Klynveld Kraayenhof & Co.
Accountants

Automatisering en Controle-groep

COMPACT 832

Computer en Accountant

Uit de inhoud

Gebruik en controle van on-line applicaties
door J.L.H. Kooijman

Beheersing, beveiliging en controle van het IBM Systeem/38
door A.H.C. Koedijk

Current developments for future thinking
door R.H. Healey, Thorne Riddell
(De microcomputer in de accountantscontrole)

Nummer 31 10e jaargang Lente 1983

Internationaal KMG Klynveld Main Goerdeler

COMPUTER EN ACCOUNTANT

INHOUDSOPGAVE

NUMMER 31 10E JAARGANG LENTE 1983

compact

Lente 1983

VAN DE REDACTIE

Compact gaat zijn 10e levensjaar in.

Even tijd voor een terugblik of misschien beter:
een jaar voor de "finishing touch" als vakblad op het gebied van Automatisering en Controle.

Onze lezerskring is flink gegroeid niet alleen binnen Klynveld Kraayenhof & Co. Ook buiten de maatschap Klynveld Kraayenhof & Co. neemt de belangstelling steeds toe. Meer en meer wordt Compact het visitekaartje van de Automatisering en Controle-groep.

Wij zijn gepast terughoudend met het toezenden van Compact, maar indien u regelmatig Compact wilt ontvangen, zullen wij u gaarne op de verzendlijst plaatsen. Wij zijn eigenlijk van mening dat al onze cliënten in de gelegenheid gesteld moeten worden om kennis te nemen van Compact. Geef Compact ter inzage aan cliënten.

Twee hoofdartikelen deze keer:
- Gebruik en controle van on-line applicaties door J.L.H. Kooijman.
- Beheersing, beveiliging en controle van het IBM Systeem/38 door A.H.C. Koedijk.

De redactie is van mening dat het hier om zeer fundamentele artikelen gaat voor wat betreft de realisering van functiescheidingen in een organisatie. Er is dan ook veel tijd aan besteed om ze zo goed mogelijk leesbaar te maken voor de specifieke lezerskring van het periodiek. Dit is de belangrijkste reden waarom de door ons nagestreefde verschijningsdatum (uiterlijk 21 juni) werd overschreden.

Verder:
Nieuws op het gebied van de microcomputer in de accountantscontrole (H. Veenman), lezing R.H. Healey deel II alsmede ons commentaar op het buitengebeuren zoals dat in openbare geschriften tot ons komt.

Uw commentaar op ons blad stellen wij op hoge prijs.
Wij ruimen gaarne een plaats daarvoor in.

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

compact

Lente 1983

Het doel van deze uitgave is informatie te verstrekken over ontwikkelingen op het gebied van automatisering en controle in binnen- en buitenland. De vermelde artikelen worden daarom soms geheel, soms verkort opgenomen, tevens als regel voorzien van commentaar.

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

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

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

Indien u belangstelling heeft voor meerdere exemplaren kunt u deze aanvragen bij de secretaris van de redactie, evenwel zolang de voorraad strekt.

ACTUALITEITEN (1)

De sectie EDP-auditing van het Nederlands Genootschap voor Informatica

Doelstelling: De in december 1982 opgerichte Sektie EDP-Auditing heeft als doel: Het bevorderen van enerzijds het inzicht in de functie van EDP-Auditing, anderzijds van kennis van methoden, technieken en middelen die ondersteunend zijn voor de EDP-Audit-werkzaamheden. EDP-Auditing beoogt het vormen van een onafhankelijk en deskundig oordeel over de betrouwbaarheid, de doeltreffendheid en doelmatigheid van het ontwikkelen en gebruiken van geautomatiseerde informatiesystemen.

Werkterrein:
- Het instellen van studiecommissies voor de bestudering van vraagstukken op het gebied van EDP-audit;
- Het houden van voordrachten, symposia, conferenties, e.d.;
- Het verzamelen en publiceren van literatuur terzake van EDP-Auditing;
- Het samenwerken met daarvoor in aanmerking komende andere secties van het genootschap alsmede met derden die zich met het vakgebied EDP-Auditing bezighouden.

Op 11 mei 1983 heeft de sektie EDP-Auditing als eerste officiële activiteit naar buiten een seminar georganiseerd.
Het droeg de welluidende naam
"Kwaliteit van de Automatisering: EDP-Auditing in breed Perspectief".

De bijdragen van de conferentiesprekers waren als volgt:
EDP-Auditing
door mw. M. van Biene-Hershey

EDP-Auditors, wie zijn dat?
door F. Dankmeyer R.A.

EDP-Audit en topmanagement
door Ir. L.A.M. Mathijssen

Onderzoek naar efficiency van rijksautomatisering
door F.G. Kordes

Beheersing van nieuwe ontwikkelingen in de automatisering
door Ir. D.W. Okker

EDP-Auditing en accountantscontrole
door Prof.dr. A.B. Frielink R.A.

Protectie en programmeertalen; naar een verifieerbaar informatiesysteem
door Prof.dr. R.P. van de Riet

Betrouwbaarheidsaspecten bij telecommunicatie
door Ir. H.A. Nossbaum

EDP-Audit: Morgen is anders
door J.J.A. Leenaars R.A.

De teksten van de lezingen kunt u lezen in nr. 6 van de serie NGI-rapporten met de titel "EDP-AUDITING in breed perspectief" (AC446). In de bundel kunt u tevens een bloemlezing aantreffen uit de Nederlandse EDP-Audit-literatuur (1964 - heden).

ACTUALITEITEN (2)

Wereldwijd informatiesysteem voor havens moet vertragingen bij gevaarlijke ladingen voorkomen

Bron: Het Financieele Dagblad, vrijdag 10 juni 1983 pag. 14.

In Vancouver is het totaalplan voor bovengenoemd systeem gepresenteerd. Het is gebaseerd op de proef gedurende 1 jaar in 9 havens. Het betreft een allesomvattend systeem voor gestandaardiseerde en gecoördineerde informatie-uitwisseling. Doel: de kostenbesparing van vele miljoenen door het voorkómen van vertragingen.

Participanten zijn de havens onderling, reders, bevrachters, douane-autoriteiten, milieu-instanties en dergelijke.
De voordelen van een gezamenlijk netwerk komen echter pas goed uit de verf bij meer uitgebreide, betrouwbare en tijdige gegevens, gekoppeld aan de vereiste procedures in de diverse havens, zo werd in Vancouver tijdens de conferentie van de International Association of Ports and Harbours benadrukt. Daarom moet de verdere ontwikkeling van een definitief systeem ook worden gericht op het verbinden van havens met elkaar op een wereldwijde schaal. Het systeem moet zodanig worden ingericht dat ook kleine havens op betrekkelijk simpele wijze contact kunnen krijgen met de centrale databanken.

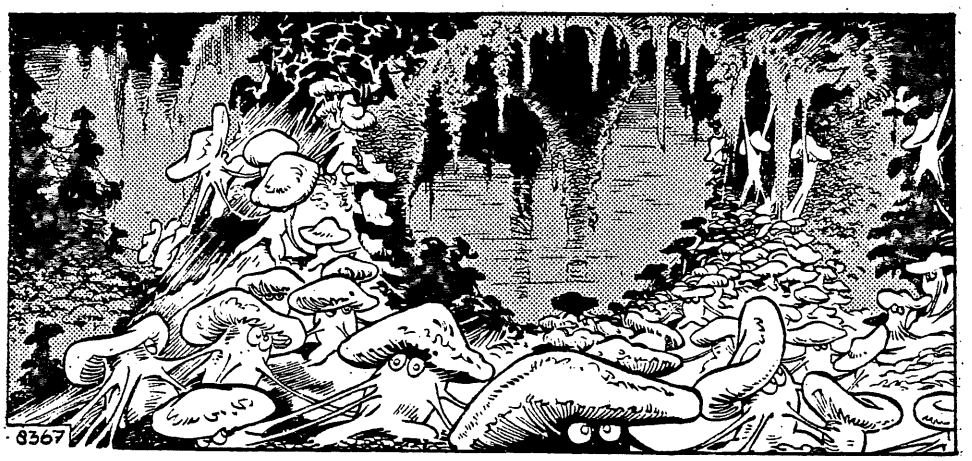
Onze zegsman vermelde dat de onderzoekingen in Rotterdam zijn gedaan door de Interfaculteit van Prof. dr. C. Brevoord R.A. Het initiatief is gesteund door de Europese Commissie in Brussel met ƒ 3.000.000 in het kader van de stimulering van de Europese elektronica-industrie. De 9 havens waaronder Rotterdam, hebben nog eens ƒ 4.000.000 in het proefsysteem geïnvesteerd in de vorm van mankracht en aanwezige know-how. Er werd daarbij gebruik gemaakt van een computersysteem van het Deense software- en systeembureau Datencentralen in Kopenhagen.

Wij hopen meer informatie te kunnen lezen bij de verdere voortgang van dit grote veelomvattend project.

Lente 1983

GEBRUIK EN CONTROLE VAN ON-LINE APPLICATIES

door J.L.H. Kooijman



8367 Onder de Zwarte Bergen bevindt zich de onderwereld. Daar wonen de Kwillen, een levensvorm die nog niet door geleerden ontdekt is en daarom wetenschappelijk niet bestaat.
Het is een rustig volkje, dat een zwijgend leven leidt in de eeuwige stilte van hun holen en gangen. Want een taal bezitten ze niet en die hebben ze ook niet nodig. Onderling zijn ze namelijk verbonden door draden waardoor ze communicatie hebben; op die manier weet de een wat de ander weet, en daardoor is er nooit ruzie.

Het perfecte datadistributiesysteem.

I - Inleiding

In dit artikel wordt een overzicht gegeven van facetten die bij beoordeling en controle van on-line applicaties een rol spelen. Het gaat daarbij met name om de invloed die een on-line applicatie kan hebben op de werkzaamheden van de accountant in het kader van de jaarrekeningcontrole.
De maatregelen van interne controle die bij on-line applicaties zoal van toepassing kunnen zijn worden besproken, waarna wordt aangegeven welke mogelijkheden de accountant ter beschikking staan om een oordeel te krijgen over bestaan en werking van die maatregelen.
Allereerst een aantal opmerkingen vooraf.

- Een belangrijke richtinggevende factor bij het onderzoek van on-line applicaties wordt gevormd door de betrokkenheid van de afdeling of afdelingen (of de organisatorische functie respectievelijk functies) die de gegevens uit de applicatie gebruikt voor het voeren van de administratie.
  De complexe technologie die voor de ontwikkeling en instandhouding van de on-line applicatie wordt ingezet kan vele gebruikers voor geweldige problemen plaatsen. Die technologie is daarmee van grote invloed op de mogelijkheden die de gebruiker ziet om mee te doen bij de ontwikkeling en het testen van de applicatie, alsmede op de wijze waarop de administratieve organisatie rondom deze applicatie zou moeten worden opgezet. Uit de opzet van die administratieve organisatie zal de accountant moeten afleiden welke greep de gebruiker heeft of denkt te hebben op zijn eigen informatieverwerkend systeem. De gebruikersbenadering is daarmee van groot belang voor de aanpak van de accountantscontrole.

