J. Ten Wolde.

compact

COMPUTER EN ACCOUNTANT

Klynveld Kraayenhof & co
ACCOUNTANTS

NUMMER 12 4E JAARGANG NAJAAR 1977

compact

VAN DE REDACTIE

In dit verlate najaarsnummer 1977 vindt U bijdragen, welke zich richten op de organisatie van systemen en de daarin opgenomen maatregelen van interne controle. D. Steeman bespreekt zijn openbare les bij de aanvaarding van het ambt van buitengewoon lector, waarin ondermeer besproken wordt welke verwachtingen de leiding mag hebben van het onderzoek, dat de accountant verricht in het kader van de controle van de jaarrekening.
"Het onderzoek van geautomatiseerde systemen door de Accountant" is de titel van het artikel van K.H. Gerritsen, waarin deze ingaat op het werk van de accountant.

In de serie "Computertoepassingen ten behoeve van de accountantscontrole" wordt de selectie van saldobiljetten bij een bank besproken.

A.B.C.- nieuws is deze keer omvangrijk. Naast een bespreking over het invoeren van de nieuwe postcode bij adressenbestanden, vindt U ook een bespreking van de "AICPA conference on computer and information systems" in mei 1977 gehouden.

In "Lezers reageren" wordt nader ingegaan op het begrip data base management systemen dat in het artikel "Het gebruik van de computer in de Accountantscontrole" van A.W. Neisingh aan de orde kwam.

Compact is een uitgave van de groep Automatisering en Controle van Klynveld Kraayenhof & Co.

Het doel van deze uitgave is informatie te verstrekken over ontwikkelingen op het gebied van automatisering en controle in binnen- en buitenland.

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

Redactie:
A.W. Neisingh, J. Philippo, D. Steeman en J.H. Urbanus.

Adres: Pr. Irenestraat 59 Amsterdam

"LEIDING, ELEKTRONISCHE INFORMATIE VERWERKING EN EIV-ACCOUNTANT"

van D. Steeman

Samenvatting van de openbare les bij de aanvaarding van het ambt als buitengewoon lector aan de Erasmus Universiteit.

Inleiding

Met de publikatie van NIvRA-geschrift 13 en het daarin tot uitdrukking gebrachte "harmoniemodel" voor de accountantscontrole kan worden gesteld, dat de theoretische behandeling van het onderwerp Automatisering en Controle voor het moment is afgerond. Men kan zich de volgende vragen stellen: Welke verwachtingen mag de leiding van een huishouding nu koesteren van de fungerende accountant in de algemene functie? Welke diepgang heeft het onderzoek van de administratieve organisatie en de daarin vervatte geautomatiseerde informatiesystemen? Hoe verhouden zich de werkzaamheden met betrekking tot de beoordeling van de opzet en de toetsing van de goede werking van de A.O.? In welke gevallen zal de leiding zelf actie dienen te nemen voor gerichte onderzoeken, daar waar de accountantscontrole niet ver genoeg reikt om in de behoefte van de leiding te voorzien?

Ontwikkelingen in het vakgebied automatisering en controle

Deze blijken enerzijds uit het groeiend aantal specialisten dat zich bezighoudt met automatisering en controle. Anderzijds blijkt dit uit de vele publikaties, vooral in de Verenigde Staten en Canada.
Van het Canadese "geschrift" Computer Audit Guidelines kan dan ten opzichte van het vergelijkbare NIvRA 13 worden gesteld, dat het meer dan NIvRA 13 een systematische en bijkans normatieve benadering geeft van de beoordeling van de interne controle.

Hoe reageert de verantwoordelijke leiding op de ontwikkeling van de automatisering?

Doorgaans is er nog een weinig systematische aanpak en reageert men heftig op incidentele gebeurtenissen als fraude en diefstal. Te weinig wordt nog systematische aandacht besteed aan de gevolgen van stagnatie in de gegevensverwerking door welke oorzaak dan ook. Vooral de maatregelen van organisatorische aard, die een blijvende bewaking vergen, krijgen te weinig continue aandacht. Overigens blijkt uit enquêtes ten behoeve van het Institute of Internal Auditors, dat in 95% van de verkregen antwoorden topmanagers zich zorgen maken over de ontwikkeling van de automatisering in hun bedrijf. De ontoereikendheid van de interne controle staat daarbij voorop.

De onafhankelijke deskundige

In Amerika kent men de EDP auditor als onafhankelijk deskundige voor de beoordeling van automatiseringsorganisaties en automatiseringssystemen. Hoewel ook in Nederland deze functiebenaming wordt gebruikt naast andere, zou een Nederlandse benaming als EIV-accountant wellicht beter kunnen worden gehanteerd.

De betekenis van het algemene EIV-onderzoek

Het EIV-onderzoek kan worden gedefinieerd als:

"Het - door een onpartijdige deskundige - kritisch beoordelen van de opzet en de werking van de automatiseringsorganisatie en de geautomatiseerde informatiesystemen."

Het algemene EIV-onderzoek richt zich op de betrouwbaarheid; het bijzondere EIV-onderzoek op de doelmatigheid en doeltreffendheid.

Het algemene EIV-onderzoek als onderdeel van het onderzoek naar de administratieve organisatie is voor de accountant een controlemiddel in het kader van de jaarrekeningcontrole.
De omvang en diepgang van het onderzoek worden voor de accountant mede bepaald door de toepassing van andere controlemiddelen. Het zal derhalve voor de leiding van een entiteit niet altijd duidelijk zijn, wat de accountant wel en wat hij niet heeft gedaan ten aanzien van de administratieve organisatie.
Deze mogelijke bron van misverstanden kan worden bedwongen door overleg tussen accountant en leiding. Dit geldt in sterke mate voor EIV-systemen, omdat hier de onzekerheid van de leiding het grootst is.

Vanuit het onderzoek naar de opzet van organisatie en systemen kan worden aangeduid wat de leiding mag verwachten van het algemene EIV-onderzoek.

Ten aanzien van de controle op de volledigheid van de verwerking kan worden gesteld, dat de behoeften van leiding en accountant parallel lopen voor zover het systemen betreft waar informatie in verwerkt wordt, die uiteindelijk zijn weerslag vindt in de jaarrekening.

Bij de controle op de juistheid van de verwerking speelt het subjectieve element een veel grotere rol. Deze controles gaan vaak tot een zodanig detailniveau, dat zij voor de accountant niet interessant zijn. Indien de leiding op grond van haar behoefte verwacht, dat aan deze controles bijzondere aandacht moet worden besteed, dient hiervoor een afzonderlijke opdracht te worden gegeven.

Het beoordelen van de bevoegdheidscontroles behoort zonder meer tot de taal van de accountant, omdat deze een onderdeel vormen van het systeem van functiescheidingen. Belangen van leiding en accountant lopen hier parallel.

Het aspect tijdigheid wordt als geen ander aspect van interne controle gediend door de automatisering. De aandacht van de accountant richt zich hier vooral op de tijdige verstrekking van de juiste informatie, voor zover van betekenis voor de verslaglegging.

Functiescheidingen zijn de basis waarop het systeem van interne controle is gebaseerd. De leiding mag rapportering over enige gebreken zonder meer verwachten. Gebrek aan functiescheidingen kan als belangrijkste

oorzaak worden gezien, zowel van fraudes als van verliezen door onbedoelde fouten als gevolg van het ontbreken van het controlerend element in de organisatie.
De als gevolg van de ontwikkelingen in hard- en software gecreëerde nieuwe functies zoals systeemprogrammeur, master terminal operator en data base administrator bevatten in hun huidige vorm dikwijls tegenstrijdige taken. De EIV-accountant kan hier een bijdrage leveren bij de analyse van de taken en dient het management te wijzen op de gevaren van functievermenging.

Procedures en instructies worden voor de accountant na kritische beoordeling een gegeven voor de controle van de werking van de organisatie.
De leiding mag hier van de accountant een redelijkheidsoordeel verwachten gebaseerd op de essentiële punten van interne controle.

Over het aspect beveiliging in relatie tot EIV bestaat anders dan over de hiervoor behandelde punten nog geen eenstemmigheid. Het gaat hier om de beveiliging van de informatie welke als gevolg van de elektronische informatieverwerking voor de leiding steeds meer waarde krijgt. Het doen treffen van beveiligingsmaatregelen behoort primair tot de taak van de leiding. Beveiliging van waarden is een onderdeel van interne controle. Het beoordelen van beveiligingsmaatregelen behoort tot de taak van de EIV-accountant werkend in het kader van de jaarrekeningcontrole. Voor de technische beveiliging zal hij zich laten bijstaan door op techniek gespecialiseerde collega's.

Het beoordelen van de privacy-aspecten behoort op dit moment nog niet tot de taak van de algemene accountant. Vooralsnog zullen onderzoekingen op dit gebied via een afzonderlijke opdracht moeten geschieden. Er zijn wel veel overlappende gebieden tussen interne controle en privacy. Dit blijkt aldaar, waar het rapport van de Staatscommissie Koopmans de functiescheidingen bespreekt. Het fungeren van de accountant zou op natuurlijke wijze kunnen worden verdiept naar aspecten van privacy in het kader van een Wet op de Persoonsregistratie.

Opzet en werking van organisatie en systemen

De controle op de werking van de organisatie door de accountant is sterk afhankelijk van zijn conclusies omtrent de opzet en de mogelijkheid van het hanteren van andere controlemiddelen.

De leiding zal hier in vele gevallen zelf actie dienen te nemen. Dit gebeurt ook daar waar een accountant fungeert die ten behoeve van de leiding de organisatie aan een systematisch kritisch onderzoek onderwerpt.
In Nederland zijn de laatste jaren ontwikkelingen gaande waaruit blijkt, dat de beperkte functie van de interne accountant belast met de controle van de interne jaarrekening thans wordt vervangen door een meer zinvolle functie ten behoeve van de leiding op het gebied van de operationele management-audit. Hier is ook in het bijzonder plaats voor de EIV-accountant. De interne EIV-accountant kan zich in het bijzonder bezighouden met de continue follow-up op de handhaving van eenmaal getroffen maatregelen van interne controle en technische beveiliging.

HET ONDERZOEK VAN GEAUTOMATISEERDE SYSTEMEN DOOR DE ACCOUNTANT

door K.H. Gerritsen

1. Inleiding

Indien de informatieverzorging in een huishouding (ten dele) wordt geautomatiseerd, houdt dit voor wat betreft de functie van het administreren slechts in, dat er een ander hulpmiddel wordt gebruikt dan voorheen het geval was. De doelstelling van de interne controle, die in dit kader voorop staat, is de zorg voor de betrouwbaarheid van de informatieverzorging in de huishouding. Hierbij kan onderscheid worden gemaakt naar de aspecten volledigheid, juistheid, bevoegdheid en tijdigheid. Ook de beveiliging van de informatie is een aspect van de betrouwbaarheid van de informatieverzorging.
Deze doelstelling van de interne controle ondergaat onder invloed van de automatisering geen wijziging.
Wel zullen de in concreto getroffen maatregelen op het gebied van functiescheidingen, procedures en voorschriften onder invloed van de automatisering van de informatieverzorging wijziging ondergaan, maar dit betreffen slechts wijzigingen in de uitwerking.

Het onderzoek c.q. de beoordeling door de accountant van systemen waarin de informatieverzorging ten dele met behulp van de computer plaatsvindt, richt zich, indien het onderzoek plaatsvindt in het kader van de controle van de jaarrekening, op de betrouwbaarheid van de informatieverzorging zoals deze hiervoor is omschreven. Dit artikel heeft ten doel inzicht hierin te verschaffen.

Wij zullen achtereenvolgens ingaan op de achtergronden van het onderzoek van systemen door de accountant, het moment waarop dit onderzoek moet plaatsvinden en de aanpak van het onderzoek, waarbij de verschillende aspecten waaraan bij het onderzoek aandacht moet worden geschonken de revue zullen passeren. Tenslotte zullen wij nog enige aandacht schenken aan de wijze van rapporteren door de accountant. Allereerst zullen wij echter moeten vaststellen, wat wij onder een systeem verstaan.

2. Wat is een geautomatiseerd (informatie-)systeem?

Onder een (informatie)systeem verstaan wij, in navolging van Frielink (Encyclopedie van de bedrijfseconomie, deel IV, Administratieve Organisatie) het stelsel van informatieverkrijging, -verwerking en -verstrekking in een huishouding, het geheel hierna aan te duiden als de informatieverzorging.

