leveren van hun 3380 compatibele eenheden. CDC hoopt haar 33800 spoedig op grotere schaal in Europa te kunnen installeren, BASF is met haar 6480 (overigens van het Japanse Hitachi) juist beginnen te leveren en Memorex heeft in de Benelux de eerste leveranties van haar 3680 schijven inmiddels afgerond. Siemens die haar apparatuur meestal van het Japanse Fijitsu betrekt heeft na het lange uitblijven van leveringen uit Japen zelfs maar besloten de eenheden van IBM te gaan verkopen.

Een vaste schijf van 14 inch diameter. De registratielaag is aangebracht op een aluminium drager.

Bij de vergroting van de informatiedichtheid per schijveneenheid gaat het er meestal om op een zo klein mogelijke oppervlakte (de DP-afdelingen kampen vaak met ruimtegebrek) zo veel mogelijk informatie op te slaan, waarbij de opslag ook nog zo min mogelijk mag kosten. Kostte de opslag van 1 Megabyte informatie in 1970 nog per maand zo'n vijftig gulden, dat bedrag is inmiddels gedaald tot een kleine twee gulden.

Floppy disc

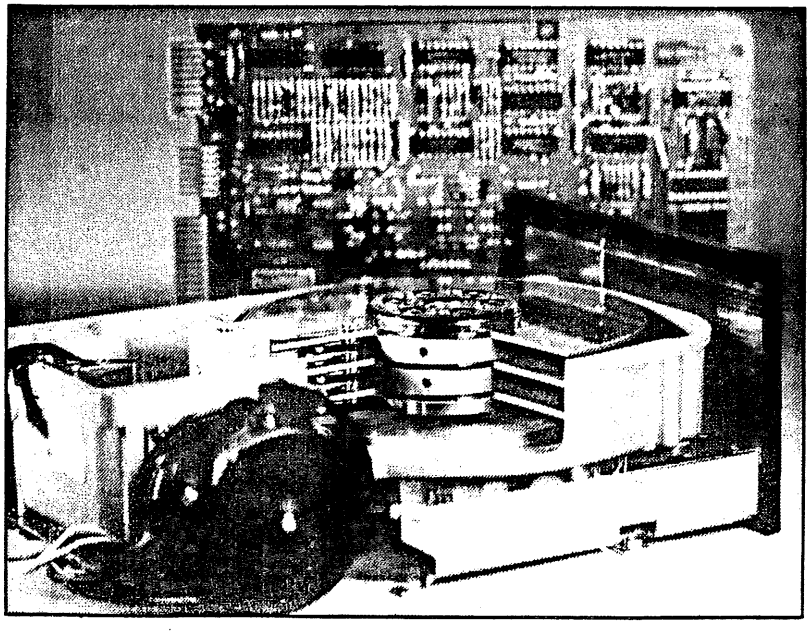
De floppy disc berust op hetzelfde principe als de harde schijf, maar hier is de gevoelige registratielaag aangebracht op niet een harde aluminium of ijzeren drager, maar op een folie zoals bij de magneetband. Door de geringere stevigheid van het medium is de levensduur ervan korter dan van de 'harde' schijf en ook de toegangstijd is langer, maar daar staat tegen over dat de apparatuur waarmee de floppy wordt gelezen en beschreven aan minder zware eisen hoeft te voldoen en daardoor veel goedkoper te produceren is. De floppy vindt dan ook voornamelijk toepassing bij personal computers en kleine systemen.
De banden, schijven en floppies bestaan in vele formaten en uitvoeringen, waarbij met name de floppy disc steeds kleiner wordt en meer informatie kan bevatten. Zo waren de floppies oorspronkelijk acht inch in doorsnede, is op dit moment de floppy met een doorsnede van 5,25 inch het meest populair en komen er al floppies aan (ten dele zijn ze zelfs al in gebruik) van 3,5 inch doorsnede. Een verkleining beneden de twee inch doorsnede zit er overigens niet in want dan zouden ze weer veel te gemakkelijk zoek raken.



Floppy discs van Centech.

De enige leverancier van 3,5 inch drives voor floppies is op dit moment Sony. Shugart heeft er recentelijk een aangekondigd, maar in Europa nog niet geleverd. De Japanse leverancier (Sony) voorziet bijvoorbeeld Apple en Hewlett Packard ervan voor hun personal computers. Andere leveranciers van drives worstelen nog met problemen om de drives in grote aantallen te fabriceren. Wel zijn een aantal fabrikanten van media al zover dat zij 3,5 inch floppies gaan vervaardigen en verkopen.

Het binnenwerk van een 5,25 inch disc drive. De drive kan 10MB of te wel 5000 getikte pagina's informatie bevatten.



Leverancier afhankelijk van PC-fabrikanten

In 1985 voor 3 miljard dollar 'kleine' drives

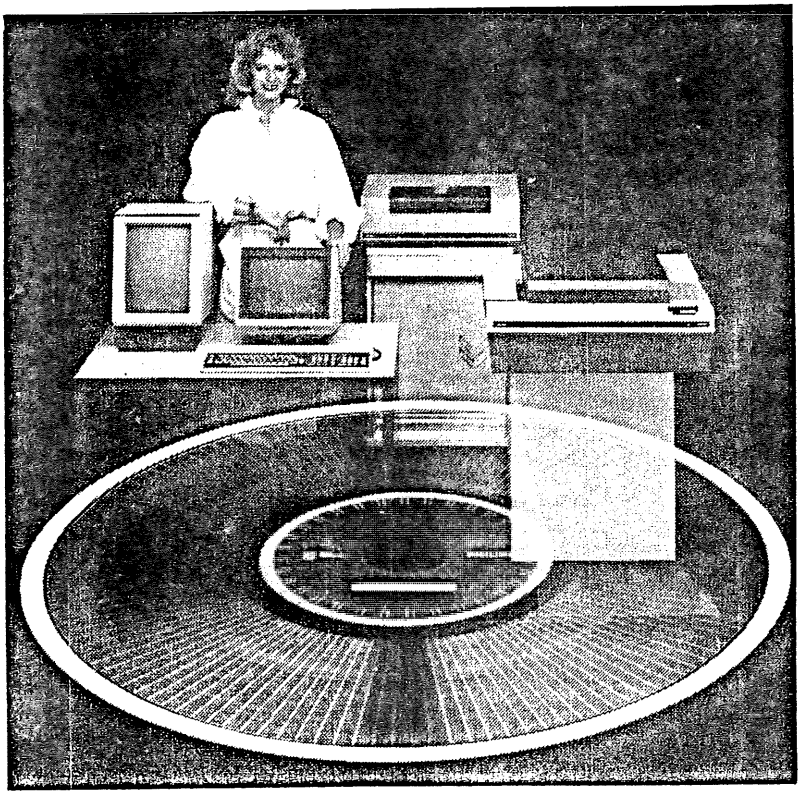
Voor de Personal Computer komt ook steeds meer de hard disc (de zogenoemde Winchester disc) in aanmerking. De enorme aantallen waarin personal computers kunnen worden verkocht en de daardoor dalende prijs per drive (die dan maar een enkele al dan niet verwisselbare schijf bevat) maken een en ander aantrekkelijk. De opslagcapaciteit van de hard disc is immers veel groter.