- Een on-line applicatie staat niet op zichzelf.
  In het kielzog van de on-line applicatie vinden wij naast de techniek van de database-, teleprocessing- en operating systemen ook nog de automatiseringsomgeving voor het management van die (algemene) software en de omringende administratieve organisatie van de gebruiker te wiens behoeve de on-line applicatie is opgezet. Zonder deze omgeving kan de on-line applicatie niet functioneren. Of het nodig is deze omgeving dan ook maar te betrekken bij het onderzoek van de on-line applicatie staat daarmee echter geenszins vast.
  Wij zullen aan deze afweging, die vooral van invloed is op de omvang van het accountantsonderzoek, ruime aandacht besteden.

- Een ander facet, dat direct samenhangt met het voorgaande is de wijze waarop de aangeleverde gegevens door de on-line applicatie worden verwerkt (verwerkingskarakteristiek).
  De techniek biedt hier onbeperkte mogelijkheden. Er zijn on-line applicaties die bij nadere beschouwing alleen data-entry omvatten, terwijl ook systemen worden aangetroffen waarbij vanaf beeldschermen rechtstreekse mutatie plaatsvindt van actuele bestanden.

Deze twee uitersten en alle tussenliggende variaties brengen hun eigen specifieke risico's mee met betrekking tot betrouwbaarheid en beveiliging.
De verwerkingskarakteristiek bepaalt daardoor in hoge mate de diepgang van het onderzoek van een on-line applicatie.
In dit artikel zullen wij hoofdzakelijk de aandacht richten op de applicaties waarbij rechtstreekse mutatie van actuele bestanden plaatsvindt.

- In het voorgaande is de term on-line applicatie al veelvuldig gebruikt en wij zijn er daarbij vanuit gegaan dat aan de lezer voldoende duidelijk is wat wij daarmee bedoelen.
  Voor de goede orde volgt hier een nadere definitie van "onze" on-line applicatie die wij in dit artikel ten tonele voeren.
  Onze on-line applicatie betreft een informatieverwerkend systeem waarbij - via geautomatiseerde hulpsystemen - beeldschermen beschikbaar zijn gesteld aan eindgebruikers. Deze zijn daardoor in staat de geregistreerde gegevens rechtstreeks te benaderen en naar eigen goeddunken direct te muteren (on-line, real-time zo u wilt). Voorts is onze on-line applicatie in de onderneming van groot belang; de bedrijfsvoering is afgestemd op de snelle en betrouwbare gegevensverstrekking uit het systeem en bij de opstelling van de jaarrekening zijn de gegevens uit onze applicatie van grote invloed.

  Dit noodzaakt een nader onderzoek naar de betrouwbaarheid van de gegevensverwerking door deze applicatie, of - beter gesteld - naar het gehele complex van administratie en organisatie, inclusief interne controle, ten behoeve van een juiste, volledige, tijdige en geautoriseerde gegevensverwerking door onze applicatie.

Wat moet er nu worden onderzocht van dit complex, met welke diepgang, in welke volgorde en op welke wijze.

In het voorgaande hebben wij kort aangegeven welke factoren een rol zullen spelen (gebruiker, automatiseringsomgeving en technologie).
De kernproblemen die voorafgaande aan de start van het accountantsonderzoek (of de EDP-audit) dienen te worden aangepakt, zijn de volgende:

1. Aanpak van het onderzoek

In hoeverre kan en mag de accountant meegaan met de aanpak die de gebruiker zelf hanteert (systeemgericht of gegevensgericht), welke overwegingen spelen daarbij een rol en welke eigen actie van de accountant kan nodig en zinvol zijn.

2. Omvang van het onderzoek

Moet de automatiseringsomgeving (het décor waartegen de applicatie wordt uitgevoerd) ook worden onderzocht? En zo ja, met welke diepgang zal dat moeten gebeuren, wat moet worden meegenomen en wat niet.

3. Diepgang van het onderzoek

Welke invloed heeft de verwerkingskarakteristiek. Kan men wellicht met een onderzoek en toetsing van enige belangrijke steunpunten volstaan, of eist de technologie diepgaand en gespecialiseerd onderzoek op vele onderdelen.

Dit artikel beoogt ideeën te geven voor de benadering van deze kernproblemen en poogt richtinggevend te zijn voor de aanpak van de controle. Voorafgaand hieraan zullen wij nader ingaan op enkele specifieke punten ten aanzien van de on-line technologie zelf en de consequenties van deze technologie voor de structuur van de interne controle.

II - On-line applicaties

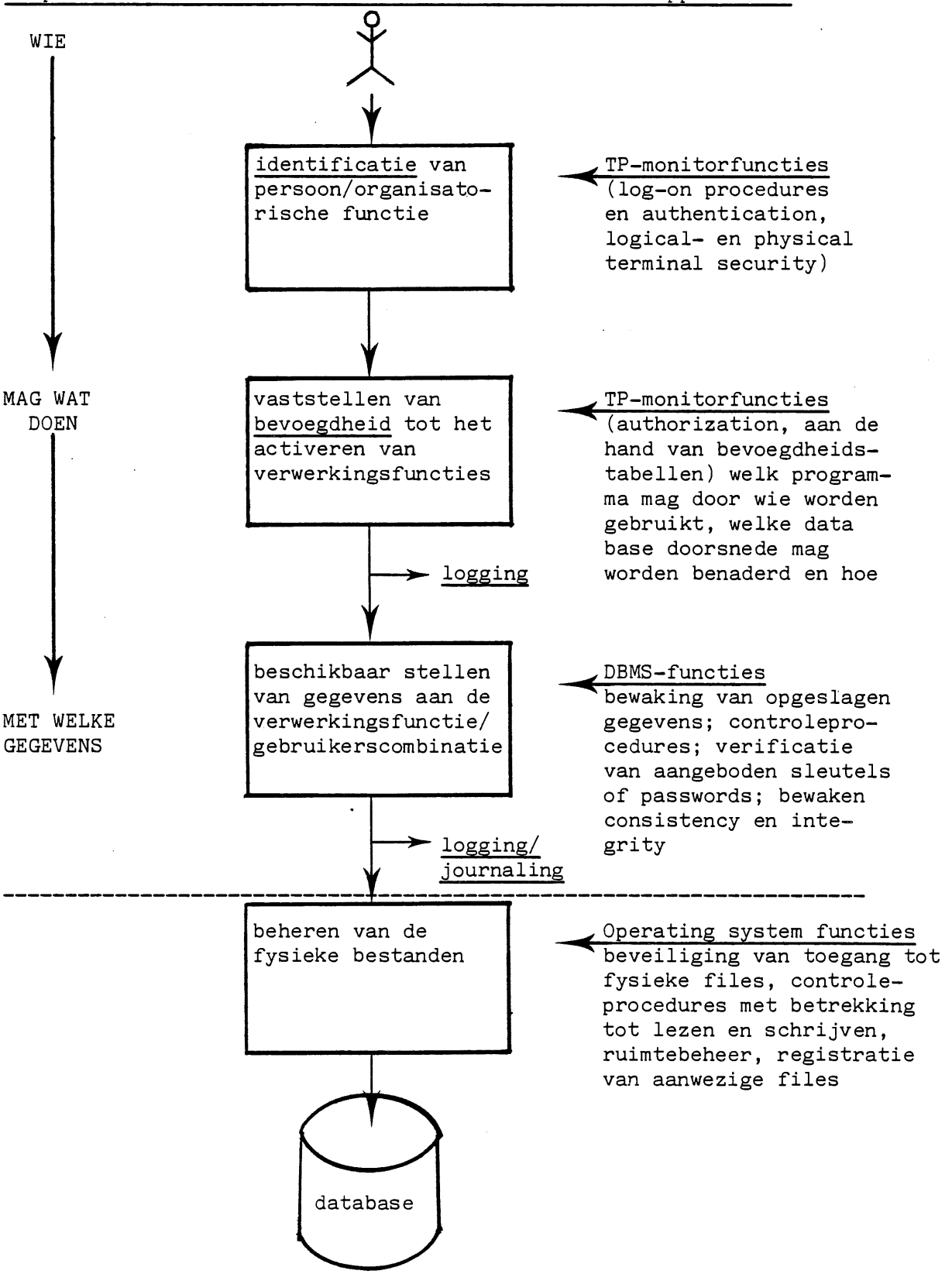
A. Technologie; algemeen

De voortschrijdende technologie heeft het mogelijk gemaakt, de automatisering veel dichter bij de gebruiker te brengen, met name door het installeren van invoer- en uitvoerfaciliteiten in de gebruikersafdelingen.
In vergelijking tot de traditionele batchomgeving heeft dit aanzienlijke verschuivingen veroorzaakt in het stelsel van interne controlemaatregelen.

De accountant staat hier voor het probleem dat bestaande controlemiddelen soms niet meer toepasbaar zijn of anders moeten worden gericht. Sommige steunpunten van interne controle zijn vervallen, ondergebracht in nieuwe organisatorische functies of vervangen door computerprogramma's.
Wij zullen nagaan welke de belangrijkste invloeden zijn van de on-line applicatie op het stelsel van interne controle.
Onze belangstelling richt zich daarbij op onze applicatie waarbij met behulp van database-management systemen en teleprocessing-monitoren, de gegevensinvoer en bestandsbewaking plaatsvindt en van directe bestandsmutatie sprake is.

De belangrijkste componenten van deze systematiek zijn in het hierna volgende schema met toelichting weergegeven.

Componenten en faciliteiten ten behoeve van on-line applicaties



Toelichting

Wie mag wat doen met welke gegevens

Interne controle ') wordt voornamelijk gerealiseerd door toepassing van functiescheiding, gevolgd door afstemming van de resultaten. Bij de controle van administratieve processen wordt dan ook altijd voor de belangrijkste activiteiten de functiescheiding nagegaan en beoordeeld. Het onderzoek naar de opzet en de betekenis van functiescheidingen is in de traditionele administratie niet al te ingewikkeld; door raadpleging van organisatieschema's en functiebeschrijvingen (taken, bevoegdheden) kan hierin een goed inzicht worden verkregen. Bestaan, handhaving en naleving van de functiescheidingen kunnen worden vastgesteld met behulp van een scala van controletechnieken.
Wanneer echter voor de gegevensverwerking gebruik wordt gemaakt van on-line systemen, wordt met name de toetsing van handhaving en naleving moeilijker. De accountant zal, met andere woorden, moeten vaststellen of het stelsel van functiescheidingen ook bestaat in het geautomatiseerde systeem en of het toezicht op de handhaving van dit stelsel naar behoren functioneert en gefunctioneerd heeft.
In de hiernaast opgenomen schets is aangegeven welke faciliteiten er ten behoeve van on-line applicaties aanwezig zijn om toezicht te kunnen uitoefenen op het gebruik van verwerkingsfuncties en het benaderen van gegevens. Deze faciliteiten zijn algemeen van aard en in standaardsoftware aanwezig (general controls). De verantwoordingsregistratie (logging, journaling, audit-trail) wordt door deze standaardsoftware geleverd. Deze verantwoordingsregistratie kan - aangezien per applicatie de gegevens ten behoeve van de functiescheiding aan de standaardsoftware worden gegeven - mede bruikbaar zijn voor de toetsing van de handhaving en naleving van deze functiescheidingen. De per applicatie aanwezige identificatie en autorisatietabellen zijn derhalve bruikbaar voor de vaststelling van het bestaan van de gewenste functiescheidingen voor de applicatie.