Binnen een huishouding zijn afzonderlijke systemen te onderscheiden, die zich met verschillende soorten informatie bezighouden (bijvoorbeeld debiteuren, crediteuren, voorraden).
De informatieverzorging in deze systemen kan zowel handmatig als (ten dele) met behulp van een computer geschieden. In het laatste geval spreken wij van een geautomatiseerd systeem. Hierbij dienen wij te bedenken, dat zelfs bij de meest vergaande automatisering nog een gedeelte van de informatieverzorging handmatig plaatsvindt

en dat dus in feite sprake is van een geautomatiseerd gedeelte van een systeem. Het is van belang dit steeds in het oog te houden wanneer de accountant een geautomatiseerd systeem onderzoekt.
Als in het hierna volgende over een systeem wordt gesproken, wordt hiermee steeds het totaal van het handmatige en het geautomatiseerde deel van een (informatie)systeem bedoeld, tenzij het tegendeel blijkt.

3. Waarom onderzoekt de accountant geautomatiseerde systemen?

Van oudsher schenkt de accountant in het kader van de controle van de jaarrekening aandacht aan de informatiesystemen die in een huishouding functioneren, voor zover deze systemen voor hem van belang zijn. De primaire verantwoordelijkheid van de gebruiker voor de systemen blijft hierbij onaangetast. Bij het onderzoek van deze systemen let de accountant op de betrouwbaarheid hiervan, dat wil zeggen, de maatregelen van interne controle die in de systemen zijn opgenomen. Indien de aanwezige maatregelen van interne controle onvoldoende zijn, zal dit enerzijds zijn weerslag vinden in de aard en omvang van de werkzaamheden van de accountant, anderzijds in de rapportering aan de leiding van de huishouding en in het uiterste geval in zijn verklaring bij de jaarrekening.

Evenmin als de functie van het administreren verandert onder invloed van de automatisering van de informatieverzorging, verandert de functie van de accountant. Wel zal de accountant (uiteraard) zijn kennis dienen aan te passen aan de gewijzigde omstandigheden en zal hij bij het onderzoek van de informatiesystemen ten dele andere technieken dan voorheen moeten toepassen om de invloed van het geautomatiseerde systeem op de administratieve organisatie en daarmede op de accountantscontrole vast te stellen.

Steeds zal bij dit onderzoek aandacht moeten worden besteed aan de maatregelen van interne controle,die zijn opgenomen in de geautomatiseerde delen van de informatiesystemen en voor de accountant van belang zijn, ten einde te kunnen beoordelen of de systemen als geheel betrouwbaar zijn. Het totaal van de maatregelen van interne controle in het handmatige en in het geautomatiseerde deel van een systeem bepaalt of het systeem als geheel betrouwbaar is en of de accountant hiervan gebruik kan maken bij zijn controle.

Bij het onderzoek van een systeem kan naast de betrouwbaarheid ook aandacht worden geschonken aan de doeltreffendheid en de doelmatigheid ervan. Indien de beoordeling plaatsvindt in het kader van de controle van de jaarrekening, zal steeds het onderzoek naar de betrouwbaarheid van het systeem voorop staan, terwijl aan de andere aspecten niet expliciet aandacht wordt geschonken. Een onderzoek gericht op andere aspecten van systemen dan de betrouwbaarheid vereist een afzonderlijke opdracht.

4. Wanneer moet het onderzoek plaatsvinden?

Ieder geautomatiseerd systeem dat voor de accountant van belang is dient te worden onderzocht. Als criteria kunnen hierbij onder meer gehanteerd worden de invloed van het systeem op de jaarrekening en andere voor de accountant van belang zijnde verantwoordingsstukken en de mogelijkheid om al of niet op eenvoudige wijze de uitkomsten van het systeem in verband te brengen met de ingevoerde gegevens.

Het onderzoek zal in principe eenmaal dienen plaats te vinden en vervolgens opnieuw, indien er belangrijke wijzigingen in het systeem zijn aangebracht. Aangezien kleine wijzigingen in een geautomatiseerd systeem soms onbedoeld een belangrijke invloed hebben op het gehele systeem, is het vaak gewenst ook deze wijzigingen te onderzoeken.

Het onderzoek van systemen kan op verschillende momenten plaatsvinden, namelijk tijdens de ontwikkelingsfase of nadat het systeem operationeel is geworden. Het is vaak nuttig, en soms zelfs noodzakelijk, dat de accountant reeds vanaf het begin bij de ontwikkeling van een systeem betrokken is. Hierdoor kan reeds in de fase van het opstellen van de systeemeisen en de uitwerking hiervan, de accountant er onder meer op toezien, dat er voldoende maatregelen van interne controle in het systeem worden opgenomen. Dit heeft tot gevolg, dat van zijn kant in een later stadium minder wijzigingsaanvragen kunnen worden verwacht, doordat bij de beoordeling van het definitieve systeem(ontwerp) door hem geen of minder tekortkomingen worden geconstateerd.

Indien de accountant een (vrijwel) operationeel systeem onderzoekt, is het gevolg vaak, dat de principiële wijzigingsaanvragen (gericht op het verhogen van de betrouwbaarheid van het systeem), welke veelal voortvloeien uit het onderzoek van het systeem, moeilijk kunnen worden gehonoreerd. Daarom is het ook gewenst, indien de accountant niet vanaf het begin bij de ontwikkeling van het systeem betrokken is geweest, dat hij in een zo vroeg mogelijk stadium, dit wil zeggen vóórdat met de programmering wordt begonnen, aangeeft welke wijzigingen in het systeem wenselijk worden geacht. Dit kan aan de hand van het (globale) systeemontwerp, waarin onder meer een overzicht van de belangrijkste maatregelen van interne controle moet zijn opgenomen.

Na het gereedkomen van het onderzoek van het systeem moet vervolgens regelmatig worden nagegaan, of het systeem nog steeds zo functioneert als op het moment van onderzoek het geval was.

5. Wie moet het onderzoek van geautomatiseerde systemen verrichten?

De in het hoofd gestelde vraag lijkt misschien eenvoudig te beantwoorden: de behandelend accountant!
Toch is de vraag hiermee niet volledig beantwoord, aangezien niet iedere accountant de kennis heeft, die nodig is om een geautomatiseerd systeem te kunnen onderzoeken. Op grond van de mate waarin deze kennis aanwezig is, kunnen wij de accountants in drie categorieën indelen:

De eerste categorie is die van accountants, die een aanvullende opleiding hebben gevolgd, gericht op de controle van geautomatiseerde administraties. Deze specialisten (bij KKC opgenomen in de groep "Automatisering en Controle", kortweg A.C.-groep genoemd) kunnen zich zowel full-time als part-time bezighouden met het automatisering en controle-werk.
Hiernaast bestaat een categorie accountants, die weliswaar niet gespecialiseerd is op dit terrein, maar wel meer dan de basiskennis heeft. Hierbij kan bijvoorbeeld gedacht worden aan degenen, die de automatiseringscursus van KKC hebben gevolgd.
Tenslotte zijn er nog de accountants, die geen of uitsluitend de basiskennis op dit onderdeel van het vakgebied (soms zelfs vele jaren geleden opgedaan) bezitten. De laatstgenoemde categorie heeft meestal onvoldoende kennis om het onderzoek van geautomatiseerde systemen te verrichten.

Welke van de eerste twee categorieën komt er nu voor in aanmerking om geautomatiseerde systemen te onderzoeken?
Dit is afhankelijk van de mate van geavanceerdheid van de systemen. Hierbij is het ene uiterste een onderzoek van zeer eenvoudige systemen, dat (zelfstandig) wordt verricht door accountants met meer dan de basiskennis op het gebied van automatisering en controle.
Het andere uiterste is een onderzoek van zeer complexe systemen, dat uitsluitend door specialisten wordt uitgevoerd. Gewoonlijk zal een combinatie van een accountant met meer dan de basiskennis op het gebied van automatisering en controle, die in de controleploeg van de betreffende cliënt is opgenomen, en een specialist op dit terrein de voorkeur verdienen, waarbij de inbreng van de specialist zich soms kan beperken tot een adviestaak bij het begin van het onderzoek ten aanzien van de aanpak van het onderzoek en bij de evaluatie van de verzamelde gegevens ten aanzien van de afweging van de geconstateerde feiten.
Het betrekken van een accountant uit de controleploeg bij het onderzoek heeft als voordeel, dat hierdoor tijdens het onderzoek gebruik kan worden gemaakt van de in deze ploeg aanwezige kennis ten aanzien van de cliënt. Ook kan de latere verificatie, of het systeem nog ongewijzigd functioneert, gemakkelijker geschieden doordat de kennis van het systeem reeds in de controleploeg aanwezig is en het daarom veelal niet nodig is hiervoor mensen van buiten de controleploeg aan te trekken.

6. De aanpak van het onderzoek

6.1 Vooronderzoek

Alvorens te kunnen beslissen of een geautomatiseerd systeem voor de accountant van belang is en of het systeem aan een onderzoek moet worden onderworpen, zal eerst moeten worden nagegaan welke systemen aanwezig zijn en wat voor systemen het betreft.
Aspecten waaraan bij deze inventarisatie onder meer aandacht moet worden geschonken zijn:

- de aard van de informatie die in het systeem wordt verwerkt;
- de geavanceerdheid van de voor het systeem gehanteerde technieken (bijvoorbeeld methode van bestandsorganisatie en batchgewijze of postgewijze verwerking van mutaties);
- wie de gebruikers van het systeem zijn (zowel voor wat betreft het aanleveren van informatie als voor wat betreft bewaring en ontvangst hiervan);
- de plaats van het geautomatiseerde systeem in het totale systeem;
- de samenhang van het systeem met andere geautomatiseerde systemen;
- het belang van het systeem voor de bedrijfsvoering.

Aan de hand van deze inventarisatie kan worden bepaald of het systeem voor de accountant van belang is (dit wil zeggen of het voor de controle van de jaarrekening van belang is) en of het systeem aan een onderzoek moet worden onderworpen.
Indien tot een onderzoek wordt besloten, kan - mede aan de hand van deze inventarisatie - worden bepaald aan welke punten in het bijzonder aandacht moet worden geschonken in het kader van het onderzoek naar de in dit systeem opgenomen maatregelen van interne controle.
Tevens kan deze inventarisatie gebruikt worden bij het bepalen van de diepgang waarmee een systeem moet worden onderzocht.
De diepgang waarmee het onderzoek van geautomatiseerde systemen dient plaats te vinden is namelijk niet steeds dezelfde, maar kan variëren van een kritische beoordeling van de systeemdocumentatie tot een uitgebreid onderzoek van het systeem.
Met name bij voor de jaarrekening zeer kritische systemen zal een meer uitgebreid onderzoek op zijn plaats zijn, waarbij naast beoordeling van de (inhoud van de) documentatie en verificatie van de werking aan de hand van de uitkomsten van de feitelijke gegevensverwerking door de accountant, ook een uitgebreide testset kan worden samengesteld. Aan de hand van de uitkomsten van de verwerking van deze testset, waarin tenminste een aantal normale situaties, grenswaarden en de belangrijkste foutmogelijkheden zijn opgenomen, kan worden bepaald of het systeem, tenminste voor wat betreft de testgevallen, overeenkomt met de documentatie en of de verwerking plaats zal vinden volgens de intenties van het systeem.

Het lijkt gewenst hier nogmaals te benadrukken, dat te zamen met het geautomatiseerde systeem ook de procedures en voorschriften welke voor het niet-geautomatiseerde deel van het systeem gelden, moeten worden onderzocht en dat deze in totaliteit moeten worden beoordeeld.

6.2 Inventarisatie

Het eigenlijke onderzoek, dat plaatsvindt nadat het vooronderzoek is afgesloten, zal in eerste instantie moeten bestaan uit een inventarisatie van een aantal gegevens, met als doel vast te stellen welke maatregelen van interne controle in het systeem zijn opgenomen. Steeds zal ook door middel van toetsing aan de werkelijkheid moeten worden nagegaan of de getroffen maatregelen van interne controle worden nageleefd.
Vaak zullen in de automatiseringsafdeling algemeen-organisatorische maatregelen zijn getroffen die bij de opzet en bouw van systemen gelden. Dit aspect dient bij voorkeur reeds te zijn beoordeeld alvorens tot het onderzoek van systemen wordt overgegaan. Tijdens het systeemonderzoek zal op deze algemene maatregelen worden teruggevallen, terwijl dan ook zal worden nagegaan of de geldende voorschriften en procedures bij de bouw van het betreffende systeem zijn nageleefd.