Marktverdeling

De belangrijkste fabrikanten van Winchester disc drives en floppy disc drives vindt men in de Verenigde Staten. Het merkwaardige feit doet zich daarbij voor dat niet één van de fabrikanten van de grote schijveneenheden voor grote computersystemen een belangrijke plaats inneemt op de markt voor 8 inch, 5,25 inch en 3,5 inch drives alsmede op de markt van de voor de PC geschikte Winchester disc drive, een drive die door speciale voorzieningen minder gevoelig is voor storingen dan de 'gewone' schijveneenheid. Wel zijn Japanse leveranciers in opmars. Immers door de grote aantallen waarin de drives verkocht kunnen worden leent de fabricage zich voor vergaande automatisering en daarin zijn de Japanners sterk. Het mechanische karakter van de drive met al haar bewegende delen speelt daarbij in de kaart van de Japanners.
De markt wordt in de hele wereld nu nog bediend door Amerikaanse bedrijven die als enigen in de zeventiger jaren een markt zagen voor deze kleine geheugen eenheden. Bedrijven als Shugart, Tandon en Seagate worden buiten deze markt nauwelijks herkend, maar de miljoenenmarkt van de drives beheersen ze. Misschien zou men moeten zeggen beheersen ze nog, gezien de recente Japanse inspanningen (bijvoorbeeld van Epson).
De meeste personal computers komen uit de Verenigde Staten en de weinige drive-leveranciers uit Europa (zoals bijvoorbeeld het Duitse Basf) nemen geen al te belangrijke plaats in. De drives worden verkocht aan producenten van PC's in de VS als IBM, Tandy, enzovoort.

Philips Megadoc was een van de eerste systemen waarin gebruik werd gemaakt digitaal optical recording.

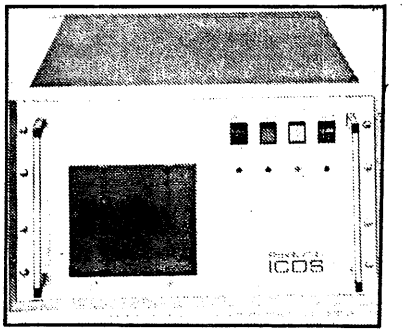
Het vermaarde onderzoeksbureau Dataquest in de VS heeft eens uitgezocht hoe de huidige marktverdeling er in de Verenigde Staten uitziet. Volgens dat bureau omvatte de markt voor de kleine drives in 1983 een dikke anderhalf miljard dollar. Daarvan werd ongeveer 1,1 miljard dollar besteed aan floppy disc drives en de rest aan Winchester disc drives. Voor 1985 verwacht het bureau een verdubbeling van de markt tot 3 miljard dollar, waarbij twee miljard dollar zal worden besteed aan drives voor floppies met een diameter van 5,25 inch of minder. Acht inch floppy disc drives worden al nauwelijks meer gemaakt.



In 1983 werden 4,7 miljoen floppy disc drives verkocht van verschillende afmetingen. Leveranciers daarvan waren voor 53 procent de firma Tandon, voor 18 procent de firma Shugart en voor 16 procent de firma ALPS Electric. De resterende 13 procent werd verdeeld onder zo'n 45 andere leveranciers.
De markt voor Winchester discs omvatte 661 duizend eenheden. De firma Seagate leverde er daarvan 42 procent. Tandon leverde 24 procent, Miniscribe 19 procent en om de andere 25 procent vochten maar liefts 40 leveranciers.
De marktleiders zijn zeer afhankelijk van de fabrikanten van Personal Computers. Toen IBM voor haar PC's naast haar huisleveranciers Seagate, Miniscribe en International Memories nog andere leveranciers ging inschakelen zakten de aandelen van Miniscribe, dat voor bijna 60 procent van haar omzet afhankelijk is van IBM, in één dag van 17 naar 12 dollar.

Inlezen

De floppy disc is door de relatief lage prijs in de loop der jaren een populair medium geworden in gegevensvastlegging toepassingen. Een servicebureau rust bijvoorbeeld haar klanten veelal uit met een eenvoudig data-invoerapparaat, waarbij na het invoeren van de gegevens de floppies per post of koeriersdienst naar het rekencentrum worden vervoerd om aldaar te worden ingelezen. Het inlezen van een floppy (die veelal enkele honderden Kilobytes aan informatie bevat) is dan een tijdrovende bezigheid wanneer niet van speciale apparatuur gebruik wordt gemaakt. Zou men de vele floppies in het gewone tempo van 1200 tot 9600 bits per seconde in lezen in het geheugen van het centrale systeem dan kost het inlezen alleen al vele uren.
De firma Longines brengt daarom apparatuur in de handel waarmee de gegevens van de floppy direct in het multiplex-kanaal van de host-computer kunnen worden ingelezen. De overdrachtssnelheid kan daardoor veel hoger zijn, zodat het inlezen van een groot aantal floppies veel min-



der tijd kost. Een volle floppy van 5,25 inch kan in 16 seconden worden gekopieerd, een volle magneetbandcassette of 8 inch floppy in een minuut respectievelijk 25 seconden. Daarbij wordt dan voortdurend de juiste overdracht van de gegevens gecontroleerd en wordt de informatie geconverteerd in een voor het centrale systeem bruikbare vorm. De Longines apparatuur wordt in Nederland geleverd door de firma Combidata te Venlo en wordt hier ten lande op verschillende plaatsen gebruikt.
Een zelfde probleem, de tijdrovendheid van het copieren van floppies, kent de leverancier van programmatuur die op floppy disc verkocht wordt. Dezelfde firma Combidata levert daarom apparatuur van fabrikant Texor om geheel automatische floppies te kopieren. Texor apparatuur kan zo'n 60 floppies in het uur voorzien van de juiste gegevens aan de hand van de te kopieren files en dat dan in de juiste formattering, want de manier waarop de gegevens over de floppy worden verdeeld verschilt vaak per PC.
Floppies zijn er in een aantal uitvoeringen. Er zijn floppies met enkelvoudige dichtheid (single density) en dubbele dichtheid (double density) en floppies kunnen enkelzijdig of dubbelzijdig gebruikt worden. In Nederland nemen Memorex, Scotch en Basf de leverantie ervan voor het grootste deel voor hun rekening. De juiste verhouding in marktaandelen van de drie leveranciers is niet te achterhalen, want alle omgeven hun omzetcijfers met de nodige geheimzinnigheid.

Ontwikkeling

De verdere ontwikkeling van de magneetband, de schijf en de floppy disc gaat hand in hand met een vergroting van de opslagcapaciteit en een verlaging van de prijs. Tegelijk met het verbeteren van de magnetische eigenschappen van de registratielaag dient daarbij de drive te worden verbeterd. Voornamelijk omdat de schijf nog niet voldoende stabiliteit heeft tijdens het draaien en de koppen nog niet gevoelig genoeg zijn. Zo verwacht men een verdere toename van de capaciteit van de schijf door toepassing van Bernoulli technologie, een techniek om de stabiliteit van de schijf te verhogen.
Zoals al gezegd vormt bij een modern registratiemateriaal als chroomdioxide de theoretische grens van 40 duizend fluxwisselingen per inch de beperking. Momenteel worden nog hoogstens 10 duizend wisselingen per inch toegepast, in het laboratorium soms 20 duizend. Bij chroomdioxide houdt de magnetische techniek echter niet op. Doordat bij chroomdioxide de magnetiseerbare deeltjes in een bed van lakdeeltjes liggen wordt de oppervlakte van de schijf nog niet optimaal benut. Vele bedrijven zijn daarom doende de schijven te voorzien van een uiterst dunne metaallaag. De magnetiseerbare deeltjes liggen daarin uiteraard tegen elkaar aan, zodat theoretisch het maximaal aantal bits per vierkante inch ook groter is. De techniek is echter nog niet volledig uitontwikkeld.
Ook wordt er gewerkt aan methoden om in plaats van de longitudinale magnetisatie (dus het in de richting van het spoor richten van magneetdeeltjes) te komen tot vertikale magnetisatie. Doordat de kleine 'magneetnaaldjes' daarbij als het ware loodrecht op de schijf staan is daarmee opnieuw een verdichting te bereiken.
Waar de ontwikkelingen uiteindelijk toe zullen leiden is vooralsnog een open vraag. Deskundigen bij Basf spreken van een praktische grens van een miljard bits per vierkante inch tegen de eeuwwisseling en bij CDC over 125 miljoen bits per vierkante inch in 1990.