In de schets is tevens aangegeven, welke controlestations achtereenvolgens moeten worden "genomen" voordat een gebruiker gegevens kan benaderen. Wij hebben daarbij de vraag gesteld: wie mag wat doen met welke gegevens.

') Met "interne controle" bedoelen wij de in de administratieve en organisatorische procedures en functies ingebouwde waarborgen met betrekking tot autorisatie, volledigheid, juistheid en tijdigheid van informatie en met betrekking tot de beveiliging van bezittingen, alsmede het geheel van maatregelen dat getroffen wordt bij afwijkingen ten opzichte van gestelde regels of normen.

De accountant zal in het kader van zijn controle-arbeid ten aanzien van deze vraag de volgende nuancering aanbrengen:

1. Wie zou wat mogen doen met welke gegevens.
   Dit geeft de eigen beoordeling weer van de accountant, gegeven de omvang van de interne organisatie, het type toepassing en de daarbij aanwezige functies.

2. Wie mag wat doen met welke gegevens.
   Dit betreft de vaststelling dat de beoogde functiescheidingen ook in het geautomatiseerde systeem aanwezig zijn.

3. Wie heeft wat gedaan met welke gegevens.
   Hier is de vaststelling van de goede werking van het systeem aan de orde. Als het goed is, wordt dit door de gebruiker aan de hand van de applicatie-uitvoer gecontroleerd; aanvullende faciliteiten uit de standaardsoftware zijn logging, journaling en audit trails.

Alvorens nader in te gaan op de mogelijkheden voor het beoordelen en toetsen van de in de applicatie aanwezige functiescheidingen, zullen wij nagaan welke verschuivingen in het stelsel van interne controlemaatregelen worden veroorzaakt door de on-line technologie.

B. Invloed op de structuur van de interne controle; gevolgen voor de accountantscontrole

Als gevolg van de toegepaste technologie (databases, TP-monitoren) treden verschuivingen op in de vormgeving van de maatregelen van interne controle.
Deze verschuivingen en de invloed daarvan zijn als volgt samen te vatten:

1. De beheersing van de gegevensverwerking en de controle daarop wordt in toenemende mate overgenomen door standaardsoftware zoals DBMS en operating systems. Dit betekent een verschuiving van application controls naar general controls.
   De controle op de betrouwbaarheid en toepassing van deze standaardsystemen zal dienovereenkomstig moeten verschuiven.
   In zeer vele gevallen zal een application-audit niet meer kunnen worden uitgevoerd zonder dat ook ruime aandacht wordt besteed aan de standaardsoftware met behulp waarvan de on-line applicatie wordt uitgevoerd.

2. Autorisatiecontroles, waarin voorheen door organisatorische maatregelen en procedures werd voorzien, zijn nu grotendeels geautomatiseerd en ondergebracht in TP-monitor, DBMS, operating system, file control systems en library pakketten.

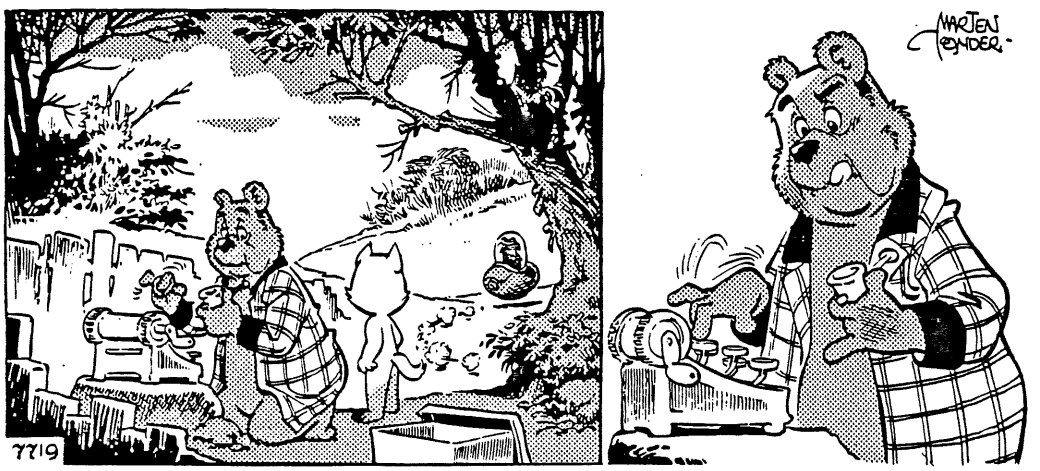
   Als voorbeeld moge dienen, het invoertraject dat bij de traditionele batchsystemen werd afgelegd langs verschillende rekencentrumafdelingen en met behulp van diverse opdrachtformulieren. Een dergelijk traject leent zich bij uitstek voor lijncontroles en proceduretests.

   De zojuist genoemde software wordt veelal slechts door één óf enkele personen beheerd en de registratie van de werking is meestal technisch gericht.
   Bij de uitvoering van het accountantsonderzoek levert dit punt vaak de grootste problemen op. De vastleggingen (logging, journaling en audit trails) zijn meestal niet erg "accountantsvriendelijk" en de vaststelling van de volledigheid van deze vastleggingen is geen geringe opgave.

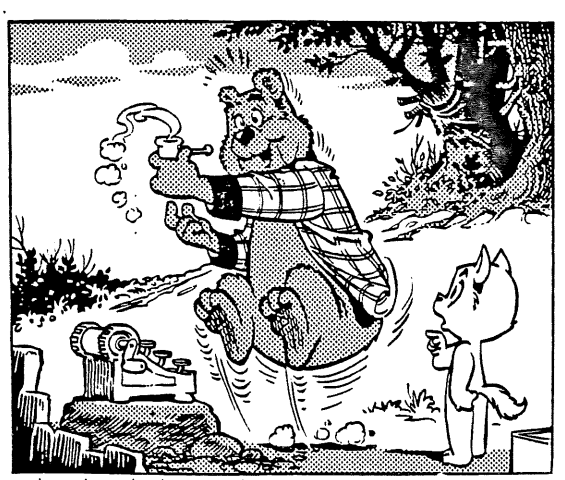
3. Een belangrijke steun voor de accountant in de traditionele batchomgeving was de aanwezigheid van aparte bestanden per applicatie en het feit dat de batchprogramma's waren gericht op de uitvoering van een afgeronde verwerkingsfunctie (een bepaald administratief proces).
   Het gebruik van het bestand en de bijbehorende programma's kon derhalve door, en voor de verantwoordelijke gebruiker/eigenaar worden gevolgd, getest, geadministreerd, etc.
   In on-line applicaties waarbij een database wordt gebruikt, is het mogelijk om gegevens aan meerdere gebruikers ter beschikking te stellen (data-sharing). De programma's zijn nu gericht op het uitvoeren van enkelvoudige opdrachten (stapjes in het administratief proces) teneinde aanvaardbare responsetijden te verkrijgen. Meestal worden ook de programma's voor gemeenschappelijk gebruik opgezet (program-sharing).
   De data-sharing en program-sharing kan het stelsel van functiescheidingen ernstig bedreigen, als hiervoor in de systemen geen toereikende bewakingsmechanismen zijn opgezet.
   Daarbij is de gegevensverwerking een continu proces geworden. Waren er bij de batchsystemen heldere meetpunten (de "batch", zie ook 2); in het on-line systeem worden verwerkingsopdrachten onmiddellijk gehonoreerd.
   In deze nieuwe omgeving zullen dan ook nieuwe technieken moeten worden toegepast om het bestaan en de werking van de functiescheidingen na te kunnen gaan.

III - De voorbereiding op het onderzoek

Een van de kernpunten voor de uitvoering van het onderzoek betreft de vraag naar de aanpak.
In het voorgaande hebben wij dat verbonden met de manier waarop de gebruiker omgaat met het geautomatiseerde systeem en op welke wijze hij vaststelt dat het doet wat het moet doen. Ter illustratie hiervan zien wij hieronder zo'n gebruiker.



„Een transmieter," sprak hij tot zichzelf. „Nooit van gehoord. Het lijkt me het beste, dat ik eens ga proberen hoe zo'n ding werkt. Wat heb ik in de gauwigheid nodig?"
Dat was een moeilijke vraag voor een heer, die eigenlijk alles al heeft. Maar toen zijn blik op zijn lege pijp viel klaarde zijn peinzend gelaat op, en hij begon te tikken.
„Waar komt die schrijfmachine vandaan?" vroeg Tom Poes.
„Stoor me niet," mompelde heer Ollie, voorzichtig op de toetsen drukkend. „Ik bestudeer deze bestelling. En dat is héél moeilijk omdat er zo weinig letters op staan. Even kijken. Juist, ja, zo kan het... Tabak in mijn pijp wordt: tapac in myn pyp. Heel duidelijk."



Met deze woorden draaide hij aan het krukje, en hij maakte een verheugde uitroep toen er plotseling een rookspiraaltje uit zijn pijpekop steeg.
„Het is gelukt," zei Tom Poes verbaasd. „Een vreemd toestel, hoor. U had hem toch niet besteld? Dat zei u zelf daarnet.
„Zeur niet!" riep Heer Bommel opgetogen. „Hij is van mij, al was de adressering een beetje fout met die nul achter mijn naam. Maar hij is aan het juiste adres afgeleverd; dat zal je met me eens zijn, jonge vriend!"

Gebruikers van on-line systemen; omgaan met geavanceerde techniek of:
Hoe Een Gebruiker Iets Groots Accepteert Op Grond Van Een Kleinigheid.

A. Gebruikers

Afgezien van de acceptatieprocedure, waarvan het van belang is na te gaan op welke wijze de gebruiker de verantwoordelijkheid voor het informatiesysteem heeft overgenomen van de ontwerpers, zal de accountant moeten onderzoeken hoe de gebruiker vaststelt dat de gegevens die uit het systeem komen, correct zijn en welke maatregelen de gebruiker in gang zet als de computer - door welke oorzaak dan ook - zou uitvallen. Dit initiële onderzoek is van groot belang voor het verdere verloop van de accountantscontrole. Wij zullen daarom even stilstaan bij de problemen die de gebruiker ontmoet wanneer hij zijn (geautomatiseerde) administratie onder controle wenst te houden.