Bij de inventarisatie en bij de latere evaluatie van de bevindingen dient aan een aantal aspecten aandacht te worden geschonken. Als belangrijkste aspecten zijn te noemen:

6.2.1 De gebruikers

Het systeem is er voor de gebruikers en is in feite ook van de gebruikers, aangezien zij van de uitkomsten van de informatieverwerking afhankelijk zijn. Derhalve dienen de gebruikers bij de ontwikkeling van een systeem te zijn betrokken en dienen zij ook hun goedkeuring te hechten aan de ingebruikneming van het systeem. Slechts op deze wijze kunnen de gebruikers verantwoordelijk worden gesteld voor de inhoud van het - in feite hun - systeem en kunnen zij ervoor zorgen, dat de organisatie rondom het geautomatiseerde deel van het systeem logisch in het gehele systeem is opgenomen en tijdig gereed is.
Om deze verantwoordelijkheid bij voortduring te kunnen blijven dragen dienen zij bij wijziging van bestaande systemen op dezelfde wijze te zijn betrokken als bij nieuwe systemen.
Ook moeten de gebruikers daarom regelmatig het bestaande systeem testen en/of de uitkomsten van de verwerking kritisch in detail doornemen en aansluiten met de ingevoerde gegevens, om na te gaan of het systeem nog steeds zo is als zij het destijds hebben goedgekeurd.

6.2.2 De documentatie

De documentatie is belangrijk om een goed inzicht in een systeem te kunnen krijgen. Dit geldt zowel voor de gebruiker als ook voor de systeemanalist, de programmeur, de operator en anderen,die zich op enigerlei wijze met een systeem bezighouden, waaronder de accountant. Voor de verschillende functionarissen is niet steeds dezelfde documentatie van belang. De inhoud van de documentatie dient daarom, ook voor wat betreft de gebruikte terminologie, te zijn afgestemd op degenen voor wie deze bestemd is.

6.2.3 De invoer en verwerking

De gegevens die in het systeem worden ingevoerd en verwerkt dienen geautoriseerd, juist, tijdig, en volledig te zijn en dit moet ook geconstateerd kunnen worden.
Autorisatie van de invoer is nodig om ervan verzekerd te kunnen zijn, dat alleen mutaties worden aangeboden en verwerkt, die door de functionaris, die voor de inhoud van gegevensinvoer verantwoordelijk is, zijn goedgekeurd, opdat hij deze verantwoordelijkheid kan dragen.

Om de juistheid en volledigheid van de invoer en de verwerking te waarborgen en om dit te kunnen constateren kan onder meer gebruik worden gemaakt van geprogrammeerde detail- en totaalcontroles. Soms kunnen geprogrammeerde controles ook voor controle op de tijdigheid van de invoer gebruikt worden.
De uitkomsten van deze controles dienen zichtbaar te worden gemaakt om te kunnen constateren, dat het programmadeel waarin deze controles zijn opgenomen is doorlopen.

Van belang is ook na te gaan welke procedures gelden ten aanzien van de afwerking van de door het geautomatiseerde systeem opgeleverde lijsten (invoerverslagen).

6.2.4 Het genereren van gegevens

Hieronder wordt verstaan het door het systeem opleveren van gegevens die geen rechtstreeks controleerbare relatie hebben met in het systeem ingevoerde gegevens.
De aanleiding hiertoe kunnen zijn externe gegevens (datum) of standen in gegevensverzamelingen.
Te denken valt hierbij aan de berekening van rente over rekening-courant (er wordt alleen een percentage opgegeven, dat voor een periode geldt) en aan het genereren van een tegenrekening om het evenwicht te krijgen met geaccepteerde mutaties, waarbij steeds de grootte van de mutatie tevoren onbekend is.
Bij dit soort mutaties dient toch de mogelijkheid te bestaan om op enigerlei wijze controle uit te voeren op de opgeleverde gegevens. De voor deze controle benodigde gegevens moeten middels uitvoer zichtbaar worden gemaakt.

6.2.5 De gegevensverzamelingen

De gegevensverzamelingen, in de automatisering gewoonlijk "bestanden" of met een moderne naam ook wel "data base" genoemd, zijn essentieel in een systeem.
Hierin zijn bijvoorbeeld in een debiteurensysteem de debiteurensaldi (in een mutatiebestand) en (in een afzonderlijk permanent of "raadpleeg"-bestand) de vaste debiteurengegevens als nummer, naam en adres opgeslagen. Het is van belang, dat alle bestanden juist en volledig zijn en blijven en dat dit kan worden geconstateerd. De wijze van bewaking van de bestanden is niet steeds dezelfde. Met name dienen gegevens

met een vast karakter anders te worden bewaakt dan gegevens met een variabel karakter. Voor de bewaking van variabele gegevens kan veelal mede gebruik worden gemaakt van totaalcontroles die bij invoer en verwerking worden uitgevoerd (6.2.3). Indien er een verband bestaat tussen verschillende gegevensverzamelingen, binnen één systeem of tussen verschillende systemen onderling, hetgeen zowel volgtijdig als gelijktijdig het geval kan zijn, moet dit verband geconstateerd kunnen worden. Ook moet de mogelijkheid bestaan de inhoud van zowel permanente ("raadpleeg") bestanden als van mutatiebestanden te toetsen aan de werkelijkheid. Deze toetsing moet periodiek plaatsvinden.

6.2.6 Beveiliging

Hoewel de maatregelen van beveiliging, die in een systeem moeten worden opgenomen, deel uitmaken van het totaal van de maatregelen van interne controle, wordt de beveiliging hier apart behandeld, omdat hieraan met betrekking tot de informatieverzorging enige bijzondere aspecten zijn verbonden.

Verschillende systemen zijn niet van gelijk belang voor de bedrijfsvoering. De verwerking van het ene systeem mag nog geen uur stilliggen, voor een ander systeem is het geen bezwaar als het enkele dagen of zelfs weken niet kan functioneren. De maatregelen van beveiliging die rond een systeem worden getroffen hangen hiermee ten nauwste samen. Voor een zeer kritisch systeem kan het zelfs noodzakelijk zijn alle mutaties tegelijkertijd op twee computers te verwerken, zodat de continuïteit van de verwerking te allen tijde gewaarborgd is (denk hierbij bijvoorbeeld aan een online order entry systeem).

Niet alleen de beveiliging van de apparatuur is echter van belang, maar ook moeten maatregelen getroffen worden in het kader van de beveiliging van bestanden en programmatuur. Hierbij valt onder meer te denken aan de technische beveiliging van de informatiedragers, de voorschriften voor het in gebruik nemen van de informatiedragers en het raadplegen van de bestanden, de bewaring van kopieën van bestanden en programmatuur en de bewaring van de mutaties (tenminste in een andere ruimte dan de originele bestanden, liefst in een ander gebouw). Voor de kopieën en voor de mutaties moeten bewaartermijnen zijn vastgesteld die door de betrokken gebruikers moeten zijn goedgekeurd. Al deze maatregelen moeten zijn vastgelegd, terwijl ook moet zijn geregeld wie voor het toezicht op de naleving verantwoordelijk is.

Steeds zullen de eisen, die in het kader van een ongestoorde bedrijfsuitoefening door de gebruikers aan het systeem worden gesteld, bepalend moeten zijn voor de getroffen, c.q. te

treffen beveiligingsmaatregelen, zowel ten aanzien van de beveiliging van programmatuur, bestanden en dergelijke van dit systeem als ten aanzien van de algemene beveiliging (bijvoorbeeld noodstroomvoorzieningen).
Tevens dient in het kader van de beveiliging aandacht te worden geschonken aan de beveiliging van de documentatie.
Indien documentatie verloren gaat, kan het geruime tijd duren voordat deze weer is opgebouwd (zie ook 6.2.2).
Ook dienen maatregelen te worden getroffen, opdat onrechtmatige kennisname van documentatie kan worden tegengegaan.

6.2.7 Correctieprocedures

De door invoer- (en verwerkings)programma's geconstateerde fouten moeten worden gesignaleerd en gecorrigeerd. Voor de afwerking van de fouten dienen procedures te bestaan, waarin ook de controle op de afwerking van de geconstateerde fouten moet zijn geregeld.

6.2.8 Controleerbare vastleggingen

Het is van belang, dat achteraf steeds kan worden nagegaan uit welke mutaties een saldo is opgebouwd, respectievelijk hoe iedere afzonderlijke mutatie in een eindsaldo is verwerkt. Deze relatie staat bekend onder de namen "reference trail", "management trail" of "audit trail", welke laatste naam aangeeft, dat dit verband voor de accountant van bijzonder belang zou kunnen zijn.
Het is niet strikt nodig, dat de betreffende controleerbare vastlegging op papier aanwezig is, als de gegevens waarmee de relatie gelegd kan worden maar aanwezig zijn en gelezen kunnen worden (bijvoorbeeld een vastlegging op magneetband die met behulp van een apart programma verwerkt kan worden).

6.2.9 Conversie

Bij nieuwe systemen moet reeds tijdens de ontwikkeling aandacht worden besteed aan de conversieproblematiek. Hierbij moeten ook maatregelen worden getroffen opdat de gebruikers hun verantwoordelijkheid voor de inhoud van de bestanden kunnen blijven dragen.
Voor een uitgebreide verhandeling verwijzen wij naar het artikel "Conversie van bestanden", dat is verschenen in het nummer van Compact van Voorjaar 1975 (2e jaargang nr. 1).

6.3 Evaluatie

Na de fase van inventarisatie, waarin mede is begrepen de toetsing (eventueel na een voorlopige evaluatie van de bevindingen) van de op papier getroffen maatregelen en van de voorgeschreven procedures aan de werkelijkheid, volgt de evaluatie van de bevindingen. Hier speelt de afweging van de verschillende bevindingen en de onderlinge samenhang een belangrijke rol.

Er zijn geen algemene maatstaven aan te geven met behulp waarvan bepaald kan worden of een informatiesysteem in totaal, dus inclusief het handmatige voor- en natraject van het geautomatiseerde deel van het systeem, al of niet als betrouwbaar moet worden beoordeeld. Hiervoor is het oordeel van de individuele accountant met kennis van automatisering en controle van beslissende betekenis.
Een hulpmiddel om tot een oordeel over het totale systeem te komen kan zijn het waarderen van de uitkomsten van het systeemonderzoek naar elk van de onder 6.2.1 t/m 6.2.9 genoemde aspecten met één der kwalificaties "goed", "bevredigend", "matig" of "slecht", maar ook voor het indelen in deze vier categorieën geldt weer, dat het oordeel van de individuele accountant beslissend is voor de uitkomst, terwijl het totaaloordeel geen gemiddelde behoeft te zijn van het oordeel over de verschillende onderdelen.
Nadat de evaluatie is afgerond, zal moeten worden nagegaan welke consequenties de bevindingen hebben voor de controlerend accountant en voor zijn controleprogramma. Het is noodzakelijk, dat deze consequenties worden bepaald door of in samenwerking met een accountant met voldoende kennis van automatisering en controle.

6.4 Vragenlijsten

Om het onderzoek van systemen te vergemakkelijken zijn verschillende vragenlijsten ontwikkeld, waarvan die in de NIvRA-geschriften nrs. 1 en 13 (Rapport Automatisering en Controle) en die van het Canadian Institute of Chartered Accountants (Computer Control Guidelines en Computer Audit Guidelines) wel de belangrijkste zijn. Binnen KKC is eveneens een vragenlijst ontwikkeld, die naar verwachting binnenkort gereed zal zijn voor publikatie. Deze vragenlijst is bedoeld om door de behandelend accountant te worden gebruikt als hulpmiddel bij het onderzoek van systemen. Voor het hanteren van deze vragenlijst is echter, omdat de lijst voor wat betreft de details niet uitputtend is en de te hanteren technieken er niet in zijn opgenomen, basiskennis op het gebied van automatisering en controle vereist (zie ook paragraaf 5 hiervoor). Het verdient aanbeveling om bij meer geavanceerde systemen overleg te plegen met een lid van de A.C.-groep. Een voordeel van vragenlijsten is, dat de te onderzoeken materie in grote lijnen vastligt. Het is echter niet zo dat vragenlijsten op ieder systeem zonder meer kunnen worden toegepast, aangezien steeds de algemene vraagstelling voor het onderzochte systeem moet worden geïnterpreteerd en uitgewerkt. Voor deze interpretatie en uitwerking is kennis van automatisering en controle noodzakelijk.