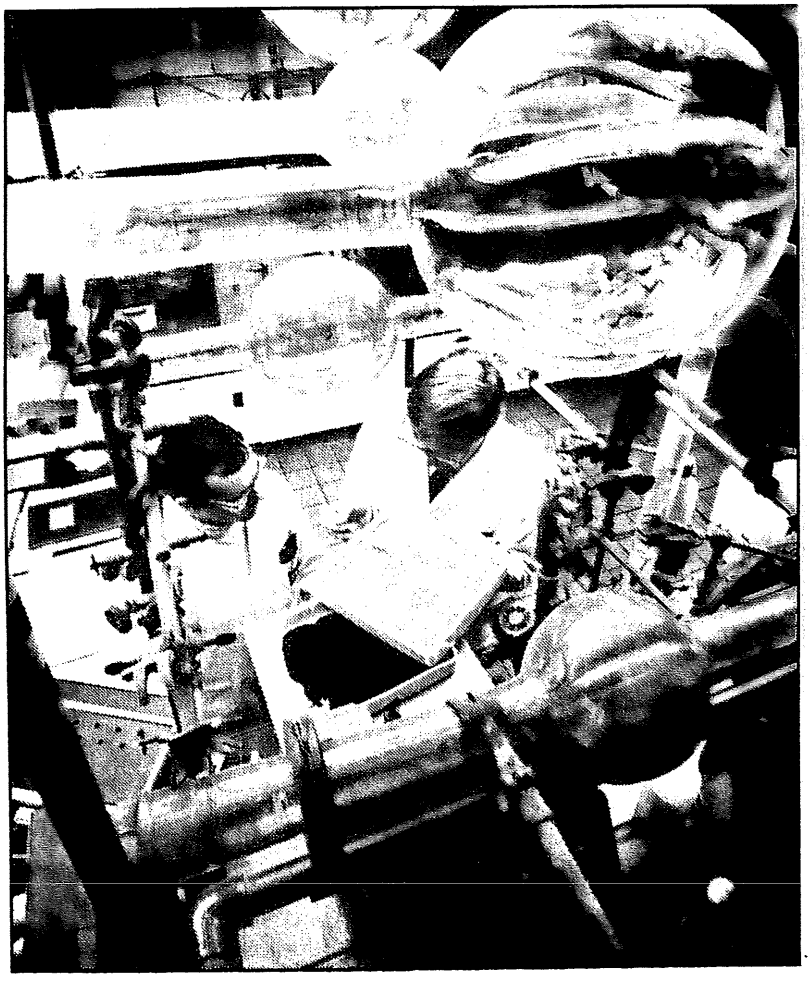
Optisch

Intussen heeft een geheel nieuwe methode van informatieopslag een groot aantal supporters gekregen. De optische optekening van gegevens doet veler harten vol verwachting sneller kloppen. Tal van concerns buigen zich momenteel over de mogelijkheden en een enkel produkt is ook al aangekondigd. Voor wat betreft de aangekondigde produkten gaat het vooral om schijven voor permanente niet wisbare optekening, later worden ook wisbare versies verwacht.

Het principe berust op het met behulp van een laser branden van gaatjes in met medium overeenkomstig de elektronische informatie. De gaatjes kunnen later weer worden afgetast met een laser zodat dezelfde informatie weer in elektronische vorm kan worden omgezet. Bedrijven die zich met deze methode van optekening bezig houden zijn onder andere Thomson CSF, Shugart, Toshiba, Storage Technology, Xerox en ons eigen Philips zowel zelfstandig als in combinatie met anderen.

Shugart heeft inmiddels een eerste produkt aangekondigd. Ook Memorex heeft vaste klanten al een werkend prototype laten zien in de VS. Het gaar daarbij om een optische schijf met een opslagcapaciteit van 1 Gigabits. In vergelijking tot de huidige magneetschijf bij gelijke diameter is dat een ongehoorde hoeveelheid. De schijf gaat samen met het bijbehorende afspeelapparaat (dat dus ook informatie kan optekenen) zo'n 25 duizend gulden kosten.

Ook Thomson CSF heeft een eerste produkt aangekondigd. De apparatuur plus schijf van Thomson CSF gaat in 1984 75 duizend gulden kosten. Het bedrijf verwacht echter in 1985 de prijs al tot 45 duizend gulden te kunnen doen dalen. Zowel voor Shugart als voor Thomson CSF hangt het succes af van de welwillendheid van andere bedrijven om op grote schaal voor dit nieuwe medium geschikte software te willen schrijven. Ook Toshiba (Toshfile) en Storage Technology (STC) hebben produkten getoond.



Iedere zich zelf respecterende fabrikant van magnetisch media beschikt over een eigen recept voor de registratielaag.

In het Nederlandse Venlo is het bedrijf Docdata ook al enige jaren bezig met het ontwikkelen van een registratieapparaat volgens de optische methode. Het bedrijf maakte vorige week bekend naar de effektenbeurs in Amsterdam te gaan om gelden te vergaren voor de verdere ontwikkeling en produktie. Docdata heeft haar activiteiten de laatste tijd overigens uitgebreid. Naast de verdere ontwikkeling van het Docwheel (een optisch geheugensysteem waarin gebruik wordt gemaakt van cassettes met optische tape en dat een grote hoeveelheid informatie vrij snel toegankelijk maakt) en de produktie daarvan heeft het bedrijf nóg twee activiteiten. De tot nu toe belangrijkste poot is het via opties op eventuele toekomstige licensies verkopen van know how. Zo heeft het bedrijf Stork in Boxmeer dat zich onder andere bezig houdt met textiel- en behangdrukmachines een optie genomen op een toekomstige licensie om gebruik te mogen maken van Docdata know how. Er zijn meer bedrijven die vooruitlopend op het uitgeven van licensies door Docdata zo'n optie hebben genomen. Met de opties zijn bedragen van vele honderdduizenden guldens gemoeid.

Standaardisatie niet rond bij optische schijf

De produktie van een 5,25 inch disc drive bij BASF.

Een derde poot van het bedrijf is nog niet zo actief, maar zal mettertijd licensies gaan verkopen voor het vervaardigen van produkten die zijn afgeleid van Docdata-produkten. Te denken valt daarbij bijvoorbeeld aan video-systemen waarbij van de Docdata registratietechniek gebruik wordt gemaakt.