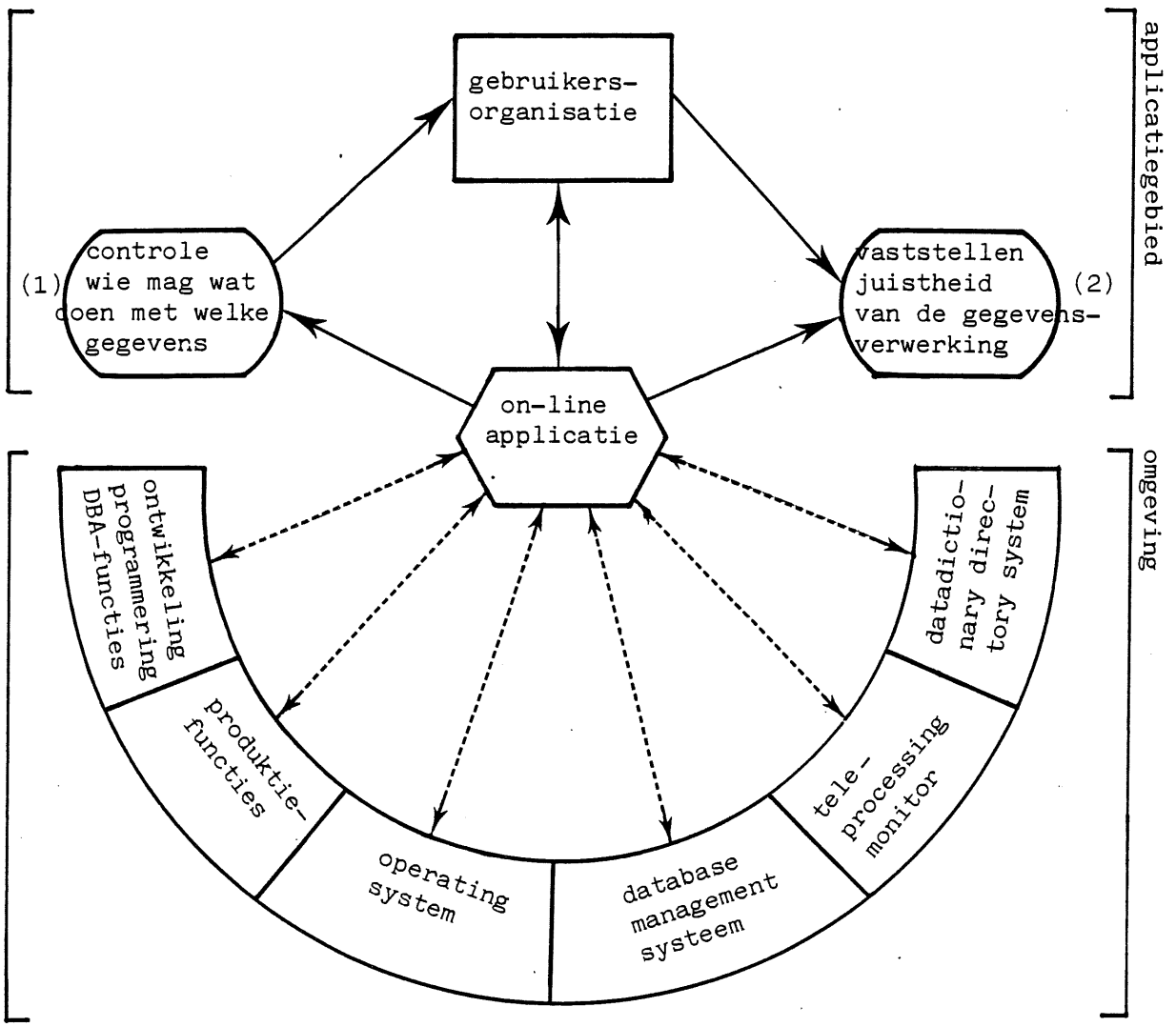
- De vertrouwde "masterbestanden" zijn ondergebracht in een grote database waarvan hij niet meer het exclusieve gebruiksrecht heeft.

- Het stapeltje ponsconcepten, de ponskaarten en het mutatiebestand (de "batch") is verdwenen en de route van deze batch door afdelingen en systemen valt als steunpunt weg.
  Het volgen van een enkele transactie door het systeem, vanaf beeldscherm tot in database en op overzichten is voor een gebruiker veel moeilijker.

- Het batchprogramma dat als afgerond geheel van verwerkingstaken gericht kon worden getest, uitgeprint of in blokschema's zichtbaar kon worden gemaakt, is nu vervangen door vele kleine TP-programma's die tijdens een beeldschermconversatie door de TP-monitor worden opgeroepen en verbonden om na de uitvoering van de transactie weer te verdwijnen in een "programmapool".

- De rubriekscontroles, validaties en opmaakroutines die vroeger door het batchprogramma werden uitgevoerd zijn nu ondergebracht in de standaardsoftware van het DBMS.
  Welke controles nu precies voor een bepaalde gebruiker aanwezig zijn, valt moeilijker na te gaan en vereist een goede rapportage van hen die het DBMS beheren.

Een minder geïnteresseerde gebruiker is dan ook geen ongewoon verschijnsel. Wij moeten daarbij tevens bedenken dat de betrouwbaarheid van de gegevensverwerking door een on-line applicatie niet meer van één enkele gebruiker afhankelijk is. Wanneer in een kring van gebruikersafdelingen er één is, waar met controle en beveiliging minder gewetensvol wordt omgegaan, zal dit van grote invloed zijn op de betrouwbaarheid van de informatie die in het totale systeem is opgeslagen en het kan tevens leiden tot een ernstige verzwakking van het toegangsbeveiligingssysteem.



B. Onderzoekgebied.

Een en ander impliceert dat de greep die een afzonderlijke gebruikersafdeling heeft op de betrouwbaarheid van zijn eigen applicatie, in principe geringer is dan die in de traditionele batchomgeving.
Dit houdt ook in - en dat is van groot belang voor de aanpak van de EDP-audit - dat de controle van de afzonderlijke applicatie (de application-audit) van minder betekenis is geworden voor de beoordeling van betrouwbaarheid en continuïteit van de gegevensverwerking ten behoeve van de betrokken gebruiker.
De applicatie als zodanig speelt voor deze facetten daarbij een te geringe rol.

B. Onderzoekgebied

Wij menen dat met betrekking tot de afzonderlijke applicatie er voor het accountantsonderzoek nog maar twee facetten van belang kunnen zijn, te weten:

1. De voor die bepaalde applicatie aanwezige verwerkingsbevoegdheden.

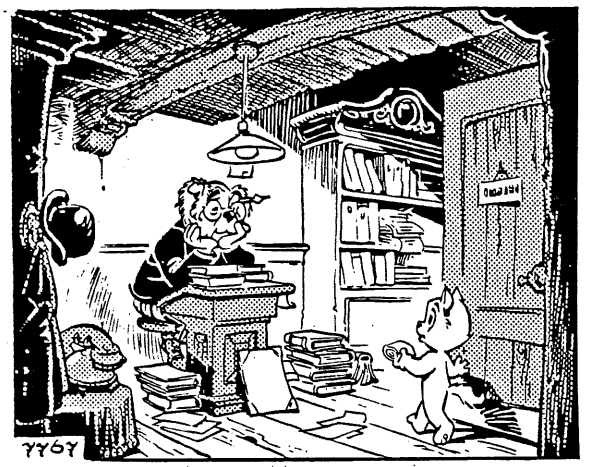
2. Controle op de verwerking zelf wanneer geen goede relatie aanwezig is tussen invoer en uitvoer.

Ten behoeve van de beeldvorming vatten wij het onderzoeksgebied hiernaast samen in twee blokken: het applicatiegebied en de omgeving die zorgt dat de applicatie kan functioneren.

C. Aanpak van het onderzoek, audit-strategy

We kennen de gegevensgerichte en systeemgerichte controle-aanpak.
Veel schrijvers adviseren een systeemgerichte aanpak wanneer sprake is van geavanceerde automatisering en een gegevensgerichte aanpak bij kleine geïsoleerde (mini/microcomputers) omgeving. Veelal wordt daarbij het keuzeprobleem voor de ene of andere richting versoepeld door het advies, met een mengvorm van beide benaderingen te werken.
In dit artikel zal dit laatste, de mengvorm, eveneens aan de orde komen.
Daarom staat centraal de benadering van de gebruiker van het systeem, waarbij moet worden nagegaan of die benadering adequaat is gegeven de systeemtypologie.
Wanneer die benadering toereikend is zal de accountant die in het algemeen moeten volgen, tenzij dit zou leiden tot grote ondoelmatigheden óf onnodig hoge controlekosten.

In grote lijnen zal de vaststelling van de wijze van aanpak, uitvoering en diepgang als volgt verlopen.



7767. De heer Dorknoper bevond zich in grote moeilijkheden. Het uitzoeken van de fouten, die door de stadsrekenmachine gemaakt waren, zou tweeduizend beambten gedurende twintig jaren van werk kunnen voorzien. En hoewel de ambtenaar eerste klasse heel wat aankon, begreep hij toch, dat hij hier voor een onmogelijke taak stond.

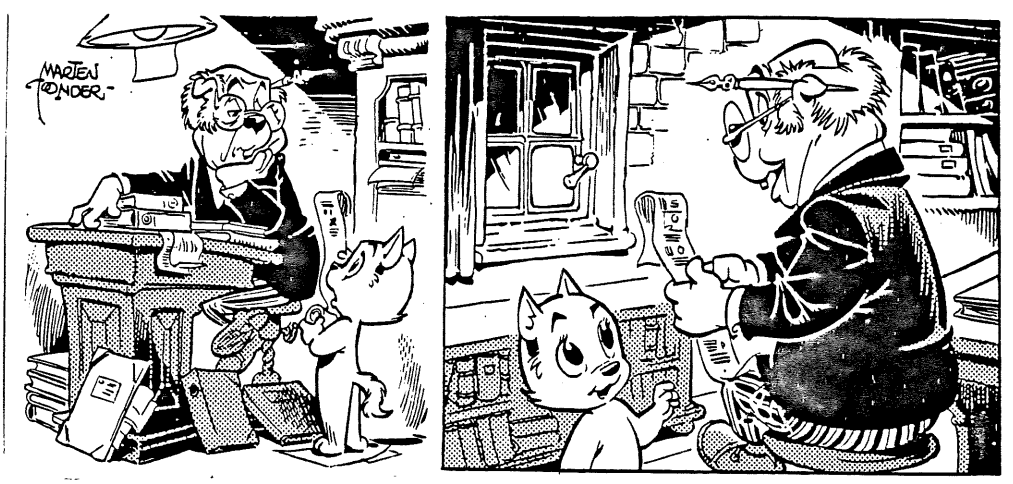
„Als ik nu maar wist, waar de fout begonnen is," zei hij somber tot zichzelf. „Toen we de heer Bommel verdachten, konden we in de OBB-lijn zoeken. Maar die vertoont geen afwijkingen, zegt referendaris Kreut."