7. Rapportering

Zoals in hoofdstuk 3 reeds is vermeld, vindt het onderzoek naar de betrouwbaarheid van geautomatiseerde systemen door de accountant plaats in het kader van de controle van de jaarrekening. Ook is reeds gezegd, dat automatisering van de informatieverzorging de functie van de accountant niet wijzigt en dat het onderzoek van geautomatiseerde systemen niet anders moet worden gezien dan het onderzoek van niet-geautomatiseerde systemen.

Het ligt daarom voor de hand, dat over de uitkomsten van het onderzoek tenminste in dezelfde omstandigheden en op dezelfde wijze wordt gerapporteerd als bij een organisatiebrief. Veelal wordt het door de cliënt echter gewenst geacht over ieder onderzoek te rapporteren. Ongeacht hoe de rapportering aan de leiding van de huishouding is, is het gewenst, dat naar aanleiding van het in het kader van de jaarrekening verrichte onderzoek van een geautomatiseerd systeem tenminste verslag wordt uitgebracht aan de leiding van de automatiseringsafdeling en aan de gebruikers van het systeem, respectievelijk de systeembeheerders, alsmede aan de controlerend accountant (dit laatste voor het geval deze een ander is dan degene die het onderzoek heeft verricht), terwijl het concept met vorengenoemde functionarissen dient te worden besproken.
In het verslag dient te worden vermeld wie de opdracht tot het onderzoek heeft gegeven, het doel van het onderzoek, een korte beschrijving van het systeem, waarin de verwerkingswijze, de vorm van de bestandsorganisatie en dergelijke naar voren komen, en de bevindingen en aanbevelingen die uit het onderzoek voortvloeien. De bevindingen en aanbevelingen kunnen veelal het beste gegroepeerd worden naar de verschillende aspecten die in 6.2.1 t/m 6.2.9 zijn genoemd om een overzichtelijk geheel te verkrijgen en tevens om het verslag te laten aansluiten met de opzet van het onderzoek.
Tenslotte zal in het verslag gewoonlijk een conclusie staan ten aanzien van de mate van betrouwbaarheid en de beveiliging van het systeem als geheel.

8. Literatuur

- J.W. van Belkum en A.J. van 't Klooster
  Automatisering van de informatieverzorging
  Alphen a/d Rijn, 1970 - hoofdstuk 3 en 4

- D. Steeman
  Leiding, Elektronische Informatie Verwerking en EIV-accountant
  Alphen a/d Rijn, 1977
  (Zie ook de samenvatting elders in dit nummer)

- D. Steeman en J.H. Urbanus
  Begrip en praktijk van EDP-auditing
  Informatie, september 1975, pag. 436 e.v.

- NIvRA-geschriften nrs. 1 en 13, "Automatisering en Controle"
  . De invloed van de administratieve automatisering op de interne controle, Amsterdam, 1970
  . De invloed van de geautomatiseerde gegevensverwerking op de accountantscontrole, Amsterdam, 1975

- Canadian Institute of Chartered Accountants
  . Computer Control Guidelines, Toronto, 1970
  . Computer Audit Guidelines, Toronto, 1975.

LEZERS REAGEREN

Collega Cornelissen betrapte de schrijver van het artikel "Het gebruik van de computer in de accountantscontrole" erop, dat deze in het vuur van zijn betoog, zeer lichtvaardig verwees naar een boekwerk, waarvan redelijkwijze niet kon worden verwacht, dat het in zijn bezit zou zijn.

Uit het boekje "Data base en accountant" (pag. 29) citeren wij derhalve enige passages met betrekking tot de drie groepen data base management systemen.

"a) Onder de host-language systemen verstaan wij die systemen, die gebruik maken van een andere taal als gastheer. In paragraaf 1.4 en in ons voorbeeld zijn wij stilzwijgend van het gebruik van een dergelijk systeem uitgegaan. Cobol is in dit voorbeeld de "gastheer". De DML-opdrachten worden tussen de gewone Cobol-opdrachten in gezet in plaats van de normale "reads" en "writes". Het programma wordt inclusief deze opdrachten gecompileerd, nadat de DML-opdrachten waar nodig met behulp van een vóórcompileerprogramma (pre-compiler) zijn omgezet in normale Cobol-opdrachten. Het merendeel van de data base management systemen behoort tot deze groep.
De host-language systemen zijn op zich ook weer te onderscheiden in twee groepen nl. in de DBTG- en de niet DBTG-systemen.
De DBTG-systemen volgen de voorstellen van de Data Base Task Group van de Codasyl-organisatie. In bijlage 2 bij dit rapport zijn enige bijzonderheden met betrekking tot deze groep vermeld.
Voorbeelden van host-language DBTG-systemen zijn IDS, IDMS en Pholas. Twee in Nederland veel gebruikte host-language (niet-DBTG) systemen zijn IMS en Total.

b) De self-contained systemen kunnen beschouwd worden als een soort hoge programmeertalen. Bij deze systemen vormen het DBMS en taal een eenheid. De data base is alleen met de bijbehorende taal te benaderen. Deze systemen, die in de zestiger jaren met name in de V.S. opgang maakten, lijken nu wat terrein te verliezen en vinden voor zover bekend hier in Europa nog weinig toepassing. Een bekend self-contained systeem is Mark-IV.

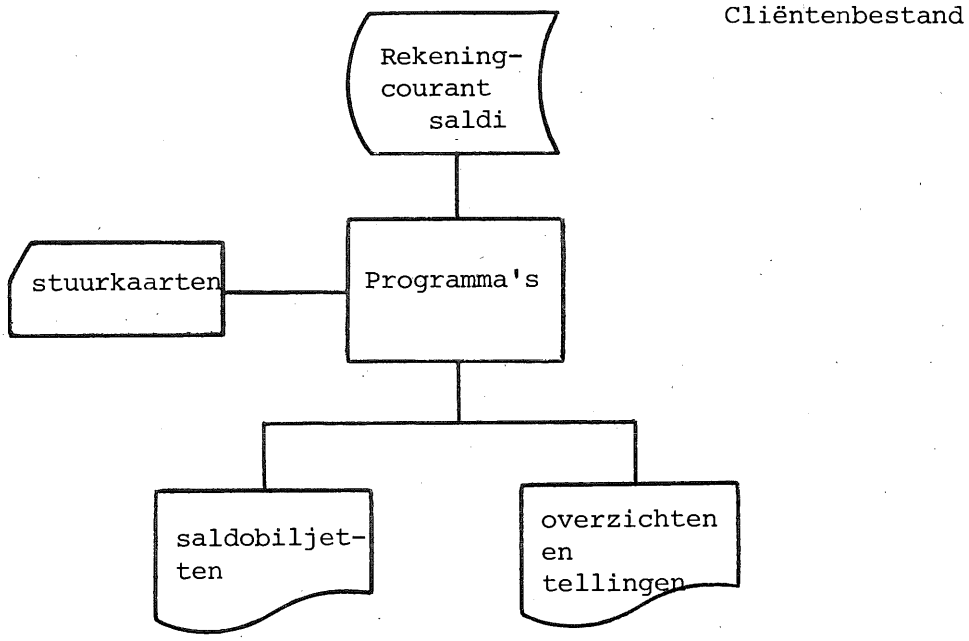
c) De full DBM systemen worden hier voor de volledigheid vermeld. Deze systemen zijn zowel host-language als self-contained. Een voorbeeld van een full DBMS is System-2000.

Wij kunnen ons voorstellen, dat deze geciteerde passages niet zo verhelderend zijn.
Om de verwarring nog wat te vergroten kan worden opgemerkt, dat de grenzen tussen de drie groepen DBM systemen vervallen.
Wij zullen in een volgend Compactnummer op deze materie terugkomen.
Van het boekje is indertijd een exemplaar naar alle kantoren gezonden.

COMPUTERTOEPASSINGEN TEN BEHOEVE VAN DE ACCOUNTANTSCONTROLE

door A. Kamstra

In het kader van de uitvoering van de controle op de jaarrekening bij een bank is in samenwerking met de interne accountant een aantal computerprogramma's ontwikkeld als hulpmiddel bij de controle op de saldi van rekeninghouders. De systeemopzet en programmering is geheel uitgevoerd door de leden van de A.C.-groep.
Het bestand, dat door de programma's gebruikt, is het cliëntenbestand waarin onder andere de volgende gegevens staan vermeld: rekeningnummer, rekeningsoort, kantoor, subkantoor, saldo, valutasoort, aantal verzonden dagafschriften, verzendcode, naam-, adres-, woonplaats-gegevens.
In schemavorm kan het ontwikkelde systeem globaal als volgt worden weergegeven:



Functies in de programma's

Selectie

De aard van de posten in het cliëntenbestand is nogal verschillend. Dit is dan ook de reden dat het bestand niet als één homogene massa wordt beschouwd, maar gesplitst is in een aantal groepen die aan verschillende selectiecriteria worden onderworpen.
Criterium voor de selectie hierbij is de mate van interne controle die per rekeningsoort kan worden uitgeoefend. Selectiecriteria zijn:

- er is een periodiek contact met de cliënt: steekproef op basis van guldenrangnummer methode;

- er is geen periodiek contact met de cliënt, doordat slechts weinig mutaties op de rekening voorkomen: selectie op grond van het aantal dagafschriften in het lopend jaar;
- de verzending van de afschriften naar de rekeninghouders geschiedt niet op de normale wijze via een onafhankelijke postkamer: selectie op grond van de verzendcode;
- het saldo is nul waardoor mogelijk het periodiek contact met de cliënt is verbroken: 1 op 10 nulsaldi wordt geselecteerd.

Stuurkaarten

Er kunnen bepaalde redenen zijn om een kantoor in haar totaliteit te selecteren (kleine organisatie met onvoldoende functiescheiding, vermoedens van fraude, twijfels ten aanzien van de werking van de organisatie). Daarom is de mogelijkheid gecreëerd ook een dergelijke selectie toe te passen.
Dit houdt in dat aan alle rekeninghouders bij een bepaald kantoor een saldobiljet wordt verzonden. Het aangeven welke kantoren geselecteerd moeten worden geschiedt evenals bovenstaande selecties door middel van in te voeren stuurkaarten. Op deze wijze zijn de selectiecriteria voor elke run aan te passen.

Uitvoer

De programma's leveren 4 soorten lijsten:

1. Saldobiljetten te verzenden aan rekeninghouders. De tekst op de saldobiljetten is zo gesteld dat indien het saldo juist is het biljet niet behoeft te worden teruggezonden (negatief saldobiljet).
2. Een lijst van de verzonden saldobiljetten; deze lijst kan gebruikt worden bij de afwerking van de retourontvangen biljetten.
3. Tellingen in aantallen en bedragen per kantoor, per selectiegroep, per valutasoort etc. Ook de geselecteerde posten worden in aantallen en bedragen geteld.
   Deze bedragen dienen ter controle op de volledigheid van het gebruikte saldibestand en voorts ter beoordeling van de diverse gebruikte selectiemethoden.
4. Een lijst met gegevens van interne rekeningen waarnaar geen saldobiljet wordt verzonden; de posten op deze lijst worden apart beoordeeld.

Waar wordt gedraaid

De structuur van het bestand is dermate complex dat via speciale bij de cliënt reeds aanwezige subroutines (kleine hulpprogramma's) de records uit het saldobestand gehaald dienen te worden. Gezien de toenmalige KKC computerconfiguratie was het onmogelijk de verwerking hierop uit te voeren. Om deze reden vindt dan ook zowel het testen als de produktie plaats op de computer van de cliënt. Beide activiteiten geschieden onder toezicht van KKCo.

A. B. C. - N I E U W S

door J.F.C. van Epen

In het tijdschrift "Alpha Topics" troffen wij een artikel aan over de invoering van de nieuwe PTT-postcode, getiteld:

"Een nieuwe postcode ..... geen sinecure".

Wij citeren:

"'Wat leeft verandert' is de aanhef van een folder waarin de PTT de komst van een nieuwe postcode bij haar eigen medewerkers introduceert.
Wat verandert is blijkens deze folder de wijze waarop straks adressen op poststukken moeten worden vermeld. Dat lijkt erg eenvoudig: Als U aan een medewerker de instructie geeft in het vervolg bij de adressering van poststukken altijd de postcode te vermelden en als U als voorbeeld ook nog de indeling van de adressen aangeeft, is die instructie eenvoudig uit te voeren."