Ontwikkeling en produktie

Philips kwam al enige jaren geleden op de markt met een systeem waarin voor het eerst optical recording werd toegepast. Het zogenaamde Megadoc vormt een afgerond geheel waarin een enorme hoeveelheid informatie kan worden opgeslagen. Het moet niet name in de plaats treden van microfilm en papier. Megadoc beschikt over een eigen computer voor het zoeken van informatie, maar is niet bedoeld voor directe samenwerking met grote computersystemen.

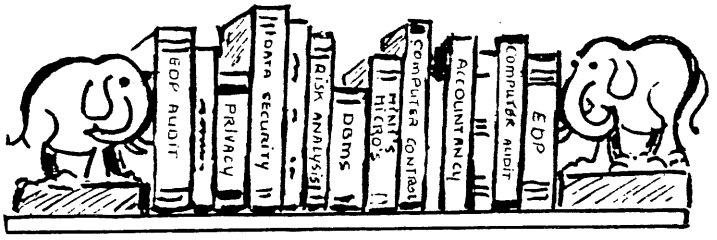
Met de schijven van Shugart en Thomson is dat wel het geval. De bedoeling is dat de optische schijven in de plaats komen van magnetische geheugens via de zogenaamde Sasi-Bus interface.

Om een dergelijk apparaat, dat dus duidelijk op de OEM-markt gericht is, te ontwikkelen ging Philips in februari 1982 een tweetal joint ventures aan met Control Data. De ene joint venture, OML (Optical Media Laboratory), is voor 52 procent in handen van Philips en voor 48 procent van Control Data. De andere jointventure, OPL (Optical Peripheral Laboratory) is voor 48 procent van Philips en voor 52 procent van MPI. MPI is een peripherie-fabrikant die voor 67 procent van Control Data is. Verder zijn aandelen in handen van Sperry (13 procent) Honeywell (17 procent) en CII Bull (3 procent).

President van OML is dr. C. J. M. Rooijmans. Volgens dr. Rooijmans zijn OPL en OML inmiddels gereed met een concept voor een 1 Gigabits cartridge (verwisselbare schijf) en bijbehorende apparatuur. OPL en OML zijn overigens ontwikkelingssamenwerkingsverbanden.

Zij zullen zich niet gaan bezig houden met de massaproduktie. Het ligt echter voor de hand dat in ieder geval Philips en MPI (delen van) het concept in produktie zullen nemen. Volgens dr. Rooijmans zijn nadere mededelingen binnen enkele maanden te verwachten.

De standaardisatie van optisch leesbare schijven is nog niet geregeld. Wel vinden er voortdurend gesprekken plaats in standaardisatiecommissies als die van de ECMA en ANSI en in sommige van die gesprekken speelt IBM een actieve rol. Volgens velen zal ook IBM namelijk binnen niet al te lange tijd met een produkt op de markt komen. Of de dan inmiddels op de markt gebrachte produkten van anderen daarna nog aan de standaard voldoen blijft tot die tijd een vraag. IBM heeft weleens vaker de markt verrast met een eigen standaard en het ligt voor de hand dat de markt straks om IBM-compatibiliteit zal vragen. Eventuele aanpassingen van de bestaande produkten na zo'n zet van IBM zullen dus moeten kunnen plaatsvinden. ●



Boeken

Boekbespreking
Titel: The Minicomputer in On-Line Systems
Auteurs: M. Healey, D. Hebditch
Gedateerd: 1981
Uitgever: Winthrop Publishers Inc., Cambridge Massachusetts
ISBN: 0-87626-579-4
Bibliotheeknummer: AC-342
Aantal pag.: 334
Besproken door H.A.J.M. Spape

"The Minicomputer in On-Line Systems" geeft een beschrijving van minicomputers en van datacommunicatie, en de wijze waarop deze samenwerken. De nadruk ligt echter duidelijk op minicomputers. De lezer die reeds bekend is met de werking van een computer en operating systems krijgt door dit boek een goede indruk van de specifiek voor kleinere computers geldende problematiek en eigenschappen in een op terminals gebaseerd computersysteem. Het boek is niet geschikt voor computerleken.
De hoofdstukken waarin het boek verdeeld is zijn vanzelfsprekend met elkaar gerelateerd, maar behandelen elk min of meer afgebakende onderwerpen. Hierdoor is het boek prettig bruikbaar voor de lezer die zich op één of enkele onderdelen van de problematiek wil richten. Om dezelfde reden zal het boek per hoofdstuk worden toegelicht. Om een indruk te geven van de diepgang waarmee een bepaald deelonderwerp behandeld wordt, is na de hoofdstuktitel procentueel aangegeven welk deel het hoofdstuk van het geheel uitmaakt, gemeten in aantal bladzijden.

Hoofdstuk 1
"The Role of the Minicomputer in Data Communications and Distributed Processing Systems" (4,4%).
Het hoofdstuk beschrijft enige typische toepassingen (bijvoorbeeld als front-end processor) van de minicomputer in datacommunicatienetwerken. De belangrijkste reden dat minicomputers in datacommunicatienetwerken worden ingezet is volgens Healy en Hebditch het feit dat ze aanmerkelijk flexibeler (en mede daardoor goedkoper) zijn dan de vroeger gebruikte niet-programmeerbare apparatuur. Ten aanzien van verscheidene aspecten wordt een vergelijking gegeven van "general purpose" mainframes, small business computers, "special purpose communications products" en minicomputers wanneer deze apparatuur wordt ingezet ten behoeve van datacommunicatie.
Dit hoofdstuk is het enige hoofdstuk dat literatuurverwijzingen bevat.

Hoofdstuk 2
"The Minicomputer: Technology and Architecture" (17,3%).
Op grond van historische ontwikkelingen trachten de auteurs aan te geven wat onder een minicomputer moet worden verstaan. Daarbij merken zij op dat hetgeen in het boek over minicomputers geschreven wordt van toepassing zal zijn op de toekomstige microcomputer. Healy en Hebditch identificeren als belangrijkste eigenschap van een minicomputer in vergelijking met andere computers het gegeven dat minicomputers oorspronkelijk ontworpen zijn voor "real-time" toepassingen (in het kader van procesbesturing). Mini's zijn "interrupt-driven"; zij worden gestuurd door gebeurtenissen in de buitenwereld. Hierdoor lenen zij zich uitstekend voor op terminals gebaseerde gegevensverwerkende computersystemen.
Er wordt uitgebreid ingegaan op de interne architectuur van de typische minicomputer. Aan de orde komen begrippen als de werking van de CPU (Central Processing Unit), busstructuren, instructiesets, adressering van het geheugen, invoer en uitvoer, hardware memory management en memory protection.
Healy en Hebditch geven aan dat steeds meer oorspronkelijk in programmatuur geïmplementeerde functies om redenen van efficiëncy in hardware worden gemaakt. Zij geven hiervan een tiental voorbeelden waaronder foutcorrigerend geheugen en hardware error logging.
Na kort op microprogrammering en 32-bit computers te zijn ingegaan wordt een beschrijving gegeven van micro-elektronica-componenten (chips), welke uitgebreid in mini- en microcomputers worden gebruikt, alsmede van de technologie waarop zij zijn gebaseerd.