Hij zuchtte diep en wendde zich tot Tom Poes, die met een rolletje papier binnen was gekomen.

„Ik heb geen tijd," sprak hij knorrig. „U gelieve zich aan de officieel vastgestelde spreekuren te houden. Goede dag."

„Hier staat alles op," zei Tom Poes. „Alles wat de transmieter gedaan heeft. Maar het is gedrukt in een soort onleesbare code."

Zo sprekende overhandigde hij de dropslip aan de heer Dorknoper, en deze wierp



er een onthutste blik op.

„Onleesbare code?" herhaalde hij. „Dat is voor ons geen bezwaar. We kunnen gewoon de computer inschakelen, die de ambtelijke taal ontwerpt. Maar hoe komt u aan deze lijst, meneer Poes? Is het mogelijk dat de heer Bommel er toch iets mee te maken heeft?"

„Iets," gaf Tom Poes toe. „Maar buiten zijn schuld, dat zult u wel merken wanneer u dit ontcijfert, denk ik. Het was allemaal een vergissing."

De hooggeplaatste klerk begreep weinig van deze uitleg, maar hoe langer hij naar de papierstrook keek, hoe meer hij opklaarde.

„Dit is het!" verklaarde hij stralend. „Nu komen we er wel uit."

Logging

Vaak gebruikersonvriendelijk maar van grote waarde voor achteraf-controles, uitzoeken en herstellen van fouten.

1. Onderzoek gericht op de desbetreffende on-line applicatie

- Op welke wijze en met welke middelen stelt de gebruiker de juistheid en volledigheid van de gegevensverwerking vast (algemeen accountant).
- In welk totaalverband functioneert de betreffende applicatie; is er sprake van program- en data-sharing; zijn er verbanden met andere applicaties (EDP-auditor).

2. Vaststellen gebruikersaanpak (algemeen accountant en EDP-auditor)

- De gebruiker steunt volledig op eigen stelsels van interne controle; invoertellingen (hash- en batchtotals) worden vooraf gemaakt, aansluiting van alle uitvoer en interfaces met de eigen "schaduw"administratie vindt plaats ..... of:
- De gebruiker steunt volledig op de maatregelen van interne controle in het geautomatiseerde systeem en de automatiseringsomgeving. De invoerstroom wordt achteraf niet integraal afgestemd met de brondocumenten.

3. Beoordelen gebruikersaanpak (algemeen accountant en EDP-auditor)

In deze stap wordt nagegaan, of de accountant in principe mee kan gaan met de gebruikersbenadering.
Het controlebelang staat hier voorop. Een enkel voorbeeld ter verduidelijking van de voorwaarden die daarbij gelden:

. De accountant moet achteraf kunnen nagaan of de controles ook in werkelijkheid hebben plaatsgevonden; het ontbreken van audit-trails, journaling- of logging-gegevens blokkeert de mogelijkheden om achteraf na te gaan of een belangrijke, zogenaamde "onvervangbare" controle naar behoren heeft gewerkt.
. In een omgeving waarbij gemeenschappelijk gegevensgebruik (data-sharing) aan de orde is, zullen alle gebruikers in beginsel eenzelfde controlebenadering moeten hanteren om te voorkomen dat de situatie ontstaat van de ketting met de zwakke schakel erin.

Deze stap is een belangrijke en kan zelfs leiden tot onmiddellijke advisering

- aan alle gebruikers (via een gebruikersbeheersgroep of een data-administrator) en
- aan de automatiseringsafdelingen, alsmede

voor beide groepen betrekking hebbend op richtlijnen voor de inrichting van de administratieve organisatie respectievelijk de voorwaarden waaraan ingebouwde controles en uitvoeroverzichten zouden moeten voldoen.

D. Een gegevensgerichte gebruikersbenadering

Behalve het verband met de overige gebruikersbenaderingen in een "shared" omgeving is hier de aard van de applicatie zelf van belang. Wanneer bijvoorbeeld niet-financiële gegevens worden ingevoerd en door het systeem worden omgezet in financiële gegevens (bijvoorbeeld premieberekeningen) dan is de juiste werking van het programma waarin de rekenregels worden uitgevoerd, niet in de greep van deze gebruiker. Die zal immers met behulp van zijn registraties alleen de volledigheid van de verwerking van de kwantitatieve gegevens (aan de hand van aantallen records invoer/uitvoer) kunnen vaststellen.
Voor programma's die salarissen, rente of actuariële gegevens berekenen geldt hetzelfde.
In deze gevallen zal de gebruiker over aanvullende middelen moeten beschikken om de juistheid van deze gegevensconversie te kunnen vaststellen.
De accountant zal moeten aandringen op de ingebruikname van deze middelen of (wanneer zij in gebruik zijn) de toereikendheid en betrouwbaarheid daarvan moeten nagaan.
Het werk voor de EDP-auditor in deze omgeving kan beperkt blijven. Wanneer vastgesteld kan worden, dat deze gebruikersbenadering geen risico's oplevert voor de andere applicaties en gebruikers, zal kunnen worden volstaan met enkele deel-onderzoeken van geringe omvang. Deze betreffen de gegevensuitwisseling met andere applicaties (de interfaces) en de checks die de overige applicaties op de uit deze toepassing opgeleverde gegevens uitvoeren, alsmede de procedures van bestandsbewaking van de voor deze gebruiker aanwezige gegevensverzamelingen.

Een basis voor de uitvoering van lijncontroles en proceduretests met betrekking tot de gebruikerscontroles door de algemeen accountant ligt hiermee binnen bereik. Ook de toepassing van audit-programmatuur ten behoeve van steekproeven, bestandsonderzoek en herhaalde verwerking is mogelijk.

E. Een systeemgerichte gebruikersbenadering

Een belangrijke stap is hier het onderzoek naar de toereikendheid van de middelen die de gebruiker voor deze benadering ter beschikking heeft en de steunpunten in de interne controle die daarmee worden getoetst.
Een voorbeeld:
In het systeem bevinden zich tabellen waarin bevoegdheden van personen c.q. organisatorische functies zijn vastgelegd. De handhaving van het stelsel van functiescheidingen staat of valt met de juistheid van deze tabel, het goede gebruik ervan door het systeem en de procedures en controles met betrekking tot beheer en mutatie van de tabelgegevens.
De bewaring en registratie van de tabelgegevens is doorgaans gedelegeerd (welke gebruiker heeft dit bewust gedelegeerd?) aan de automatiseringsafdeling. De mutatiebevoegdheid blijft uiteraard bij de gebruiker.
Het is duidelijk, dat aan een gebruiker, die ten behoeve van de handhaving van de door hem gewenste functiescheidingen, gaat steunen op de administratieve organisatie en interne controle in de automatiseringsafdeling, op behoorlijke wijze hierover verantwoording moet worden afgelegd.

De EDP-auditor zal moeten beoordelen of van een goede verantwoordingsrapportage sprake is en moeten nagaan op welke wijze de rapportage tot stand komt, c.q. welke functiescheidingen daarbij bestaan.

Het onderzoek naar de toereikendheid van de middelen die de systeemgerichte gebruiker hanteert, zal veelal een omvangrijke EDP-audit met zich brengen.

Deze EDP-audit is in onze visie primair gericht op het onderzoek naar de maatregelen die aanwezig zijn ter handhaving van de functiescheidingen zoals die door de gebruikers binnen de on-line applicatie worden gewenst.
Vanuit dit centrale onderzoek (transactie-analyse), zuiver gericht op de desbetreffende on-line applicatie, wordt bepaald welke onderdelen van de automatiseringsomgeving ("general controls") voor nader onderzoek in aanmerking komen. De aanpak van het onderzoek staat nu in grote lijnen vast; omvang en diepgang zullen worden bepaald nadat de transactie-analyse is voltooid.

IV - De uitvoering van het onderzoek

A. Transactie-analyse

De transactie-analyse wordt uitgevoerd in een systeemgerichte controleaanpak. Het onderzoek is erop gericht gegevens te verzamelen aangaande functiescheidingen zoals die in de applicatie aanwezig zijn of voor de applicatie in stand moeten worden gehouden.
Het doel is verband te leggen tussen de gebruikersbevoegdheden en de bevoegdheden die in de on-line applicatie zijn vastgelegd.

De onderzoekmethode is op de volgende uitgangspunten gebaseerd:
1. Gegevens in een database kunnen uitsluitend worden benaderd door middel van speciaal daarvoor geschreven programma's (transactieprogramma's of TP-programma's).
2. De transactieprogramma's kunnen alleen met behulp van beeldschermcommando's worden gestart door daartoe bevoegde gebruikers.

(Uiteraard zijn hierop uitzonderingen; een technicus kan via speciale commands de database rechtstreeks benaderen en de operator zal - ook in on-line systemen - nu en dan wel eens een batchprogramma starten hetwelk meestal niet aan de TP-monitor controles wordt onderworpen.)

Transactieprogramma's en beeldschermfaciliteiten vormen derhalve de kern van het onderzoek. Voor elke on-line applicatie moet zijn geregistreerd welke transactieprogramma's door wie kunnen worden gebruikt. Door van deze registratie uit te gaan, kan worden vastgesteld, hoe de functiescheiding van de gebruikersorganisatie in de bijbehorende on-line applicatie is verankerd.
De procedure hiervoor is als volgt.