Alpha Topics stelt echter, dat het minder eenvoudig is dan het lijkt:

"De narigheid is, dat ieder wel zijn eigen code kan weten (de PTT heeft deze reeds meegedeeld aan alle adressen), maar hoe weten wij de code-gegevens van de geadresseerde? Ik heb mij laten vertellen, dat een boek waarin alle codes vermeld staan zal bestaan uit plm. 1300 pagina's met vijf kolommen per pagina, dus vergelijkbaar met een erg dik telefoonboek."

Ten einde bij de PTT tot een beter (machinaal) sorteerproces te komen, bleek een nieuwe code noodzakelijk. De PTT zal de invoering bij de grootverbruikers doen plaatsvinden tussen 1 april 1977 en 1 april 1979. Daarna zal men trachten de particulieren te bewegen de code te vermelden (streefdatum 1 januari 1982).

In tegenstelling tot de grootverzender heeft de particulier geen voordeel van de nieuwe code. Aangezien de zogenaamde grootverzenders wel voordelen hebben van vermelding van de postcode, althans onder bepaalde voorwaarden, zal de invoering daar waarschijnlijk wel tijdig en volledig geschieden, maar dat geeft een aantal financiële en organisatorische consequenties waar wij niet te licht over moeten denken.

Bijna elk bedrijf beschikt over één of meer adressenbestanden. Bestanden waaruit periodiek een aantal poststukken worden vervaardigd, bijvoorbeeld periodiek wordt aan een aantal debiteuren een factuur gezonden of periodiek wordt aan een aantal abonnees een tijdschrift verzonden.

Vaak zijn adresgegevens onderdeel van andere gegevens en met name als deze gegevens via een geautomatiseerd systeem verwerkt worden moet men zich realiseren, dat opneming van de nieuwe postcode in het "record" en de vermelding daarvan op de poststukken de nodige software-voorzieningen kan vragen.
Grootverbruikers zullen, indien zij tenminste van de kortingmogelijkheden, die de PTT bij partijenpost-aanbiedingen (gesorteerd op postcode) geeft, willen blijven profiteren, vóór 1 april 1979 de nodige voorzieningen moeten treffen.

In technische zin zijn er twee soorten grootverbruikers:

- zij die gebruik maken van een geautomatiseerd systeem (al dan niet in eigen beheer),
- zij die gebruik maken van een mechanisch hulpmiddel bij de adressering, met als gegevensdrager een metalen of kartonnen plaatje.

Bij beide groepen zal de oude postcode reeds bestaan en moeten worden vervangen door de nieuwe. Met andere woorden: Er zal een conversie van oude naar nieuwe postcode moeten plaatsvinden. Hoe dit bij beide groepen in grote lijnen zal kunnen gebeuren, wordt hieronder beschreven.

De conversie van computerbestanden

De beheerders van computerbestanden zijn beter af dan de beheerders van plaatjesbestanden. Anderzijds doet de PTT voor de plaatjesbestanden méér dan voor de geautomatiseerde bestanden.
De beheerder van een geautomatiseerd bestand zal zich in de eerste plaats moeten afvragen of in het adresrecord ruimte is gereserveerd voor het opnemen van een zes posities vragende postcode (4 numeriek, 2 alfa).
Zo neen, dan zal ruimte geschapen moeten worden en zal de programmatuur moeten worden aangepast voor opneming en mutering van de rubriek postcode.
Voorts zal men programmatuur moeten ontwikkelen die de gegevens straatnaam, huisnummer, woonplaats, alsmede een uniek zoekgegeven uit het bestand licht en deze vastlegt op een magneetband die voldoet aan de door de PTT verstrekte specificaties.
De aldus vervaardigde tape wordt verzonden naar de PTT.
En dan komt de PTT aan bod. Met behulp van daartoe ontwikkelde programmatuur zoekt de PTT aan de hand van de woonplaatsnaam eerst de vier cijfers van de code op en voorts aan de hand van de straatnaam en het huisnummer de bijbehorende twee letters van de code. Dit stuk wordt door de PTT gratis verricht.
Inmiddels zal de beheerder van de adressenbestanden programmatuur hebben moeten vervaardigen voor het inlezen van de PTT-outputtape en het aanbrengen van de (eventueel gestandaardiseerde) straatnaam, woonplaatsnaam en de nieuwe postcode in het bestand.
Om dan tenslotte het aangepaste bestand te kunnen gebruiken dient een nieuw programma voor het sorteren en afbundelen van poststukken te zijn ontwikkeld en dienen ook de nodige printprogramma's te zijn aangepast, omdat immers in tegenstelling tot de bestaande gewoonte, straks de postcode vóór de plaatsnaam moet worden afgedrukt.
Tenslotte dient men erop bedacht te zijn, dat de conversie bij de PTT ongeveer zes weken in beslag zal nemen en dat, zo men het bestand in die tijd wil gebruiken en bijhouden, ook daarvoor de nodige maatregelen moeten worden getroffen.

Hoewel de PTT de werkelijke toekenning van de code gratis verzorgt, zal blijken, dat de invoering in de gebruikersbestanden een beduidende kostenpost zal vormen. Toch zal men zich, zolang de PTT geen andere kostenvergoedingen in het vooruitzicht stelt, deze kosten moeten getroosten, wil men in het genot blijven van de thans verkregen porti-kortingen.

De conversie van plaatjesbestanden

De beheerders van plaatjesbestanden komen nog onvoordeliger uit dan die van geautomatiseerde bestanden, ondanks het feit, dat de PTT voor de plaatjesbestanden méér gratis werk verricht.
Aan de plaatjeshouders wordt door de PTT een verzameling vóórgenummerde ponskaarten gezonden, waarop per kaart één adres kan worden afgeslagen. Daarna kunnen de kaarten worden opgezonden naar de PTT, die de postcodes erbij zoekt. Op verzoek van de bestandsbeheerder kan de PTT de gegevens uitprinten op lijsten, maar het is ook mogelijk dat de PTT een tape aflevert.
Bij aflevering van de gegevens , geprint op papier, zal daar vanaf gemuteerd moeten worden in de plaatjes. Dat betekent, dat tenminste één regel uit het plaatje volledig moet worden "gevlakt" en volledig moet worden geponst. (Immers, de postcode moet vóór de woonplaats!)
Erger nog wordt het bij gebruik van sommige soorten niet-metalen plaatjes die niet gemuteerd kunnen worden. In die gevallen moet een volledig nieuw bestand worden aangelegd.
Het is duidelijk, dat - ondanks de gratis PTT-hulp - de conversiekosten voor rekening van de gebruikers nog beduidend hoger zullen zijn dan bij de gebruikers van computerbestanden.
Ten behoeve van een plaatjesbestand kan men in principe niets doen met een door PTT te leveren tape.
Het is echter niet onwaarschijnlijk, dat een groot aantal beheerders van plaatjesbestanden van de gelegenheid gebruik zal maken om tot automatisering over te gaan.

Van de softwaremarkt

- Dynam/D

  Van het in het vorige nummer van Compact aangekondigde pakket Dynam/D van Computer Associates ten behoeve van het beheer van schijvenruimte is inmiddels een tweede versie op de markt, met een aantal nieuwe mogelijkheden, die doorvoersnelheid en beveiliging van bestanden nog verder verbeteren. Dit CA-Dynam/D-dienstprogramma maakt het mogelijk om willekeurige bestanden naar magneetband over te brengen en deze later weer op te nemen in het schijvengeheugen. Hierdoor kan de beschikbare schijvenruimte maximaal worden benut. Daar de functie onafhankelijk is van de toegepaste apparatuur, kan bijvoorbeeld een bestand van een 2314 disk pack naar een 3330 type schijf worden overgebracht.

  Verder bevat de nieuwe release een disk pool managementfunctie, die de gebruiker in staat stelt om toewijzing van schijvenruimte te doen plaatsvinden op - door middel van het serienummer gespecificeerde - disk packs, wat het mogelijk maakt om ruimtetoewijzingen in verband te brengen met de partitie waarin een programma wordt uitgevoerd. Het resultaat hiervan is een meer evenwichtig gebruik van schijvenruimte.

Behalve een beter gebruik van schijvenruimte, maakt deze functie het tevens mogelijk om op elk willekeurig disk pack bepaalde gebieden te reserveren, welke niet voor ruimtetoewijzing mogen worden gebruikt.

Voor multiprogrammeringssystemen (alleen bij DOS/VS) is er een bijzondere nuttige dynamische LUB (Logical Unit Block) functie, waarmee de gebruiker kan specificeren welke SYS-nummers dienen te worden gebruikt ingeval CA-Dynam/D deze nummers tracht te wijzigen. Tenslotte beschikt de versie 1.1 nog over de praktische eigenschap, dat alle bijzonderheden van elk in de Dynam D catalog opgenomen bestand kunnen worden weergegeven. Hoewel CA-Dynam/D slechts vijf maanden geleden in Amerka en Europa werd uitgebracht, namen tot op heden reeds meer dan 100 gebruikers het pakket in bedrijf.

(De Automatiseringsgids, 25 augustus 1977)

- Nieuwe versie van CA-Earl (= IBM-versie van IS/08!)

CA-Earl, de snelle en eenvoudig te gebruiken report generator van Computer Associates, wordt regelmatig voorzien van nieuwe toepassingsmogelijkheden. Met de nieuwste versie is de mate van flexibiliteit van het pakket dermate toegenomen, dat het volgens CA nu in staat is om tot aan 90 procent van de behoeften aan rapporteringsprogramma's van een doorsnee commercieel rekencentrum te dekken. Doordat dergelijke programma's vaak tot aan 50% van de totale ontwikkelingswerkzaamheden uitmaken, kan naar de mening van CA, toepassing van CA-Earl aanzienlijke besparingen aan programmeertijd opleveren. De nieuwe versie 2.2 van CA-Earl werd uitgebreid met de volgende mogelijkheden. Alle versies van het DL/1 data base systeem zijn nu toegankelijk door middel van een interface-routine, waarmee de CA-Earl-gebruiker de voor het systeem vereiste bewerkingsparameters kan ingeven. Het drukken van zelfklevende etiketten en voorbedrukte formulieren is nu mogelijk. Dankzij een door CA geleverde interface is nu ook VASM-support aanwezig, met inbegrip van ESDS-, KSDS- en RRDS-organisaties. Door middel van een "print exit" mogelijkheid kan de gebruiker, indien gewenst, zijn eigen routines schrijven voor de verwerking van de afzonderlijke lijnen in de CA-Earl-rapporten, wat bijvoorbeeld van nut kan zijn bij het overdragen van deze rapporten op microfilm en dergelijke.

(De Automatiseringsgids, 13 oktober 1977).

- IBM 3277 terminal werkt onder Grasp als systeemcontrole

SDI Benelux zal voor het gebruik onder de IBM besturingssystemen DOS en DOS/VS een programmapakket met de naam GRASP-OCS op de markt brengen. Behalve op de console-regeldrukker kunnen nu ook systeemboodschappen worden weergegeven via een 3277 beeldschermeenheid van IBM. Maximaal zeven van deze eenheden kunnen dan tot op achthonderd meter van de centrale verwerkingseenheid worden geplaatst. De op het scherm geprojecteerde gegevens kunnen alsnog worden vastgelegd met een regeldrukker of worden gebruikt bij GRASP en GRASP/VS-programmatuur. Hiermee kunnen gegevens betreffende bepaalde systeemfuncties, alsmede doorberekeningen van systeemgebruik worden aangemaakt.

ICL-club naar Amsterdam

In juni jl. heeft in Brussel een conferentie plaatsgevonden van een groep Europese instellingen en ondernemingen, die geïnteresseerd zijn in de 2900-computerserie van ICL. De deelnemers, verenigd in de zogenaamde 2900-club, zijn in tegenstelling tot voorheen, voor het overgrote deel géén gebruikers van deze ICL-computersystemen. De leiding van de conferentie was in handen van W.B. Cousins, managing director van het Engelse servicebureau Computel. In een commentaar op de samenstelling van de 2900-club zei Cousins: "Wij hebben besloten, dat de 2900-club zich ook moet openstellen voor hen die belangstelling hebben voor de 2900-serie.

De juni-conferentie, geopend door de Britse ambassadeur in België, heeft "The development of European computing" als thema gekregen. Een lange rij sprekers heeft dit thema van diverse zijden belicht.
De volgende onderwerpen werden behandeld:

- Wensen voor ontwikkeling van werkelijk Europese computing.
- Relatie tussen informatieverwerking en de ontwikkeling van Europese communicatienetwerken.
- De te volgen strategie voor de grote computergebruikers in een multinationale situatie.
- Verplaatsbaarheid van software en operating systems in de Europese omgeving.
- Beheer van in computergeheugens vastgelegde gegevens.