Hoofdstuk 3
"Data Transmission and Terminals" (17,3%).
Hoofdstuk 3 behandelt diverse aspecten van datacommunicatie zoals soorten datacommunicatieverbindingen, ruis en andere verstoringen, en protocollen. Dit laatste is het meest uitgebreid toegelicht.
Het tweede deel van het hoofdstuk gaat in op diverse soorten terminals en op de verschillende mogelijkheden waarop een terminal met een computer kan communiceren.

Hoofdstuk 4
"Transaction Processing and a Review of Minicomputer Software" (14,3%).
Zoals de titel aangeeft is dit hoofdstuk gericht op twee verschillende onderwerpen. Het eerste geeft een inleiding tot de specifieke eisen die aan op terminals gebaseerde computersystemen te stellen zijn. Hierbij wordt naast hardware vooral gelet op de taken van de programmatuur. Het tweede onderdeel van het hoofdstuk geeft dan aan waar de implementatie van die specifieke eisen in het algemeen binnen de besturingssoftware te vinden is. Hierbij komen zaken aan de orde als Operating Systems, Transaction Processing Monitors, Terminal Drivers, alsmede multi-tasking, reentrancy, virtual storage e.d.

Allerlei begrippen die met besturingsprogrammatuur te maken hebben worden verduidelijkt. De auteurs verzuimen hierbij niet de gehanteerde terminologie te definiëren alvorens deze te gebruiken.

Tevens wordt ingegaan op het gebruik van "high-level-languages" op minicomputers. Hierbij wordt de conclusie getrokken dat nogal wat verbeterd kan worden aan de bruikbaarheid van hogere programmeertalen op minicomputers. De auteurs vinden, in het licht van computers met vele terminals, het feit dat er weinig compilers zijn die reentrant code afleveren veruit het zwakste punt bij toepassing van deze programmeertalen.
Het hoofdstuk besluit met File Management Systems en een korte beschrijving van datacommunicatie software.

Hoofdstuk 5
"Data Communications Handling on Minicomputers" (6,3%).
Dit hoofdstuk gaat vrij gedetailleerd in op de functies van computer hardware die belangrijk zijn bij terminal-afhandeling. Dit gebeurt aan de hand van twee voorbeelden, de PDP-11 serie van Digital Equipment Corporation (DEC) en de MODCOMP II CP2 van Modular Computer Systems. De eerste is min of meer een "general purpose" minicomputer, de tweede is speciaal bedoeld als datacommunicatiecomputer (CP=Communications Processor).

Hoofdstuk 6
"Data Communications Software" (7,4%).
Enkele fundamentele problemen ten aanzien van besturings- en applicatieprogrammatuur voor teleprocessing omgevingen worden onderzocht en praktische oplossingen voor aan dit soort programmatuur te stellen eisen worden voorgesteld. De problematiek wordt behandeld aan de hand van een applicatie die een bestand bijwerkt aan de hand van berichten van terminals. Met name de structuur van een operating system is in zo'n geval geheel anders dan wanneer het bijwerken van het bestand stapelgewijs zou gebeuren (bijvoorbeeld door de mutaties te lezen van een magneetband). Voor de problematiek die veroorzaakt wordt doordat verschillende gebruikers één programma moeten delen worden steeds verder verfijnde oplossingen voorgesteld.
Op soortgelijke wijze worden problemen geschetst die ontstaan door het gebruik van meerdere programma's door meerdere gebruikers en wordt ingegaan op de moeilijkheden die voortkomen uit het feit dat alle gebruikers gebruik maken van het interne en externe geheugen.

Hoofdstuk 7
"Minicomputer Operating Systems: Some Examples" (16,1%).
In dit hoofdstuk kan de lezer vaststellen in welke mate de in voorgaande hoofdstukken geschetste eisen welke aan een terminalgeoriënteerd computersysteem te stellen zijn, kunnen worden teruggevonden bij in de praktijk gebruikte operating systems. Dit hoofdstuk is eveneens van belang voor degene die niet zozeer gericht is op on-line systems of de rol van de minicomputer daarin maar die geïnteresseerd is in de werking van de beschreven operating systems.

Er worden vier besturingssystemen voor minicomputers en één voor microcomputers toegelicht zijnde:
- RSX 11-M (Digital Equipment Corporation);
- RDOS (Data General);
- MAXCOM (MODCOMP);
- DX10 (Texas Instruments);
- CP/M (Digital Research).

Naast de beschrijving van de besturingssystemen wordt uitgebreid ingegaan op een netwerk (DECNET) om minicomputers met elkaar te verbinden.

Hoofdstuk 8
"High-Level Packages" (5,0%).
Dit hoofdstuk geeft een globale beschrijving van frequent op minicomputers toegepaste software in "Small Business" toepassingen.

Hoofdstuk 9
"Acquisition and Implementation" (1,3%).
Hier worden, zeer beknopt, enige punten van aandacht bij aanschaf en implementatie van een minicomputer beschreven.

Hoofdstuk 10
"Case Studies" (10,6%).
De case studies die in dit hoofdstuk beschreven worden verlangen geen antwoorden van de lezer maar zijn bedoeld om hem een indruk te laten verkrijgen van de uitgebreide toepassingsmogelijkheden van minicomputers en de verscheidenheid van aspecten verbonden aan op terminals gebaseerde computersystemen.

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

winter 1983/lente 1984

TIJDSCHRIFTEN

door mw. D. Jansen Heijtmajer, J.L.H. Kooijman en L.N.M. Straathof met medewerking van J. Kuipers

De veerkracht van grote computers
De Automatisering Gids september 1983

In tegenstelling tot de enorme aandacht die er de laatste jaren aan de ontwikkeling van de micro- en minicomputer is besteed, is er relatief weinig geschreven over de opmerkelijke ontwikkelingen van de grote mainframes.

Toen enige jaren geleden een nieuwe richting in de computertechniek werd aangekondigd, het gedistribueerd verwerken van gegevens met gebruikmaking van krachtige minicomputers, verwachtte men een opkomend gebruik van kleinere computersystemen ten opzichte van mainframes. Dit is echter niet het geval gebleken; hiervoor zijn een aantal redenen aan te wijzen:
- er waren reeds grote investeringen gedaan in apparatuur en programmatuur;
- toepassingen waren niet gemakkelijk over te zetten naar kleinere systemen;
- de DP-organisaties waren niet voldoende bereid om over te gaan op kleinere systemen.

Door de opkomst van fabrikanten van plugcompatibele verwerkingseenheden ontstond er bovendien een toenemende concurrentie op de markt van mainframes. Dit leidde tot een betere prijs-prestatieverhouding.
Voorts bracht de introductie van het systeem 3033 van IBM aan het licht dat de markt voor mainframes niet was verzadigd maar dat een relatief lagere prijs leidde tot meer afzet. Deze elasticiteit van de markt was wel verondersteld voor minicomputers maar niet voor mainframes.
De dalende apparatuurprijzen van grote systemen hadden tot gevolg dat IBM behoefte kreeg aan extra bronnen van inkomsten.
Men ging zich toeleggen op het ontwikkelen van doelmatiger systeemprogrammatuur voor mainframes, met de nadruk op een prestatieverbetering in de interactieve verwerkingsomgeving.
Andere grote computerfabrikanten, zoals Amdahl Corporation en National Advanced Systems volgden deze ontwikkelingen op de voet. Door deze verbeterde systeemprogrammatuur is het nu zo dat de moderne mainframe systemen veel doelmatiger zijn dan kleine computers bij het ondersteunen van gemengde werkzaamheden, waarbij zowel groepsgewijs als interactief wordt gewerkt. Niet alleen zijn grote systemen doelmatiger, maar ook de eenheidskosten van het on-line geheugen, de overige randapparatuur, de programmatuur, de ondersteuning en het onderhoud zijn veel lager dan bij kleinere systemen.