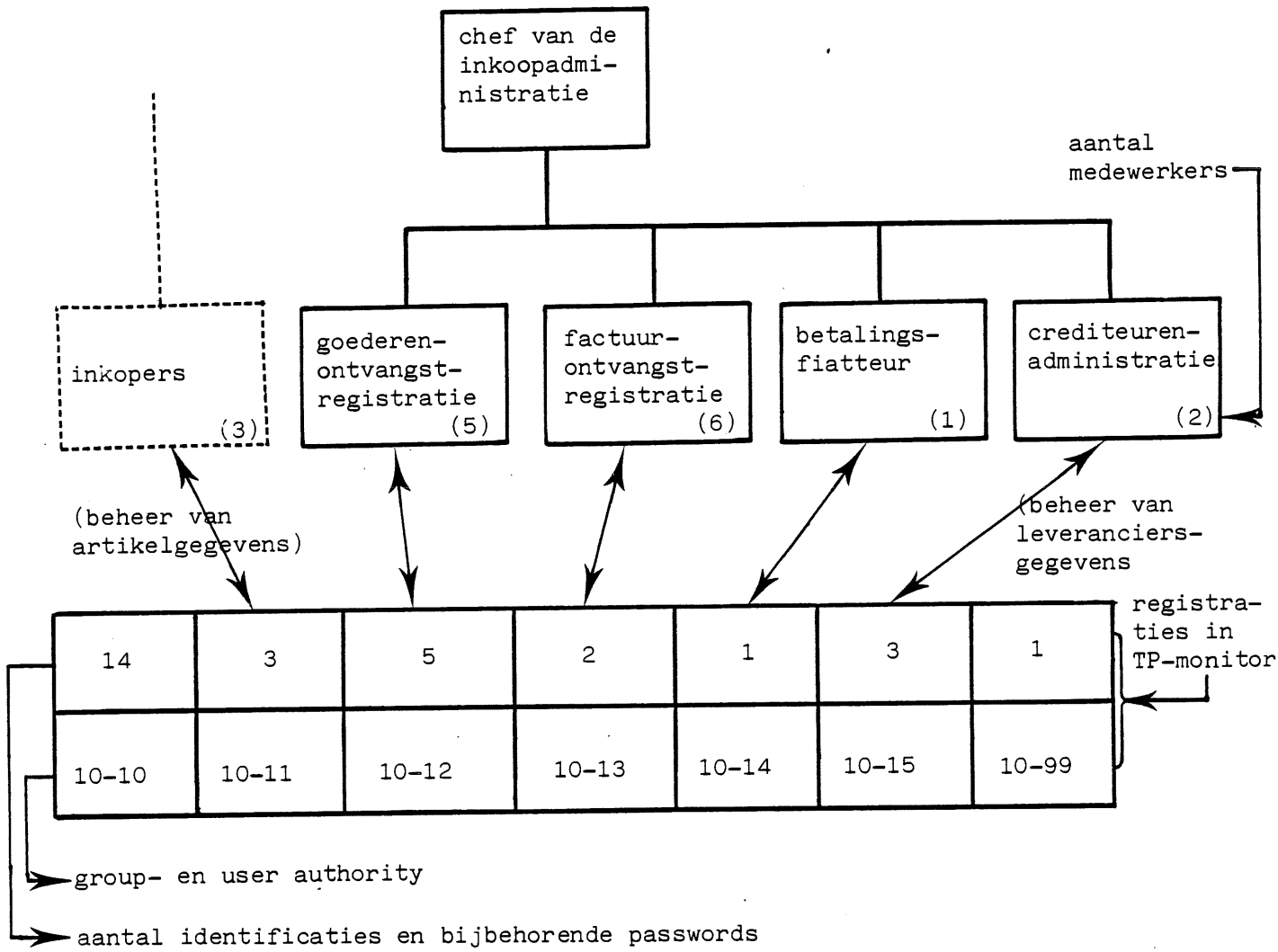
. Welke gebruikers.

1. De eerste stap is het onderzoeken van de organisatorische opbouw van de gebruikersafdeling en het vastleggen van de daarin aanwezige functiescheidingen, c.q. relevante functies.
   Parallel hiermee loopt de beoordeling van de aanwezige administratieve organisatie en de daarin aanwezige maatregelen van interne controle.
   Hierdoor kan al een indruk worden verkregen met betrekking tot de risico's van functievermenging die vanuit die organisatie zelf, al aanwezig zijn (omvang, structuur, sfeer, leiding, etc.).

2. Nu volgt de vastlegging van de aan die afdeling c.q. gebruikers verstrekte beeldschermfaciliteiten (TP-Monitor).
   Hierbij gaat het erom, vast te leggen welke gebruikers in het systeem zijn geregistreerd en over welke bevoegdheden elke gebruiker beschikt.
   Doorgaans zijn de bevoegdheden in een aantal niveaus of klassen aangegeven.

Een eerste beoordeling van de verzamelde informatie kan al in dit stadium worden uitgevoerd. Er kan bijvoorbeeld nagegaan worden of de bevoegdheidsverdeling zoals die blijkt uit zogenaamde user- classes of authority-codes aansluit met de afdelingsopbouw. In een voorbeeld hebben wij de eerste twee stappen nader uitgewerkt (figuur 1).

Figuur 1. Voorbeeld afdelingsopbouw versus systeembevoegdheden.



De aldus opgezette registratie geeft al een eerste indruk van het verband tussen bevoegdheden die met betrekking tot de desbetreffende online applicatie zijn vastgelegd in de TP-monitor en de eigenaar/gebruiker (user-groep 10).
Bevindingen:

- Zo zijn er aparte bevoegdheidsklassen in het systeem aanwezig die aansluiten op de organisatorische functies van de afdelingen (maar voor welke afdelingen of personen zijn de klassen 10-10 en 10-99 aanwezig?).
- De password-toepassing lijkt hier en daar niet helemaal in orde; bij de factuurontvangstregistratie worden twee passwords door 6 medewerkers gedeeld en bij de crediteurenadministratie is één password te veel aanwezig (van een ex-medewerker?).
- Overigens is er in de opzet van de gebruikersorganisatie zelf de primaire functiescheiding tussen de goederen en geldbeweging niet aanwezig.

. Welke verwerkingsmogelijkheden.

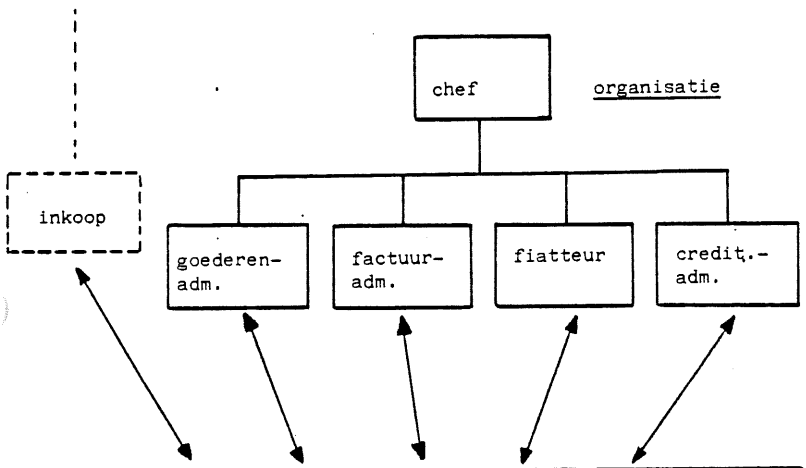
Een belangrijke volgende stap is nu de vraag wat men met deze bevoegdheden kan doen in het systeem.
Stappen 1 en 2 laten ons als het ware de inhoud van de sleutelkast zien, nu moet worden nagegaan welke deuren met de sleutels kunnen worden geopend.

Stap 3. In deze stap moet worden vastgelegd welke bevoegdheid nodig is voor het uitvoeren van een bepaald transactieprogramma.
Dit is doorgaans vastgelegd in de TP-monitor zelf of bij elk transactieprogramma afzonderlijk.
Stel dat na uitgebreid onderzoek van de bibliotheek met geautoriseerde programma's de volgende transactieprogramma's worden gevonden.

Progr. nr.	Benodigde authority	Omschrijving
01	10-10	Algemeen inquiry
02	10-11	Muteren artikelgegevens algemeen
03	10-11/13/14	Muteren artikelprijzen
04	10-13/14	Factuurgegevens wijzigen
05	10-14	Facturen fiatteren
06	10-15	Muteren leveranciersgegevens
07	10-12	Goederenontvangst vastleggen
	etc.	etc.

Door toevoeging van deze gegevens aan ons voorbeeld en het leggen van de verbindingen tussen de terminals en de programma's, ontstaat informatie waar we wat aan hebben:
"wie kan wat doen" (zie figuur 2).

Figuur 2. Transactieprogramma's.



14	3	5	2	1	3	1
10-10	10-11	10-12	10-13	10-14	10-15	10-99
X						X
	X					X
	X		X	X		X
			X	X		X
				X		X
					X	X
		X				X

Beschikbare verwerkingsfuncties

Benodigde authority	Programma-omschrijving	Progr. nr.
10-10	Algemeen inquiry	01
10-11	Muteren artikelgegevens alg.	02
10-11/13/14	Muteren artikelprijzen	03
10-13/14	Factuurgegevens wijzigen	04
10-14	Facturen fiatteren	05
10-15	Muteren leveranciersgegevens	06
10-12	Goederenontvangst vastleggen	07
	Etc.	-

In de praktijk zal deze kruisjeslijst aanzienlijk groter zijn en hopelijk ook wat minder eigenaardigheden bevatten.
Hoewel we nog niet precies weten welke gegevens in de database kunnen worden gemuteerd, kunnen toch al uit de programma-aanduidingen en de kruisjeslijst enige voorlopige conclusies worden getrokken.
Zo kan iemand die factuurgegevens behoort vast te leggen, blijkbaar ook artikelprijzen wijzigen. Met die artikelprijzen is toch het een en ander aan de hand, want niet minder dan drie afdelingsfuncties kunnen hierin muteren. Op het eerste gezicht lijkt dit niet wenselijk, etc. etc.

Elke kolom geeft voorts een volledig beeld van de taken die aan een bepaalde functie of functionaris blijkbaar zijn toegewezen; zo heeft de betalingsfiatteur veel meer mogelijkheden dan men op het eerste gezicht zou denken. Raadpleging van de functiebeschrijving lijkt hier nodig.

. Welke gegevens.

Welke gegevens kan men nu benaderen en wat kan met de gegevens worden gedaan.

In stap 4 moet worden vastgelegd wat elk transactieprogramma in de database kan uitrichten.
Dit lijkt een omvangrijk karwei, doch de ontwerpers van het DBMS hebben in de meeste gevallen verbindingsmechanismen gemaakt waarvan we in het onderzoek gebruik kunnen maken.

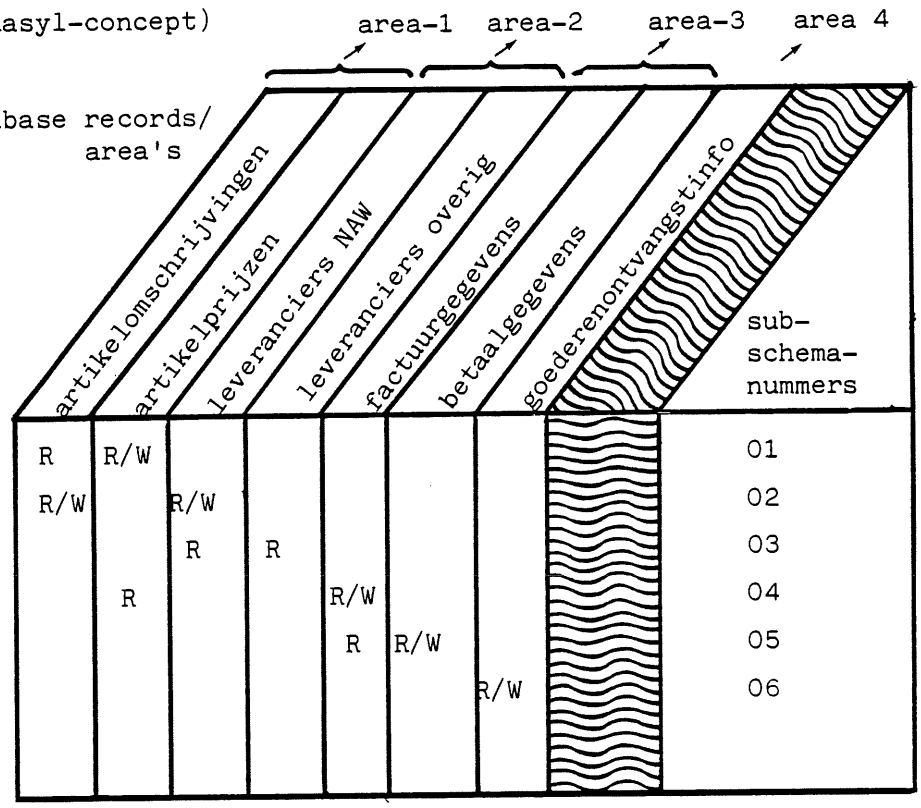
In een DBMS bestaan faciliteiten waardoor deelverzamelingen kunnen worden gemaakt uit de aanwezige gegevens. Zo'n deelverzameling wordt bijvoorbeeld subschema genoemd.
In een subschema kan nauwkeurig worden beschreven welke gegevens daarmee kunnen worden bereikt en welke manipulaties (lezen, schrijven, update, etc.) mogen worden uitgevoerd.
Een programma kan uitsluitend met de database communiceren via een subschema.
Wanneer wij dus weten welke subschema's er zijn en welke programma's van een subschema gebruik maken, weten we ook wat elk programma met de gegevens kan doen.