Als gastspreker tijdens de lunch op de eerste dag was ICL's managing director Geoffry Cross uitgenodigd. Hij belichtte het belang van de internationale computermarkten voor ICL. Dit toespitsend op de 2900-computers, zei hij: "De toekomst van de 2900-serie ligt in de 95% van de computermarkt, die buiten Groot-Brittanië is gelegen.

Op de tweede dag sprak de Nederlander C. Berkhouwer, vice-voorzitter van het Europese parlement, de conferentie toe. Op de hem typerende wijze waren zijn toch wel ernstige woorden humorvol verpakt, hetgeen al bleek uit de leidraad van zijn toespraak: "John citizen and the computers", waarin hij inging op de bescherming tegen elke vorm van inbreuk op individuele vrijheid. Deze lijn doortrekkend naar de automatische gegevensverwerking wees de heer Berkhouwer op het verhoudingsgewijs gemakkelijk misbruiken van vertrouwelijke gegevens door iedereen die weet hoe hij met computers moet omgaan. Een heel ander probleem dat de heer Berkhouwer aansneed, was dat van het copyright of het intellectuele eigendom van computerprogramma's. Naar zijn mening wordt het tijd, dat op dit gebied juridische maatregelen worden getroffen om de intellectuele inspanningen en geldelijke investeringen te beschermen.

Afgaande op de reacties na afloop was de tweedaagse ontmoeting uitermate geslaagd. Zo zelfs, dat intussen is besloten dat volgend jaar weer een dergelijke conferentie zal worden belegd. Die bijeenkomst zal in Amsterdam worden gehouden. Daarvoor heeft men voor 13 en 14 april het Amsterdamse Hilton Hotel besproken.

(Samenvatting van een artikel in De Automatiseringsgids, 13 oktober 1977)

Uitslag van Sherwood-enquête in VS: Netwerkconcept SNA van IBM is nog niet volmaakt

Van H.F. Sherwood & Associates - een onderneming, bestaande uit een groep van automatiseringsadviseurs - is onlangs een rapport verschenen over IBM's computernetwerkconcept SNA, voluit Systems Network Architecture. Sherwood heeft een onderzoek verricht naar de verwachtingen, die grote Amerikaanse ondernemingen hebben van het IBM-concept. In totaal tweeëntwintig bedrijven hebben hieraan meegewerkt. Het rapport bevat behalve een korte beschrijving van SNA, de lijst met vragen, een analyse van de antwoorden en een apart gedeelte met conclusies. Bijna alle deelnemers stellen zich ten opzichte van het IBM-concept nogal gereserveerd op. Dit wordt waarschijnlijk mede veroorzaakt door het feit, dat niet alle componenten voor SNA reeds beschikbaar zijn of nog niet lang genoeg op de markt om te kunnen worden beoordeeld.

VTAM-besturingssysteem vraagt veel geheugenruimte

Over de verwachtingen van SNA voor toepassing binnen hun bedrijf, hebben tweeëntwintig grote Amerikaanse gebruikers van IBM-apparatuur hun mening gegeven in een rapport, dat is samengesteld en gepubliceerd door H.F. Sherwood & Associates. Tot de ondervraagden behoorden bekende concerns als Coca Cola, Ford Motor, Northrop, Rockwell en Chemical Bank. Achttien van de deelnemende bedrijven hebben intern het IBM-concept aan een grondige analyse onderworpen, terwijl de overige vier bezig zijn met een voorstudie.
Qua apparatuur is het netwerkconcept gebaseerd op de verwerkingseenheden van de systeemserie 370 en op het 3705-communicatiebesturingssysteem. Het belangrijkste stuk systeemprogrammatuur wordt gevormd door VTAM (Virtual Telecommunications Access Method), dat dienst doet als schakel tussen de applicatieprogrammatuur en het netwerk. De 3705-besturingseenheid is uitgerust met het programma NCP/VS (Network Control Program/ Virtual System). Volgens het Sherwood-rapport is de VTAM-programmatuur weliswaar geavanceerd, maar nogal gecompliceerd en vraagt bovendien erg veel geheugenruimte.

SDLC niet compatibel met andere lijnprotocols

Verder heeft IBM voor SNA een nieuw lijnprotocol ontwikkeld, genaamd SDLC (Synchronous Data Link Control). Dit communicatieprotocol is niet compatibel met andere protocols, waardoor een aantal potentiële gebruikers van SNA gedwongen zijn om hun terminals te vervangen door SDLC compatibele terminals, hetgeen uiteraard aanzienlijke kosten met zich mee zal brengen. Volgens een aantal van de door Sherwood ondervraagde ondernemingen heeft IBM haar netwerkconcept in technisch opzicht nog niet volledig uitgewerkt. Op een aantal vragen kon men zelfs geen antwoorden krijgen en bleven IBM's mededelingen beperkt tot "heb vertrouwen in ons".
In het algemeen vonden de deelnemers aan het Sherwood-onderzoek het nog te vroeg om een gedegen analyse van het SNA-concept te maken. De meesten willen een dergelijk onderzoek over één of twee jaren weer verrichten in de hoop, dat men dan meer praktische en op ervaring gebaseerde

informatie zal kunnen krijgen. Het Sherwood-rapport besluit dan ook met de aanbeveling, dat men ten aanzien van IBM's SNA een afwachtende houding moet aannemen en ondertussen voor de teleprocessing-problemen, waarmee men nu wordt geconfronteerd, moet zoeken naar alternatieve oplossingen. Het rapport verwijst naar een aantal artikelen over SNA, te weten: "Another Look at SNA, verschenen in Het Amerikaanse blad Datamation van 23 maart 1977", "SNA, Patroon Voor Groei en Verandering (2)", in het blad Informatie, een uitgave van het Novi, verschenen in mei 1977 en de IBM-brochure nummer GA 27-3102.

(Computable)

Consumenten van computer moeten vuist leren maken

Onder deze titel verscheen in NRC/Handelsblad op 6 oktober jl. een artikel waarin het verhaal van een Amerikaanse juwelier en zijn problemen met IBM.

"Wilt U werkelijk beweren", vroeg de rechter aan de directeur van een succesvolle juweliersfirma aan de Amerikaanse oostkust, "dat een zakenman van Uw allure zo maar zijn hoofd in de strop heeft gestoken?"
Dat bleek inderdaad het geval: de juwelier had bij IBM een computersysteem aangeschaft, dat compleet de mist was ingegaan.
Ieder bedrijf dat zichzelf respecteert, heeft tegenwoordig wel een computer lopen, maar in dit geval werd eerst een verkeerd apparaat aangeschaft en toen liep ook nog eens alles mis met bijvoorbeeld de inventarissystemen. "Zij kochten goud aan wanneer zij zilver te kort hadden", zegt een deskundige die bij de zaak betrokken was losjes; "zij tuimelden van een winst van één miljoen dollar per jaar tot een half miljoen verlies".

Ten einde raad weigerde de juwelier de laatste drie maanden computerkosten te betalen. Het computerbedrijf diende daarop een vordering in en toen pas besloot de juwelier op zijn beurt het bedrijf aansprakelijk te stellen voor de geleden ellende. Dat bleek een goede gedachte te zijn geweest: de juwelier kreeg ruim elf miljoen dollar schadevergoeding toegekend (er is tegen deze uitspraak wel hoger beroep ingesteld).

Moraal van dit verhaal: "De computerconsumenten moeten niet alles slikken wat de computerindustrie hen toeschuift. Zij moeten leren een vuist te maken." Dit zegt de Amerikaanse consulent Dick H. Brandon.
Deze consulent merkt op, dat een groot deel van de "computeromzet" geheel zonder of door middel van gebrekkige contracten wordt gerealiseerd. De gebruiker is hiervan meestal de dupe, omdat hij nauwelijks terug kan. Zijn investering (inclusief software) is meestal hoger dan die van de leverancier. Hij loopt dus een groter risico.
Kern van de zaak is, dat computergebruikers leren te weten wat zij willen in plaats van zich slaafs voor de machine te buigen. Dat is een aanbeveling, die niet alleen in het belang van de portemonnaie is, maar die ook kan helpen om de nieuwe technologie beter te beheersen en op menselijke maat te houden.

AICPA conference on computers and information systems

Van deze conferentie, gehouden in Chicago van 16 tot 19 mei jl., is een verslag opgenomen in The Journal of Accountancy van juli 1977.
De conferentie werd bijgewoond door meer dan 500 belangstellenden, van wie ongeveer de helft de acht-urige sessie over "Basic computer Auditing" bijwoonde. Daarnaast vonden sessies plaats gewijd aan onder meer:

- Audit and control of advanced computer systems.
- Remote computing (time sharing), waaronder "State of the art" en "Remote computing applications".
- EDP in an accounting practice.
- Computer operations in a CPA-firm.
- Study and evaluation of internal control in EDP systems.

Genoemd verslag geeft een kort overzicht van een aantal presentaties. Wij citeren hieruit enkele passages.

Basic computer auditing

Conducted by Carol Schaller and Paul Levine of the Institute's computer services division, the course was primarily an introductory session on the impact of EDP on traditional auditing procedures. Topics included:

- EDP controls versus manual controls.
- Internal control over data processing.
- Basic audit considerations.
- Auditing files and systems.

Selecting a computer audit software package was discussed and certain requirements suggested to pick the package offering the best fit. Schaller and Levine said the following question should be asked:

- What computer audit applications will be processed?
- What computer resources are available?
- What data media must be processed?
- What level of data processing expertise is available?
- What training is required?
- What kind of support is provided?

Audit and control of advanced computer systems

Because of the success of the basic session last year, a course on the audit and control of advanced computer systems was offered at this year's conference. The course, taught by Donald L. Adams, managing director of the Institute's administrative services, attracted the second largest number of participants. The course, said Adams, is designed to fill the needs of both systems and audit personnel and assumes a basic understanding of EDP and the related controls. "Auditors must have a basic understanding of the elements of advanced systems so they can review controls and recommend revisions to meet their requirements during all the stages of design and implementation", noted Adams. Moreover, he added, auditors "must have enough expertise to get involved early and stay involved".

Study and evaluation of internal control in EDP systems

Conducted by Fred L. Lilly of Lilly & Harris, Cleveland, who is chairman of the Institute's EDP auditing standards subcommittee, the course covered requirements for reviews of internal control. Lilly stressed the importance of advance planning for the review, noting that the CPA should have a copy of the company's organization chart, position descriptions and installation standards. Separation of duties within the EDP department is crucial, he added. "Programmers shouldn't play with the computer".

Fraud and security

Professor Allen elaborated on his article "The Biggest Computer Frauds: Lessons for CPA's", in the May 1977 Journal (p. 52). He stressed lessons to be learned from large computer frauds. According to last year's records, bank losses due to computer fraud amounted to $ 200 million, Allen said. A decade ago, such losses amounted to only $20 million. Allen noted that losses for corporations are probably two to three times greater than for banks.

The methods of computer manipulation in the 150 computer fraud cases Allen studied were "not too sophisticated", the methodology was also very basic, consisting primarily of alterations and deletions. This, in Allen's opinion, suggests that there is much undetected computer fraud yet to be discovered. He predicted that there will be some major computer fraud cases uncovered in the near future.

Some contributing factors to the rise in computer fraud cases, Allen said, are as follows:

- "Internal auditors aren't keeping up with new technology".
- In the area of physical security, "auditors don't practice what they preach".
- As to online verification, the only major technical problem left to be solved is access controls.
- In the area of file controls, the question is: "How do you know the files haven't been altered?".
- Computer personnel can be difficult to manage.

Professor Allen emphasized the need for controls to combat computer fraud, particularly in the areas of transaction controls, EDP audits and responsibility reporting. Also needed is improved EDP management, especially in operations, he added.

Speaking on the same theme, Mark Polanis told of the difficulties in establishing an EDP antifraud strategy. The problem, he said, was compounded by difficulties in obtaining data because of time lags in discovery (sometimes two to three years and the reluctance of victims to give EDP fraud information. There is a need, he added, to quantify risk and exposure. No method has been set forth to grade risk "as a function of probable dimensions and frequency loss".

Polanis also observed that effective internal control can be difficult to achieve, noting that the problem of "management abdication" is often encountered. Control, he added, "must begin with top management".