Verder bieden de huidige mainframes nog vele functionele voordelen ten opzichte van kleinere machines, men denke bijvoorbeeld aan responsetijden; het aan te sluiten on-line geheugen, etc.
Hoewel men over het algemeen aanneemt dat grote systemen tegenwoordig enige van de hierboven omschreven voordelen bieden, wordt vaak beweerd dat de toekomstige kleine systemen uiteindelijk deze voordelen zullen reduceren of elimineren. Er bestaan echter geen tekenen die erop wijzen dat de evolutie van de kleine systemen zich sneller zal voltrekken dan die van de grote systemen.

Conclusie
De opkomst van distributed data processing heeft niet geleid tot een relatieve vermindering van de vraag naar grote computers ten gunste van microcomputers.
Eén van de factoren die hierbij een rol spelen is het feit dat toepassingen vaak niet gemakkelijk en zonder aanzienlijke kosten over te zetten zijn van mainframes naar microcomputers.
Andere belangrijke factoren zijn de verlaging van de apparatuurprijzen van grote systemen, de efficiëntere werking van die apparatuur en de sterk verbeterde systeemprogrammatuur voor mainframes.
Dit alles heeft geleid tot een grotere afzet van grote computersystemen.

To install an Access Control System, Activities and Checklists
door Per L. Hoving
Bron: Computers & Security 2 (1983).

Naarmate steeds meer terminals worden gebruikt om toegang te krijgen tot computersystemen en de informatiesystemen steeds complexer worden, is het des te noodzakelijker om een goed toegangsbeveiligingssysteem te hebben.
Een toegangsbeveiligingssysteem dient er voor zorg te dragen dat gegevens (data) worden beschermd tegen ongeautoriseerd gebruik, wijzigen of verwijderen.

In dit artikel zijn de stappen weergegeven, die volgens de schrijver dienen te worden gevolgd om voornoemde doelstelling te realiseren.
De bedoelde stappen zijn:
1. Classification of information.
2. Information availability.
3. Access control system - implementation project.
4. Criterias for the access control system.
5. Evaluation and choice of access control program product.
6. Survey of user needs.
7. Definition of implementation activities.

1. Classification of information

De te beschermen gegevens worden ondergebracht in groepen.
Elke groep vereist een bepaalde mate van bescherming, hetgeen kan variëren van laag naar hoog.

2. Information availability

Inventarisatie van de toegangsmogelijkheden tot de gegevens.
Hierbij wordt een onderscheid gemaakt tussen:
- fysieke structuur: centrale computersysteem, computernetwerk, datatransmissiesysteem;
- logische structuur: de manier waarop bepaalde programma's toegang krijgen tot gegevens.

3. Access control system - implementation project

Installatie van een projectorganisatie, die verantwoordelijk is voor het uitvoeren van gedetailleerde studies, evaluaties en de implementatie van een toegangsbeveiligingssysteem.

4. Criterias for the access control system

Om een toegangsbeveiligingssysteem tot stand te brengen is altijd een toegangsbeveiligingsprogramma nodig, afhankelijk van de eisen en de tekortkomingen in zo'n programma zullen aanvullende beveiligingsmaatregelen nodig zijn.
Bij stap 4 worden de eisen te stellen aan een toegangsbeveiligingssysteem, vastgesteld.

Deze eisen zijn als volgt gerubriceerd:

4.1 Eisen voor verschillende wijzen van verwerking:
- batch;
- remote-job-entry;
- time-sharing;
- on-line.

4.2 Eisen met betrekking tot de componenten:
- personeel (gebruikers, analysten/programmeurs enz);
- equipment (computers, terminals e.d.);
- programma's (operating systeem, toepassingsprogrammatuur enz.);
- gegevens.

Hieronder vallen ook de criteria die bepalen hoe lang een bepaalde bewerking mag duren en wanneer een bepaalde bewerking mag plaatsvinden.

4.3 Eisen op gebied van systeembeheer, zoals (met betrekking tot):
- bijwerken van access parameters;
- mogelijkheid om lijsten op te leveren waarin bijvoorbeeld de relaties zijn vastgelegd tussen de componenten genoemd bij punt 4.2;
- bescherming van access parameters tegen onbevoegd wijzigen;
- resource calculation (berekening van het beslag dat wordt gelegd op de apparatuur en de programmatuur door het toegangsbeveiligingssysteem);
- escape routine (het verkrijgen van toegang buiten het toegangsbeveiligingssysteem om in geval van noodsituaties);
- auditing functies (rapportage van alle ongewone gebeurtenissen; bijvoorbeeld pogingen tot ongeautoriseerde toegang);
- installatie van een toegangsbeveiligingssysteem;
- onderhoud.

5. Evaluation and choice of access control program product

Op basis van de eisen gesteld in de voorafgaande fase wordt het meest geschikte toegangsbeveiligingssysteem gekozen dat op de markt verkrijgbaar is.
Indien dit geen "waterdicht" systeem is dienen aanvullende beveiligingsmaatregelen te worden getroffen om alsnog aan de gestelde eisen te kunnen voldoen.

6. Survey of user needs

In deze fase worden voor de gebruikers (of groepen van gebruikers) de behoeften vastgesteld om toegang te krijgen tot bepaalde gegevens.
Uitgangspunt hierbij is, dat niemand toegang mag krijgen tot meer gegevens dan nodig is om zijn/haar taak uit te voeren.
Hierbij komt de schrijver tot de conclusie dat een hiërarchische toegangsstructuur, die overeenkomt met de organisatiestructuur een onjuiste structuur vormt om geautoriseerde toegang tot de gegevens te regelen.

7. Definition of implementation activities

De activiteiten verbonden aan de invoering van een toegangsbeveiligingssysteem zijn in een vijftal groepen ondergebracht:

7.1 Access control system administration project.
Hieronder vallen alle activiteiten gericht op het vestigen en onderhouden van een overall beveiligingsstructuur en de noodzakelijke interfaces tussen de toegangsbeveiligingsprogrammatuur enerzijds en de toepassingsprogrammatuur datasets/files en database(s) anderzijds.

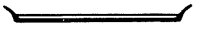
7.2 Production site project.
Het treffen van beveiligingsmaatregelen in het computercentrum.

7.3 User security administration project.
Het opstellen van procedures en standaarden voor de gebruiker ten behoeve van het (dagelijks) gebruik en onderhoud (bijvoorbeeld wijziging van parameters) van het toegangsbeveiligingssysteem.

7.4 Access control program product installation project.
De installatie van het toegangsbeveiligingsprogramma (programmatuur).

7.5 Telecommunication project.
Het zonodig treffen van maatregelen gericht op het voorkomen dat via het telecommunicatiesysteem bepaalde beveiligingsmaatregelen worden omzeild.

Aan het einde van het artikel is een checklist opgenomen waarin de activiteiten van de laatste fase gedetailleerder zijn uitgewerkt.