Net als bij de terminalfaciliteiten kan hier worden gesproken van sleutels die toegang geven tot opgeslagen database-gegevens.
Het subschemanummer is de sleutel, het verbindingselement tussen programma en database.

Een voorbeeld van een mogelijke indeling van een database is hierna opgenomen. De mate van detaillering kan van geval tot geval verschillend zijn. Dit hangt af van de vraag welke gegevens in het kader van het onderzoek van belang zijn.

Voorbeeld database onderverdeling

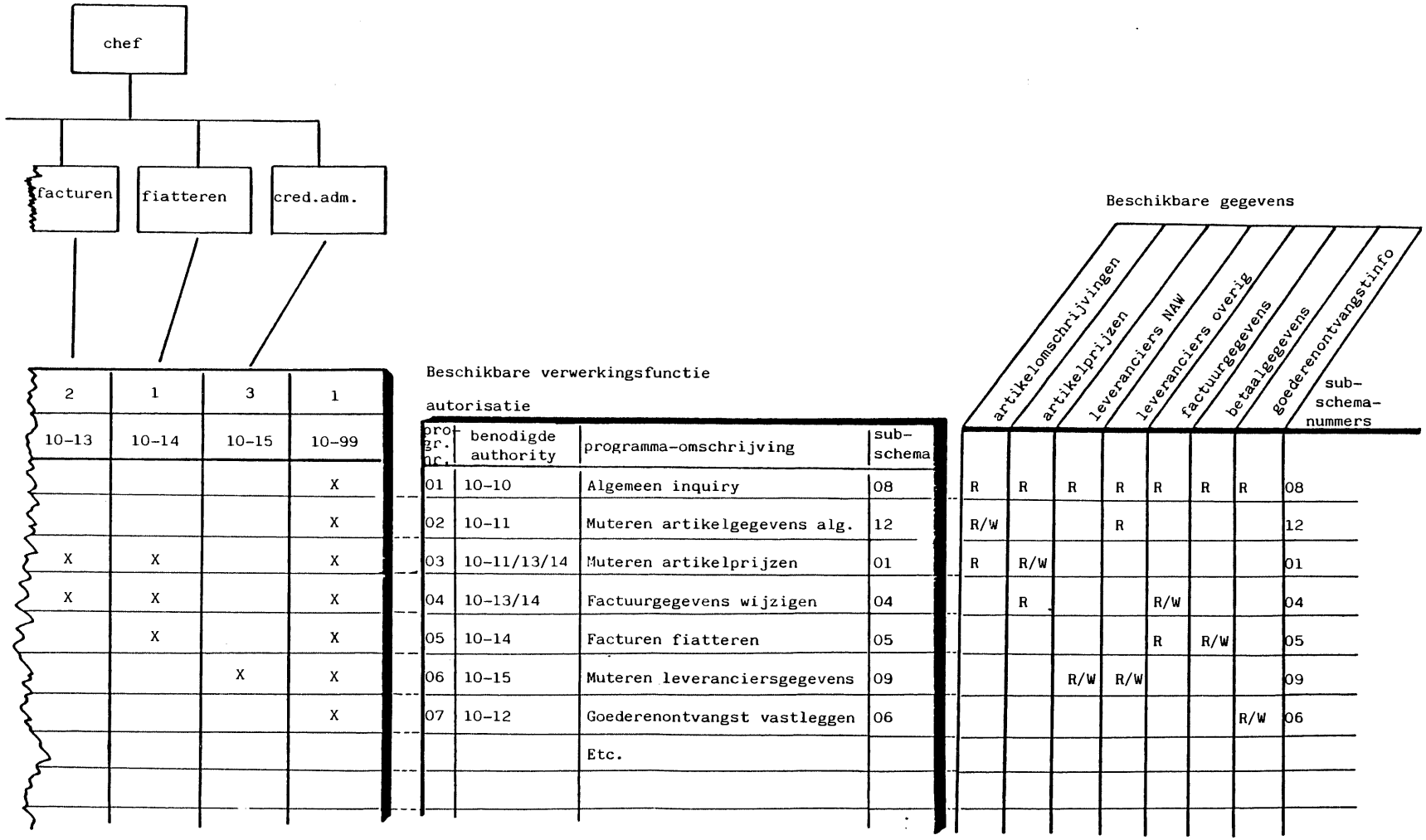
(codasyl-concept)



R = READ, W = WRITE

In dit geval is aangegeven hoe de recordonderverdeling van de database eruit ziet, welke records kunnen worden bereikt door de aanwezige subschema's en welke verwerkingsopties via die subschema's kunnen worden uitgevoerd.
Bij kritische deelverzamelingen (bijvoorbeeld financiële gegevens die door meerdere toepassingen worden gebruikt) kunnen in een gedetailleerder onderverdeling van het record de belangrijkste gegevenselementen worden opgenomen.

Inpassing in het overzicht van de betreffende applicatie geeft het volgende beeld (zie figuur 3).



Figuur 3. Overzicht bevoegdheden (authority profile).

Van de te onderzoeken applicatie is nu voldoende materiaal verzameld en gerangschikt om een oordeel over de ingebouwde functiescheidingen te kunnen vormen.
Een nadere analyse van de hiernaast gegeven informatie laten wij gaarne aan de lezer over.

B. Informatiebronnen

Waar komt de informatie voor het samenstellen van het overzicht vandaan.

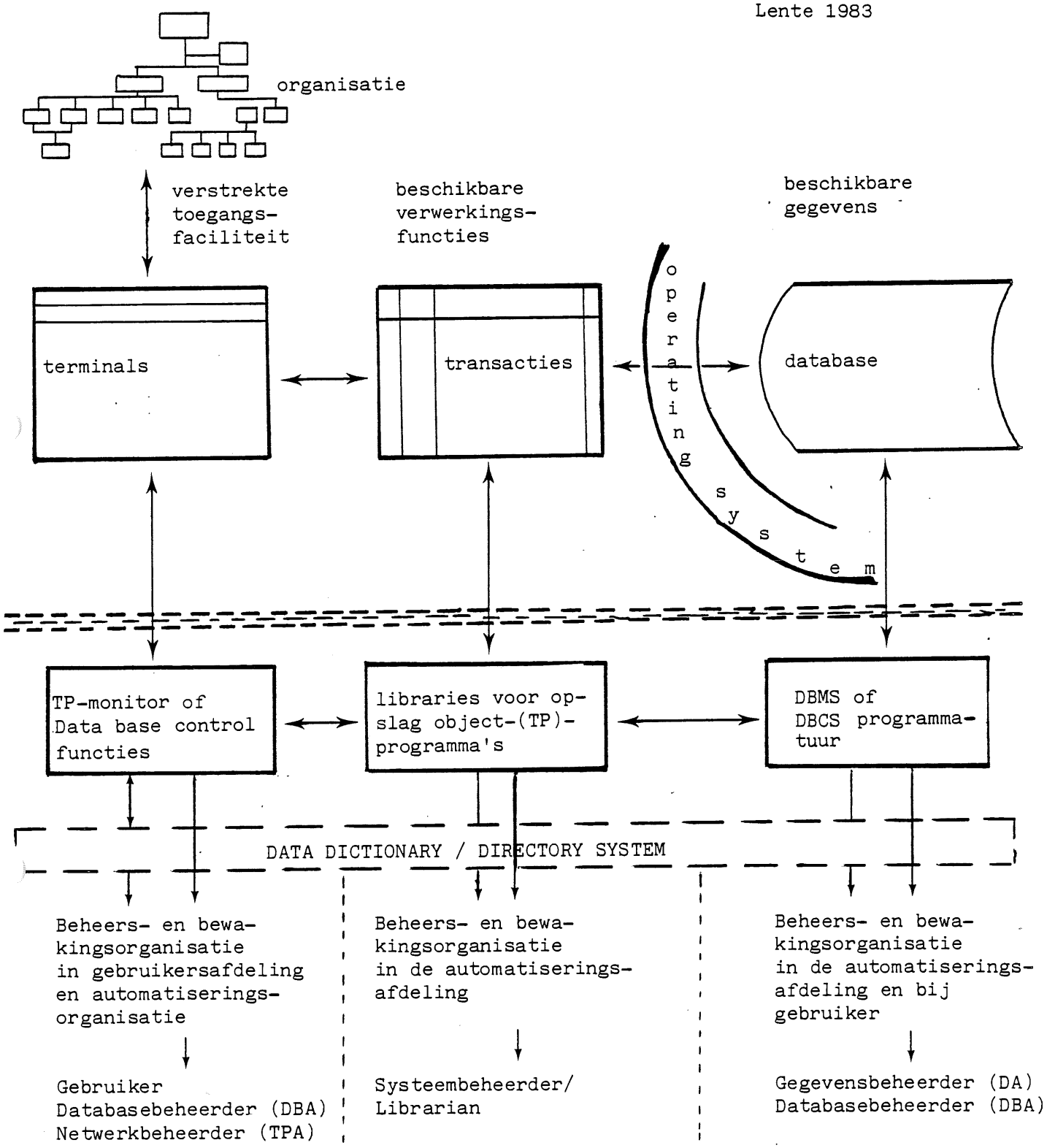
- Idealiter uit de systeemdocumentatie die bij de betreffende applicatie behoort. Deze documentatie geeft het zuiverste beeld van de opzet van de maatregelen van interne controle. Het is bovendien een gebruikersboek, waardoor de gebruiker zelf kan nagaan of een en ander volgens zijn aanwijzingen is opgezet. Wanneer bovendien een goede procedure voor wijzigingen van dit zogenaamde "authority profile" bestaat zal de accountant aan de hand van de wijzigingsformulieren, parafen, etc. kunnen nagaan of de bedoelde maatregelen van interne controle bestaan c.q. de procedures worden nageleefd. Helaas vinden we zelden een dergelijk gestructureerde omgeving, die het mogelijk maakt om met een geringe hoeveelheid arbeid het werkelijk in de computer aanwezige authority profile te toetsen aan de hand van de gebruikersdocumentatie.
- Soms is een datadictionary/directory systeem in gebruik waaruit de benodigde informatie kan worden verkregen.
  Ook hier gaat het om de vraag hoe sterk dit DD/DS verbonden is met de eindgebruiker van de applicatie enerzijds en met het actuele produktiesysteem anderzijds.
  Door bestudering van organisatie en procedures met betrekking tot het beheer van het DD/DS en de verantwoording die ten aanzien van dat beheer aan gebruikers wordt afgelegd, kan een indruk worden verkregen van de controle die een afzonderlijke gebruiker kan uitoefenen op "zijn" authority profile zoals dat in het actuele produktiesysteem op een zeker moment aanwezig is. Ook hier kan de accountant de inhoud van het DD/DS (de bedoeling) toetsen met het actuele produktiesysteem (de werkelijkheid).
  Een vervelend verschijnsel in de huidige DD/DS-en is dat zij doorgaans niet ingericht zijn om ermee te controleren. De hoeveelheid output (cross listings, authority listings, programma- en subschemaoverzichten) die wordt verstrekt op grond van de vraag: wie mag wat met gegeven-X is veelal te overstelpend voor een snel, eenvoudig antwoord.
- Tenslotte is er de mogelijkheid dat de informatie slechts kan worden verkregen na raadpleging van tabellen van de TP-monitor en de generatie-overzichten van het DBMS.
  Die informatie moet dan worden afgestemd met de gebruiker om te zien of de automatiseringsafdeling heeft gehandeld conform de aanwijzingen van de gebruiker.