State of EDP art

On a different theme, Harold Weiss, director of the Automation Training Center, Inc., spoke on the current status of computer auditing. Weiss said that internal auditors now use few advanced techniques and that EDP staffs generally "are inadequate in both quality and quantity".
But audit methods and scope are advancing despite certain road-blocks, such as the scope of audits being limited by fee size and the resistance of some audit partners to adopting sophisticated computer auditing techniques.
In the near future, Weiss predicted that auditors will require considerably more EDP knowledge. "There will be no place for traditional auditors in 5 to 10 years", he asserted, noting that the traditional auditor will be "a dinosaur in a decade".
However, he added that effective EDP specialists can't be produced in a short time. The revelation of major computer frauds in the near future, predicted Weiss, "will speed up education and the need for EDP specialists". The key to EDP in the future, Weiss said, rests with top management. In the next decade, "young management with EDP knowledge will be moving to the top in business", he added.

Kryptografie bij datatransmissie

Ontwikkeling in computerbeveiliging

De antwoorden op de groeiende behoefte aan beveiliging komen, zoals verwacht kon worden, vaak uit de Verenigde Staten van Amerika. Daar werd onlangs door Senator A.A. Ribicoff een voorstel ingediend voor een Federal Computer Systems Protection Act bij het Amerikaanse Congres, met welke wet men diefstal met behulp van computers wil tegengaan.
Ribicoff en de collega's die zijn voorstel steunen gaan ervan uit, dat computermisdaad exact genoeg is aangegeven in deze wet, zodat de bevoegde instanties effectieve stappen tegen de overtreders kunnen nemen.
Hoewel de reacties in de pers ten aanzien van de wetsvoorstellen zeer gunstig zijn, kan men zich toch afvragen of eenmaal door het Congres aangenomen de wet wel zo effectief zal blijken. In ieder geval geeft de wet geen oplossing voor de onvoorziene situatie waarin een computermisdaad aan het licht zou moeten worden gebracht. Volgens de ervaringen van deskundigen als Parker in Systems Research Institute (SRI), blijken de traditionele controlepraktijken niet in staat om subtiele wijzigingen in programma's op te sporen. Het blijkt ondoenlijk om zulke wijzigingen tijdig te onderkennen, vooral omdat zij soms op zodanige wijze zijn geprogrammeerd, dat zij bijvoorbeeld pas een halfjaar later worden uitgevoerd en dus geëffectueerd.

De mogelijkheid om op afstand toegang tot centrale computereenheden te krijgen door terminalgebruik en de mogelijkheden om terminals onderling via telefoonlijnen te verbinden, geven een nog grotere en verschillende dimensie aan het onderhavige vraagstuk.

Het Amerikaanse National Bureau of Standards (NBS) heeft van technologisch gezichtspunt een belangrijk initiatief genomen waarmee in de zojuist aangegeven omstandigheden kan worden opgetreden ter beveiliging van in computersystemen opgeslagen gegevens.
In het voorjaar van 1975 werden de computerproducenten uitgenodigd voorstellen in te leveren voor het gebruik van een encryptie-algoritme waarmee een beveiligde digitale gegevensuitwisseling mogelijk zou zijn.
In de wetenschappelijke laboratoria van IBM werd aan de ontwikkeling van zulk een procedure 17 manjaren gewerkt en het resultaat van deze studie werd door het NBS aanvaard. Dit houdt in, dat het NBS de IBM-encryptie-algoritme-toepassing verplicht stelde voor alle niet-geclassificeerde communicaties van de federale overheid. In Amerika wordt verwacht, dat deze Data Encryption Standard (DES) ook voor het bedrijfsleven verplicht zal worden gesteld.

Verschillend van de oude mechanisch werkende encrypters die eenvoudigweg symbolen door andere symbolen vervingen, verdeelt het DES-systeem de informatie in blokken van 64 bits. Het algoritme stelt vervolgens eenheden van 8 bits samen en transformeert deze volgens een block cipher code en een 56 bit "password" sleutel die door de gebruiker geheim gehouden wordt.
Een soortgelijke codesleutel is uiteraard weer nodig om informatie te decoderen.
Naar verluidt hebben ook Britse banken reeds besloten van DES gebruik te gaan maken.

Zoals te verwachten valt, worden er ook bezwaren tegen DES gelanceerd en deze zijn goeddeels het gevolg van de geheimgehouden tests die DES heeft ondergaan bij het National Security Agency (NSA).
NSA en NBS worden ervan verdacht in de encryptie algoritme de mogelijkheid te hebben ingebouwd om voor eigen gebruik informatie toch te kunnen ontcijferen, hetgeen uiteraard door het NBS ten stelligste wordt ontkend.
Niettegenstaande deze verklaring heeft onder andere Bell Telephone Laboratories Inc. besloten niet tot DES-gebruik over te gaan, maar een verbeterde versie te ontwikkelen met een uitbreiding van het sleutelformaat, omdat men van oordeel is dat de DES 56 bit sleutel te klein is.
Daarin wordt Bell bijgevallen door de Bankers Trust, dat de lengte van de sleutel tot 128 bits wil uitbreiden om discussie over een mogelijk te korte 56 bit sleutel te voorkomen.

Intussen staan de ontwikkelingen niet stil. Professor Martin Hellman van Standford University zoekt een eigen weg, zich baserend op het gebruik van zeer grote priemgetallen als sleutel. Om zulk een code te ontcijferen is zeer veel rekenwerk nodig, waarvoor onnoembare aantallen computerjaren nodig zouden zijn.

Dichter bij huis zijn er ontwikkelingen waaraan onder andere door IBM wordt gewerkt en waarmee beoogd wordt de codesleutel in de computer zelf of in de randapparatuur te verbergen, waardoor men de conceptie van "veilige systemen" zou benaderen.

Tenslotte is er dan nog een groep die stelt, dat het met de bescherming van informatie, ook van informatie in de persoonlijke levenssfeer, allemaal niet zo'n vaart loopt, maar dat daarentegen een veel groter gevaar ligt in systemen waaruit de overheid, NSA (onze BVD) of Internal Revenue Service (onze Belastingdienst) naar believen kunnen putten. Een ontwikkeling in Amerika die ons ook te wachten staat. Van grote zorg over deze problematiek is in Nederland nog niet veel te onderkennen.

(Informatie, september 1977; ingekort)

Misdaad

Brandstichting in het rekencentrum van een Duitse verzekeringsmaatschappij berokkende deze maatschappij 3,5 miljoen DM schade: apparatuur total loss.
Die Computerzeitung meldde hierover onder andere:

Ein Brandstifter legte das Rechenzentrum eines norddeutschen Versicherungsunternehmens mit einem gezielten Anschlag still. Die EDV-Anlage im Wert von 3,5 Mio. DM muss als Totalschaden abgeschrieben werden. Datenträger und der Maschinenraum sind stark in Mitleidenschaft gezogen. Der unbedingt notwendige TP-Betrieb konnte inzwischen über ein Rechenzentrum des Herstellers wieder aufgenommen werden.

Untersuchungen der Kriminalpolizei ergaben, dass weder Türen noch Fenster gewaltsam aufgebrochen worden waren.
Die gesamte Datenverarbeitungsanlage war durch Brand, Hitze oder Rauchniederschlag so stark beschädigt, dass - wie sich nach eingehender Prüfung herausstellte - keines der Geräte zu retten ist. Die meisten Datenträger sind wegen der starken Verschmutzung unbrauchbar, ein Teil der Daten kann durch Duplizierung wiedergewonnen, andere müssen rekonstruiert werden. Der Maschinenraum und die Klimaanlage sind besonders durch Salzsäureniederschlag aus den verbrannten Kunststoffen geschädigt; der Zeitaufwand für deren Sanierung und Wiederherstellung dürfte bei 4 bis 6 Wochen liegen.

Alle Schäden sind durch Sachversicherungen bzw. Haftungsfreistellung, Datenträger- und Mehrkostenversicherung für die Benutzung einer Ersatzanlage gedeckt. Wegen der Online-Verarbeitung mit Bildschirmterminals bei den verschiedenen Sachbearbeitern hängt der Geschäftsbetrief in grossem Mass von einer funktionierenden Datenverarbeitungsanalage ab.

Datenschutz und Datensicherung durch Zutrittskontrolle

Ein wichtiger Anwendungsbereich des rechnergesteuerten, freiprogrammierbaren Datensystems Tenodat 7000, das nicht nur Daten erfasst, sondern zwischenspeichert und verdichtet bzw. verarbeitet, is die Zutrittskontrolle. Für diesen Anwendungsfall stellt Telefonbau und Normalzeit dem Kunden ein spezielles Programmpaket zur Verfügung.

Zum Schutz von Sicherheitsbereichen eines Unternehmens wird beispielsweise an Türen, Schranken und Drehkreuzen jeweils ein Personaldatenterminal PDT installiert. Es dient zum Einlesen der codierten Daten von Ausweisen und zum Eintasten persönlicher Geheimnummern. Die Zentrale des Datensystems prüft dann die Zutrittsberechtigung und veranlasst bei positivem Prüfergebnis die Freigabe zum Sicherheitsbereich. Liegt aufgrund des Prüfungsergebnisses keine Zutrittsberechtigung vor, dann wird durch eine negative Quittung die Freigabe der Tür verhindert.

Im Anwendungsfall "Zutrittskontrole" erfüllt das Datensystem Tenodat 7000 folgende Aufgaben: Es prüft Zutrittsberechtigungen, überwacht Türöffnungszeiten, führt Buch über die in den Sicherheitsbereichen anwesenden Personen, druckt alle Vorgänge aus und zeichnet die erfassten Daten zur späteren Auswertung oder Dokumentation in einer zentralen DVA auf Datenträger aus.

(Die Computerzeitung, 5 oktober 1977)

Internationale Conferentie over gegevensbeveiliging te Wenen

In de Oostenrijkse hoofdstad zijn 300 deskundigen uit 24 OECD-landen bijeen geweest. Doel was het formuleren van aantal wetsregels met betrekking tot het grensoverschrijdend gegevensverkeer. Over een aantal voorgestelde wetsregels werd gediscussieerd, zoals:

- Alleen gegevensverwerking in een ander land toegestaan als de privacywetgeving van dat land overeenkomstige voorschriften kent als die in het eigen land van de onderneming.
- Verbreiden van gegevens in het buitenland is alleen toegestaan als de privé-sfeer niet wordt aangetast.
- Gegevensbanken mogen slechts met speciale vergunning persoonsgebonden gegevens exporteren.
- De "exporterende" instantie dient een kopie van de geëxporteerde gegevens te bewaren.

Die Computerzeitung, waaruit bovenstaande is ontleend, schrijft hierbij:

Dr. Gerhard Stadler (österreichisches Bundeskanzleramt) erklärte, die in den einzelnen Ländern diskutierten Gesetze sollen verhindern, dass private Informationen ins Ausland gelangen. Diese Entwicklung drohe zu einem neuen Protektionismus, zu neuen Handelseinschränkungen zu führen, wie man sie in den internationalen Beziehungen schon überwunden zu haben glaubte.

Anderseits können tatsächlich "Piraten-Datenbanken", so heisst es in der Stellungnahme weiter, in Staaten ohne Datenschutzgesetze entstehen, mit denen die staatlichen Gesetze umgangen werden können, da der Grenzübertritt von Informationen nicht kontrolierbar sei.
Weltweite Informationssysteme für die internationale Polizei, für multinationale Unternehmen, Banken oder Fluglinien, seien im Aufbau und lassen sich nicht mehr einem Staat, einer nationalen Rechtsordnung unterordnen. International Absprachen müssten zeitgerecht diese Entwicklung steuern, damit nicht tatsächlich die Anwendung der modernen Informationstechnologien zu einem Verlust an menschlicher Freiheit und zu einer Verletzbarkeit unserer Gesellschaftsordnung führen.

Apotheek met eigen computer

In verschillende dag- en weekbladen is hierover bericht. Wij citeren er één.

In de Slotervaartapotheek, in een buitenwijk van Amsterdam, heeft apotheker drs. J. Schijf (34) als eerste van zijn collegae in Nederland en misschien wel Europa, een computer met speciaal programma ingezet.