BUYING SOFTWARE OFF THE RACK
(het kopen van programmapakketten om de software-schaarste op te lossen)

door J. Kuipers

Bespreking van het artikel zoals dit is opgenomen in Harvard Business Review, november/december 1983 over het boek Software Maintenance: The Problem and its Solutions, geschreven door James Martin and Carma McClure.

De auteurs beschrijven dat steeds meer gebruik wordt gemaakt van kant en klare pakketten. Het gebruik van kant en klare pakketten heeft bij een aanzienlijk aantal bedrijven grote problemen gegeven. Hoewel het volgens de auteurs nodig is op te passen voor valkuilen, zijn zij van mening dat er nog te weinig gebruik wordt gemaakt van pakketten.

Goede parameterisatie is de manier om pakketten, met zo min mogelijk verandering in de procedures, te doen passen in de organisatie en de onderhoudskosten te beperken.
Met parameterisatie van een pakket wordt bedoeld dat het pakket in delen, die elk een aparte functie vervullen, is opgesplitst. De gebruiker kan door het opgeven van parameters alleen die functies nemen die hij nodig heeft. Zo is een kleinere en goedkopere versie van een pakket te kopen.

De software bronnen

Er worden vijf bronnen genoemd waar pakketten kunnen worden gekocht:

1. Computer leveranciers.
   De leveranciers leveren een zeer grote hoeveelheid applicaties, de gebruiker moet deze echter net zo kritisch beoordelen als de pakketten van andere bedrijven. Sommige pakketten zijn soms "silent salespeople", ze dwingen tot de aanschaf van extra hardware.
2. Software huizen.
   Software huizen hebben vaak uitstekende produkten, maar de kleinere bedrijven door hun zwakke management, een kort leven. De gebruikers moeten zich hiertegen wapenen door het eisen van goede documentatie en de source code, die vrijgegeven wordt indien het bedrijf failliet gaat.
3. Software makelaars, uitgevers.
   Dit zijn tussenpersonen tussen de ontwikkelaars en gebruikers.
4. Time sharing bedrijven.
   Deze bedrijven stellen software beschikbaar via teleprocessing. Time sharing kan vooral wat de kosten betreft voordeliger zijn dan kopen of leasen.

5. Gebruikersgroepen en individuele gebruikers.
   Omdat deze groepen frequent wijzigen, moet hier de nodige aandacht besteed worden aan ondersteuning, documentatie en overige zaken die de onderhoudbaarheid bepalen.

Zelf ontwikkelen of kopen?

Voordat besloten wordt een pakket te ontwikkelen of te kopen moet men de toepassing als zodanig analyseren. Naast kosten moeten de volgende aspecten overwogen worden.

- De functionele eigenschappen. Hoe complex is het? Welke tijd is er beschikbaar voor het zelf ontwikkelen?
- Achterstand in programmatuurontwikkeling.
  Een grote achterstand kan een goede reden zijn om het kopen van een pakket te overwegen. Van een gekocht pakket weet men in tegenstelling tot het zelf ontwikkelen, dat men over twee maanden voor een vastgesteld bedrag klaar is.
- Verspilde energie.
  Veel zelf ontwikkelde projecten halen de geplande eindstreep niet, dit is een verlies van geïnvesteerde energie.
- De aanwezigheid van een database.
  Is het pakket op een of andere manier aan de database te koppelen?
- De opstelling van het topmanagement.
  Soms zijn senior managers tegen het idee, van het kopen buiten de eigen onderneming, als zodanig. In dit geval zou men de economische voordelen moeten voorrekenen en erop moeten wijzen dat er programmeurs vrij komen voor belangrijker problemen.

Het selecteren van een pakket

Het selecteren van een pakket moet op een systematische manier volgens een formele procedure geschieden. Dit zou op de volgende wijze kunnen.

1. Inventariseer de huidige en toekomstige eisen voor de toepassing in detail.
2. Onderzoek alle beschikbare pakketten voor die toepassing.
3. Onderzoek programmadocumentatie en gebruikershandleidingen.
4. Controleer of het pakket voldoende geparameteriseerd is.
5. Controleer of het pakket over voldoende onderhoudshulpmiddelen beschikt.
6. Stel dan een verkorte lijst van geschikte pakketten op.
7. Indien mogelijk wordt het pakket met bedrijfsgegevens getest.
8. Stel vast of het pakket gekoppeld kan worden aan de data base.
9. Voer benchmark tests uit wanneer prestatieniveau kritisch is.
10. Laat, als de eindgebruiker interface van wezenlijk belang is, de gebruikers op tijdelijke basis met het pakket werken.
11. Ga onderhandelen om een passend contract te krijgen.

Het is vaak praktisch met gebruikers te gaan praten die het pakket al gebruiken. Hiertoe dient de leverancier een lijst met gebruikers ter beschikking te stellen.

Onderhoudsproblemen

Misschien is één van de grootste onvoorziene gevaren in het gebruik van applicatiepakketten het onderhoudsprobleem. De meeste toepassingen veranderen in de loop der tijd.
Een goede documentatie en een systematisch ontwerp zijn dus bijzonder belangrijk voor een pakket.

De Valkuilen

Een van de valkuilen in het gebruik van pakketten is het gevolg van het onvoldoende aansluiten bij de gebruikerseisen. Als in de haast een pakket wordt gekocht komen de fouten pas later aan het licht. Sommige gebruikers gaan het pakket dan zelf aanpassen, waarna blijkt dat het pakket maar moeilijk onderhoudbaar is. Daar komt dan nog bij dat de leverancier het pakket later herziet op een manier die niet aansluit op de veranderingen die de gebruiker aanbracht.
Bovendien hebben deelbedrijven een database opzet waarmee het voorgestelde pakket niet compatibel is. Steeds vaker passen de leveranciers hun pakket aan zodat van het DBMS gebruik wordt gemaakt, maar zelfs dan is er de kans dat de records en velden niet bij de, door de database administrator, gedefinieerde aansluiten.
In het laatste geval wordt, in plaats van wijzigen van het pakket, schrijven van een conversieroutine bepleit.
Een bijzonder risico is het failliet gaan van het software huis. Gebruikers moeten erop staan dat de source code goed gedocumenteerd wordt vrijgegeven ingeval van faillissement.
Om een aantal valkuilen te dichten moet gezorgd worden voor een degelijk geschreven contract tussen software leverancier en gebruiker.

Het contract

Een van de beste manieren om problemen te voorkomen is om een contract met de leverancier op te stellen. Voorkomen is beter dan genezen.
De auteurs stellen dat het contract zo belangrijk is dat de gebruikers elders naar een pakket moeten gaan zoeken als de leverancier weigert om een redelijk contract op te stellen.
Het contract moet gedetailleerd zijn en algemene of subjectieve normen vermijden.

De volgende gebruikersbescherming dient opgenomen te worden.

1. "Quiet enjoyment", het onverbreekbaar recht op het gebruik van een goed functionerend systeem.
2. Onbeperkt gebruik, het recht om het systeem over te dragen of te gebruiken ten behoeve van dochterondernemingen, filialen of opvolgers.
3. Integratie met andere systemen, het recht om het systeem en/of de bijbehorende data met andere, niet van de leverancier afkomstige, systemen te integreren.
4. Back-up, het recht om het systeem en de bijbehorende documentatie te kopiëren voor back-up doeleinden ingeval het originele vernietigd wordt.
5. Need-to-know toegang, het recht derden als personeel, software leveranciers of adviseurs kennis te laten nemen van het systeem en de documentatie.

Gekochte software moet een acceptatietest ondergaan op het moment van installatie. De koper moet wachten met betaling van de laatste termijn tot voldaan is aan de testeisen. In een testclausule kan worden vastgelegd dat zonder kosten terugbetaling plaatsvindt als niet voldaan wordt aan de testeisen. De testeisen worden hiervoor duidelijk in het contract opgenomen.

Onderhoudbaarheid wordt verder bevorderd door het opnemen van precies omschreven garantiebepalingen. Om voldoende aandacht van de leverancier te krijgen (vooral indien de afnemer commercieel minder aantrekkelijk is voor de leverancier) dienen in het contract voorwaarden opgenomen te worden die de contractbreuk behandelen, bijvoorbeeld vervanging van de software binnen een bepaalde termijn en boetebedingen.

Speciale contractvoorwaarden dienen te voorzien in een servicegarantie, een clausule voor nieuwe versies, een contractverlengingsoptie en een beëindigingsclausule:

Met betrekking tot service

De snelheid waarmee de leverancier op een verzoek tot service moet reageren, binnen welke tijd en op welke manier fouten hersteld dienen te worden en een boetebeding voor het geval aan bovenstaande niet wordt voldaan.

Met betrekking tot nieuwe versies

De eis dat het uitgeven van een nieuwe versie aan de klant bekend wordt gemaakt, de voorwaarden waartegen nieuwe 'releases' worden verkregen.

Met betrekking tot contractverlengingsoptie

De leverancier dient het onderhoud gedurende de bruikbare levensduur (veelal langer dan de contractduur) van het pakket te garanderen. Omdat leveranciers zich over het algemeen niet graag vastleggen voor langere periodes dient een contractverlengingsoptie opgenomen te zijn.

Ingeval de software geleased wordt is de klant vaak geheel afhankelijk van de leverancier voor het onderhoud. Wanneer de leverancier niet voldoet aan de voorwaarden is het vaak zinvoller om een andere leverancier het onderhoud te laten verzorgen dan het bedingen van boete. Daartoe wordt een beëindigingsclausule opgenomen die dit regelt. Een clausule voor het verkrijgen van de source code voor het geval de leverancier met het pakket stopt kan hier op aansluiten.

Een niet uitputtende opsomming van contractclausules en onderwerpen is hieronder opgenomen.

Algemeen
Namen en adressen van partijen.
Effectieve contractdatum.
Contractvoorwaarden.
Arbitrage in geval van onenigheid.
Overmacht.
Garanties.
Contractbreuk en verhaalmogelijkheden.
Beperking van aansprakelijkheid.
Recht op contractbeëindiging.

Specifiek
Betaling.
Bijkomende kosten.
Koopopties.
Verlengingsoptie.
Levering en installatie.
Prestatiespecificaties.
Computersysteemvereisten.
Documentatie:
- bediening;
- gebruikershandleiding;
- systeemdocumentatie;
- beschikbaarheid toekomstige documentatie.

Training, instructie van gebruikers.
Garantiebepalingen en verhaalsrecht bij contractbreuk ten aanzien van:
- prestatie;
- kwaliteit;
- recht op herziening;
- copyrights, patenten;
- eigendomsgarantie.

Software eigendomsrecht en gebruiksrechten.
Bescherming van vertrouwelijke informatie.
Software onderhoud in relatie tot:
- betrouwbaarheidsgarantie;
- herstellingsonderhoudwerkzaamheden;
- nieuwe versies;
- het recht om software te veranderen.

De beschikbaarheid en toegang tot de source code.
Opdrachtgeving.

Dit artikel is ontleend aan het boek:
Software Maintenance: The problem and its solutions (Prentice-Hall 1983) en aan het artikel "Buying Software off the rack".
James Martin en Carma McClure.

In dit boek wordt verder ingegaan op het software onderhoudsprobleem. Martin schetst het toepassen van 4e generatie software als mogelijke oplossing voor de onderhoudbaarheid.
Het boek is in zijn algemeenheid vlot geschreven en snel door te nemen. Directe, specifieke oplossingen voor het beheersen van het onderhoudprobleem worden, voor f 168,--, niet aangedragen.

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

Praktijkdiploma Computerboekhouden
In mei wordt voor het eerst een landelijk examen voor het Praktijkdiploma Computerboekhouden afgenomen. Het examen heeft hetzelfde niveau als het Praktijkdiploma Boekhouden. Ook de opleidingen voor beide examens zullen even lang duren. Het verschil zit in de stof.

De volgende wijzigingen in de stof hebben zich voorgedaan (bezien vanuit het oogpunt van het Praktijkdiploma Computerboekhouden):
1. minder aandacht voor zaken die door de computerprogramma's worden verzorgd;
2. verwerven van vaardigheid in het invoeren van financiële gegevens in een boekhoudsysteem;
3. automatiseringstechniek en automatiseringsjargon;
4. meer aandacht voor administratieve organisatie.

Het examen bestaat uit een schriftelijk deel dat twee avonden duurt en een vaardigheidstest met betrekking tot het gebruik van computer en het boekhoudpakket.

Beveiliging

ACF2 voor het VM-besturingssysteem
Het beveiligingspakket ACF2, dat al eens in Compact nummer 26 winter 1981/1982 in het artikel "Toegangsbeveiligingsprogrammatuur" is besproken, kent naast de MVS- en VS1-versies, nu ook een VM-versie. Zijn naast VM, ook MVS en/of VS1 geïnstalleerd met de overeenkomstige ACF2-versies, dan kunnen deze samen met de VM-versie worden geïntegreerd en zo voor de beveiliging van het hele systeem zorg dragen.

VM-versie van het bibliotheekcontrolesysteem Panvalet
Panvalet is een bibliotheekcontrolesysteem voor opslag, onderhoud en beveiliging van bronprogramma's van Pansophic Systems. De VM-versie maakt communicatie tussen de programmabibliotheek en CMS-werkbestanden mogelijk. Eerdere versies waren er al voor CICS, TSO/SPF en ICCF. Het systeem is een hulpmiddel voor het effectueren van een functiescheiding tussen de ontwikkeling en de produktie.

Computer insecurity
In het Amerikaanse tijdschrift EDPACS is een bespreking opgenomen van een nieuw boek over computerbeveiliging met de nogal opvallende titel: COMPUTER INSECURITY. Schrijver is Adrian R.D. Norman; uitgever Chapman & Hall, New York.
De benadering is inderdaad vanuit de tegenovergestelde richting, namelijk die van de onveilige situatie waarin computers verkeren. Aan de hand van meer dan 100 gevallen van computermisbruik en -fraude maakt de schrijver duidelijk hoe slecht het gesteld is met risicobeheersing. Ter verduidelijking citeren we enkele fragmenten van de betreffende recensie.

> "There are many books about computer security. This interesting volume provides a compendium of information concerning computer security failures. It bridges the gap between theory and practice. The reader can see what went wrong and, hopefully, can make some rational decisions about things that need to be done.

...

> "The cases in the book are grouped into several classifications. This helps the reader to identify common elements in the situations and decide on practical controls to help prevent various threats. Norman quotes W. Ross Ashby's "Law of Requisite Variety". This law states that any set of controls must be able to handle the variety of states that is found in the system to be controlled. In short, security measures must be designed to meet all the potential attacks that may take place.