Het ding is uiterst veelzijdig. Het vermindert de wachttijd voor de patiënt, het onthoudt perfect wat de patiënt in de loop van de tijd aan medicijnen heeft geslikt, het constateert voorts of bepaalde medicijnen wel of niet te combineren zijn bij deze patiënt en en passant is het een verkapte boekhouder. Het systeem is ontwikkeld op een minicomputer van Datasaab door CMG Computer Management Group en het zal volgens deskundigen een revolutie teweegbrengen in de apothekerswereld, vooral op administratief gebied.
De patiënten hoeven zich geen zorgen te maken, dat hun medische details onder verboden ogen komen, want de computer heeft een veiligheidscode ingebouwd. Schijf heeft 11.000 patiënten en ruim 6.500 artikelen. Hij is verplicht de recepten zes jaar te bewaren. Een fout bij de administratie kan noodlottige gevolgen hebben. Schijf heeft momenteel in zijn middelgrote apotheek vijftien mensen in dienst, maar hij kan dit aantal natuurlijk niet eindeloos uitbreiden.
Van elke patiënt worden nu door Schijf de gegevens als naam, adres, ziekenfonds - particulier, arts en dergelijke ingetoetst. Het beeldscherm gaat voorts vragen stellen. Het recept komt vervolgens onder ogen van de computer, die in enkele seconden een enorme hoop handelingen verricht. Zo controleert de machine of de dosering wel voldoet aan de normen voor deze medicijn en deze gebruiker. Het belangrijkste is wel het signaleren van "interacties", dit is de invloed die medicijnen op elkaar hebben (verzwakken of versterken bijvoorbeeld). Er zijn duizenden van deze interacties en geen enkel apothekershoofd kan ze alle bevatten. Het recept gaat tenslotte naar een geheugen. De computer gaat ook na of de medicijn in voorraad is, of dat de opdracht tot bijbestellen moet worden gegeven. Het foutloos uittikken van etiketten wordt ook door de machine gedaan en het belang hiervan is evident.

Maar daarmee is de taak van de listige machine nog niet compleet. Hij tikt rekeningen uit, houdt de administratie bij van kas, giro en salarissen enz. Drs. Schijf voorziet een grote toekomst voor de computer. Over tien tot vijftien jaar zullen zijns inziens alle apotheken beschikken over zulk een elektronische dienaar.

Softwarebureaus

In Elseviers Weekblad van 8 oktober jl. troffen wij een artikel van D. Overkleeft aan waarin de betrouwbaarheid van softwarebureaus aan de kaak gesteld wordt, getiteld:

Erecode moet avonturiers uit computersector weren.

Samenvattend schrijft Overkleeft:

> De service-/softwarebureaus vormen een nog vrij jonge bedrijfstak, en de bureaus lijken soms als paddestoelen uit de grond te schieten. Onder het vele koren zit af en toe wat kaf, en wanneer er weer eens een avonturier in de computerwereld over de kop gaat, kan dat voor zijn klanten vèrstrekkende gevolgen hebben. Niet voor hen alleen trouwens, de activiteiten van een servicebureau kunnen grote delen van de samenleving omspannen. Controle en inspectie zijn dan ook meer dan noodzakelijk.

Uit het artikel ontlenen wij de volgende passages:

Er zijn momenteel zo'n 250 à 300 service-/softwarebureaus in ons land; dat zijn bureaus die computers, programma's en kennis tegen betaling ter beschikking stellen van bedrijven, die om wat voor reden dan ook (meestal de kosten) zelf geen computers en alles wat daarbij hoort in huis halen. Een soort veredelde administratiebureaus dus, al is hun dienstenpakket veel en veel uitgebreider dan dat van de traditionele administratiekantoren. Voor iemand die van de diensten van een service-/softwarebureau gebruik maakt, is het van het allergrootste belang, dat dat bureau goed werkt (de uitkomsten zijn immers door de klant niet of nauwelijks te controleren), en dat het solide is. Immers, als een gewoon administratiekantoor over de kop gaat, kan de klant vrij eenvoudig zijn stukken terughalen en een nieuw bureau zoeken; met computerprogramma's en dergelijke is dat oneindig veel moeilijker.

De service-/softwarebureaus vormen een nog vrij jonge bedrijfstak, en zoals altijd indien het om iets nieuws gaat waarmee veel geld is te verdienen, heeft ook een aantal avonturiers zich erin gestort, met alle nare gevolgen van dien. In verhouding tot het aantal bureaus is het aantal "ongelukken" misschien niet eens zo groot, maar zij vallen natuurlijk wel op. En voor de potentiële klant is het hoogst vervelend, dat er nergens een instantie is, die toezicht houdt op de handel en wandel van de service-/softwarebureaus en daarover inlichtingen kan verschaffen.

Al in 1971 werd de Vereniging van Computer Service en Software Bureaus (COSSO) opgericht. Doel van de Vereniging onder meer: "Het regelen van de eisen waaraan de kwaliteit van de dienstverlening moet voldoen". Slechts 25 bureaus zijn lid van de COSSO, maar dat zijn wel de grote; samen bestrijken zij ongeveer vijftig procent van de markt.
"Continuïteit", zo zegt COSSO-voorzitter drs. J.M. Albers (directeur van het bureau RAET), "continuïteit is de basis van de betrouwbaarheid van een bureau. Als de continuïteit van de dienstverlening niet is gewaarborgd, is niets gewaarborgd;"

Gezien de grote belangen is het uiterst noodzakelijk, dat de bedrijfstak van de service-/softwarebureaus volwassen wordt. Dat er geen regels komen, standaards, een erecode desnoods, kortom een kader waarbinnen de bureaus zich hebben te gedragen, willen zij niet openlijk aan de schandpaal gezet worden.
"Het begin is er", zegt drs. Albers. "Wij hebben in de COSSO gedragsregels geformuleerd en daar proberen wij ons aan te houden. Zonder sancties, dat wel, maar in overleg tussen ondernemingen die elkaar tegelijkertijd heel enthousiast beconcurreren. Maar het gezamenlijke belang van een goede image staat boven de onderlinge concurrentie."
De volgende stap waar COSSO nog aan werkt, is het invoeren van gezamenlijke leveringsvoorwaarden. Weliswaar kunnen voor elk automatiseringsprobleem diverse oplossingen worden gekozen, en moet elk bureau vrij zijn in die keuze, maar er zijn wel degelijk minimumeisen te formuleren, waaraan iedere oplossing altijd moet voldoen. Zo kunnen er eisen worden gesteld aan de documentatie van een nieuw project, aan de mate waarin standaards worden toegepast, aan de planning, aan de methodiek.

Men kan zich dan ook afvragen, of de betrouwbaarheidsbewaking wel kan en mag worden overgelaten aan een vereniging als de COSSO of aan de klanten van de bureaus zelf. Misschien dient er wel een soort inspectie te komen, die van geval tot geval beoordeelt of een bepaald bureau wel de beschikking mag krijgen over privacy-gevoelige of anderszins maatschappelijk kwetsbare gegevens. Dat gaat natuurlijk veel verder dan een controle op de continuïteit en de degelijkheid van de verwerking. Er staat hier meer op het spel dan alleen maar financiële verliezen. Per slot van rekening is er vorig jaar nog een directeur van een servicebureau het land uitgewezen op verdenking van spionage. En je moet er eigenlijk niet aan denken, wat een verkeerd-willend bureau met de ter beschikking staande gegevens en bestanden allemaal niet zou kunnen doen.
Het COSSO-bestuur is niet erg gecharmeerd van het idee van zo'n controle en inspectie van buiten. Niet onbegrijpelijk. Maar toch kan het niet anders zijn, dan dat de belangen van de bonafide bureaus in uiterste instantie parallel lopen met die van de klant en ook van de samenleving achter die klant.

Tot slot een aardige anekdote

Once upon a time a programmer was given the task of changing a master file update program. The change was simple enough, except that he found one open logic path which led to a quite impossible data condition for which nothing was specified.
Being a helpful kind of chap, he programmed in a flexo-writer message just to mention that the impossible had occurred, and thought no more of the matter.
A few days later the manager responsible came to the programmer's desk and in hushed tones recounted what had happened in the production run.
After eight hours and 169 pages of output the flexo-writer had broken and the machine was out of action for 24 hours awaiting replacement.
Yes, the data condition was impossible, but there had been mistakes in the data generation before the master file take-on.
No, the operators were not supposed to allow jobs to continue in this way for that sort of time, but there had been some argument recently over operations allegedly cutting off program runs in their prime of life.
Moral: Be prepared for all eventualities - particularly the worst ones.

(Computer Weekly, 13 oktober 1977)

LITERATUUROVERZICHT

door J. Philippo

In de A.C.-bibliotheek opgenomen boeken

AC 152 Financial Accounting Estimating through Statistical Sampling by Computers - M.S. Newman (227 pagina's, Engels)

De toepassing van Estimation (schattings) Sampling bij aanwezigheid van grote (computer)bestanden is een multidisciplinair probleem dat kennis vereist op het gebied van administreren, automatiseren en statistiek. Het boek beoogt deze gebieden te dekken door in te gaan op de volgende onderwerpen:

- Statistische schattings(waarden) steekproeven, waarin de toe te passen statistische techniek wordt beschreven in termen van te hanteren schattingswaarden, populaties, steekproefontwerp, -selectie en -evaluatie.
- Financiële schattingswaarden toegepast op activa en passiva, inkomsten en uitgaven, beleids- en beheersinformatie.
- Gebruik van de computer voor het uitvoeren van de steekproeven.

Duidelijk moet gesteld worden, dat het boek zich richt op Estimation Sampling, steekproeven gericht op het schatten van waarden, en niet op steekproeven ten behoeve van accountantscontrole, zoals men - in onze kringen - zou verwachten bij het lezen van het woord sampling.
Deze verwachting zou zelfs versterkt worden als men verneemt, dat de schrijver van dit stuk partner is bij Haskins & Sells en dat voor het nemen van de steekproeven het pakket Auditape de mogelijkheden biedt.
Als Appendix 1 is een casus opgenomen waarin getoond wordt hoe een statistische regressieschatting gemaakt kan worden; het voorbeeld berekent de waarde van een (fysieke) voorraad (zonder volledige telling) door verbanden te leggen tussen de fysieke deelopnamen en de boekwaarde. De grenzen van de strata worden via het computerprogramma zodanig vastgesteld, dat de verkregen schattingswaarde een juist beeld geeft voor de waarde. Het laatste is onder meer van belang bij afwijkingen tussen de boekwaarde (historisch) en current value (huidige kostprijs) bij LIFO-systemen. Een dergelijke methode van berekening is recent door de SEC goedgekeurd.
Het gebruik van de Auditape-routines "Estimation Sampling Design and Selection" en "Estimation Sample Evaluation" wordt in Appendix 2 beschreven.
Een lijst met definities, een bibliografie en een index besluiten dit goede boek, dat vooral voor de beginner in dit vak een goede handleiding zal blijken door de duidelijke, verklarende aanpak.

Noot van de redactie

In het volgend nummer van Compact zal aandacht besteed worden aan het pakket Auditape. Naast de bovengenoemde Estimate Sampling routines is aan de laatste versie van dit standaard auditpackage nog een saldobiljetten-routine toegevoegd. Daarboven zal de binnenkomst van de IBM 370/125 II op het KKC-computercentrum het gebruik binnenshuis mogelijk maken. Door voortdurende verbeteringen is dit pakket "still going strong".

AC 161 Corporate Fraud - M. Comer
(Engels, 387 painga's inclusief glossary, reading-list en index)

Michael Comer beschrijft hoe men kan vaststellen of bij bedrijven fraude wordt gepleegd, hoe men bij fraude verliezen kan beperken en in de toekomst kan voorkomen.
Over het algemeen wordt fraude, zo het wordt ontdekt, slechts bij toeval ontdekt. De schrijver beschouwt eerst de motivaties en commerciële achtergrond van fraude, waarbij het probleem, dikwijls gedefinieerd als een stil risico, belicht wordt.
Het vrijwel vormloze verschijnsel fraude classificeert hij in 17 basiscategorieën en geeft daarbij voorbeelden.
Analyse van de samenstellende delen van frauduleuze praktijken stelt de lezer in staat te leren waarop te letten en waar.
Technieken om de aandacht te richten op kritieke symptomen vormen de eerste stap op ontdekking. Voor het onderzoek, dat daarna komt, wordt een praktische leidraad gegeven.
Tot slot worden verdedigingssystemen beschreven en de wijze waarop deze in het bedrijfsbeleid kunnen worden geïntegreerd.
Dat aan het verschijnsel computer ruime aandacht wordt geschonken zal niemand verwonderen. De computer, vaak een hulpmiddel bij fraude, kan ook een machtige hulp zijn bij opsporing en voorkoming van fraude.

In de A.C.-bibliotheek zijn recent ook nog een aantal studieboeken opgenomen uit de NOVI-reeks, zoals:

AC 158/9 Basiskennis Wiskunde W1 (+ antwoordenboek) - F.S. Wijmans

AC 160 Operationele Research - A.M. ten Broeke e.a.