Dit is een omslachtige procedure en veelal is de informatie moeilijk leesbaar en slecht gestructureerd.
Ook de communicatie tussen automatiseringsafdeling en gebruiker zal in dit geval waarschijnlijk gebrekkig zijn.
De accountant zal zich moeten realiseren, dat hij hier in feite bezig is de "ist" situatie van een bepaald moment (namelijk van het tijdstip waarop de TP-monitor en het DBMS op de computer zijn geladen) te beoordelen.
Het is daarbij noodzakelijk, dat hij beschikt over de "soll"-positie zowel die van de gebruiker als die, welke hij zelf heeft opgesteld.

C. General controls

Al eerder merkten wij op dat de tot nu toe uitgevoerde activiteiten waren gericht op het verkrijgen van gegevens over de functiescheidingen met betrekking tot een bepaalde on-line applicatie voor de beoordeling van de opzet daarvan.

Uiteraard geeft de procedure en het verzamelen van gegevens al een indruk over de wijze waarop de gebruiker bij het automatiseringsgebeuren is betrokken, hoeveel controle hij kan of heeft kunnen uitoefenen op de activiteiten van de automatiseringsafdeling en hoe er in de automatiseringsafdeling wordt gewerkt.
Niettemin zal, om een gefundeerd oordeel te krijgen over het bestaan en de werking van de "general controls" verdergaand onderzoek nodig zijn.
In het volgende overzicht hebben wij de on-line applicatie geplaatst in zijn natuurlijke omgeving (zie figuur 4).



Figuur 4: De on-line applicatie in zijn natuurlijke omgeving.

Wij hebben in het overzicht de belangrijkste punten in de general controls aangegeven.
Voor wat betreft de automatiseringsorganisatie en de daarbij aanwezige functies en techniek valt uiteraard veel meer op te sommen dan waartoe wij ons hier beperkt hebben, doch voor die aspecten zullen inmiddels voldoende controlemiddelen en technieken bij de lezer bekend zijn.

Met welke diepgang het onderzoek van de general controls moet worden verricht, zal van geval tot geval verschillen.
Ook hier moet onderscheid worden aangebracht tussen een beoordelings- en een toetsingsfase.
Zoals al eerder opgemerkt is, zal in de procedure van het verzamelen en vastleggen van materiaal over de applicatie al een indruk ontstaan van de invloed die uitgaat van de general controls. Met behulp van checklists voor automatiseringsorganisaties kan deze indruk nader worden getoetst.
Het oordeel over de opzet en de werking van de general controls is tenslotte bepalend voor de frequentie waarmee controles ter plaatse zullen worden uitgevoerd (bijvoorbeeld vergelijkingen van in de computer aanwezige authority profiles, actuele programma's, subschema's e.d. aan de hand van de documentatie).

V Afronding

Er zijn nog vele andere facetten die samenhangen met gebruik en controle van on-line applicaties. Wij hebben deze aspecten bewust weggelaten omdat het artikel dan nog langer zou worden dan nu al het geval is. Voor de geïnteresseerde lezer geven wij een korte opsomming van de belangrijkste aspecten met een korte toelichting.

- Testen.
  Hoe test de gebruiker de on-line applicatie; kan een accountant er nog een testset op nahouden, die hem toereikende informatie geeft?
  - Gebruikerstesten zouden in "batch-mode" moeten worden uitgevoerd om een goede vastlegging te krijgen van hetgeen getest is en hoe.
  - De testset van de accountant is niet meer bruikbaar. Het mooiste zou zijn, wanneer er een retrievalpakket zou worden meegeleverd door de makers van het DBMS waaruit eenzelfde overzicht kan worden gehaald, als wij in dit artikel hebben opgebouwd. Dit pakket zou dan informatie moeten krijgen uit het "live-system".
- Rechtstreekse ingangen.
  Niet elke databasebenadering loopt via het bewakingssysteem dat voor "normale" gebruikers is opgezet. Database-administrator, operators, systeemprogrammeurs kunnen in noodgevallen (reparatie databasestructuren) rechtstreeks gebruikersdata benaderen.
  Procedures voor gebruik van deze commands moeten aanwezig zijn, evenals toezicht en verantwoording achteraf.
- Batchprogramma's.
  Bedacht moet worden, dat een batchprogramma niet via de TP-monitor/ gebruikersbeeldschermen wordt gestart. De passwords voor onder andere het openen van de database moeten niettemin worden opgenomen. In het ergste geval zijn deze passwords in het batchprogramma opgenomen waardoor iedereen die de programmasource te pakken kan krijgen, kan beschikken over passwords van database, subschema's, etc.

- Menu-security.
  We hebben het niet gehad over een belangrijk additioneel middel om gebruikers beperkingen op te leggen met betrekking tot het starten van verwerkingsfuncties, namelijk het gebruik van beeldschermmenu's.
  Door een goede opzet van de menu's wordt een gebruiker gedwongen een bepaald (verwerkings-)pad te volgen dat speciaal voor hem is gemaakt. Een pad komt beschikbaar wanneer een bijbehorende gebruikersidentificatie en password bekend wordt gemaakt aan het systeem. Helaas beschikken vele systemen daarbij ook over mogelijkheden om uit het menu te "springen".
  Op de menu-security kan zodoende niet altijd onvoorwaardelijk worden vertrouwd; gebruikers die à la carte wensen te werken (al dan niet met toestemming) dienen ook in dat geval met voldoende beveiligingsmaatregelen te worden geconfronteerd.

Samenvatting

In grote trekken is in dit artikel het verschijnsel on-line systemen belicht vanuit de behoefte hiervoor een adequate controlebenadering te vinden. Voor deze benadering hebben wij - na enige beschouwende paragrafen over techniek en algemene controleproblematiek - gekozen voor een stapsgewijze beschrijving van de belangrijkste werkzaamheden die zullen moeten worden uitgevoerd.
De aanpak van de accountantscontrole dient daarbij zoveel mogelijk te worden afgestemd op de gebruikersbenadering. Uiteraard niet zo vanzelfsprekend als dat hier wordt samengevat; een beoordeling van die gebruikersaanpak met het oog op verwerkingsaard en de belangen van collega-database gebruikers is noodzakelijk.
Uitgaande van een systeemgerichte gebruikersbenadering onderzochten wij via transactie-analyse de aanwezige functiescheiding in de on-line applicatie. De ervaringen uit dit onderzoek en de wijze waarop de gebruiker vanuit de automatiseringsomgeving wordt geïnformeerd bepalen de omvang en de diepgang van het onderzoek naar bestaan en werking van de "general controls".

Dit artikel zal mogelijk nog een aantal vragen van praktische aard oproepen. In onze cursus "Accountantscontrole bij Geïntegreerde Gegevensverwerking" (GGV) worden de verschillende facetten meer diepgaand behandeld. In de rubriek Onderwijs in dit blad staat aangegeven hoe u onze brochure kunt aanvragen.

(Met toestemming van Marten Toonder Studio's hebben wij uit twee stripverhalen overdrukken in dit artikel opgenomen.
De 1e strip komt uit "De Weetmuts", een schitterend relaas over de lijdensweg van een Heer die alles weet.
De 2e en 3e strip zijn overgenomen uit "De Transmieter", een verhaal waarin Bommel een zeer bijzondere terminal in bezit krijgt en in zijn goedheid daarmee de computersystemen van de gemeente Rommeldam onbedoeld ontregelt.)

Lente 1983

Beheersing, beveiliging en controle van het IBM Systeem/38

door A.H.C. Koedijk

(Dit artikel is gebaseerd op de presentaties die door de schrijver zijn gegeven op de 13th Conference on Computer Audit, Control and Security, Chicago, 9-13 mei 1983.)

1. Introductie

De architectuur van het IBM Systeem/38 biedt nieuwe mogelijkheden op het gebied van beheersing, beveiliging en controle. Voorwaarde is evenwel, dat betrokkenen een goed begrip hebben van de wijze waarop parallelen kunnen worden getrokken tussen algemene beheersbaarheidsconcepten en de bijzondere S/38-filosofie.

Na een korte beschrijving van de beheersbaarheidsconcepten in hoofdstuk 2, worden in de hoofdstukken 3, 4 en 5 de architectuur en de beheersings- en beveiligingsstructuur van de S/38 behandeld. In hoofdstuk 6 worden vervolgens de parallelen getrokken tussen de automatiserings- en bedrijfsfuncties en de technische S/38 computeromgeving; dit wordt gedaan door middel van een stapsgewijze beschrijving van de wijze waarop de beheersbare conceptuele organisatie ook in de computer kan worden geëffectueerd. In hoofdstuk 7 worden tenslotte de controlemogelijkheden belicht; eerst een stapsgewijze beschrijving van een (door geautomatiseerde procedures ondersteund) onderzoek naar de wijze waarop van de mogelijkheden van de S/38 gebruik wordt gemaakt, vervolgens de S/38 bij het werken met "conventionele" controleprogrammatuur.

2. Conceptuele bedrijfsorganisatie: een raamwerk voor beheersing en controle

Introductie

In het algemeen is in een S/38-omgeving sprake van een door verschillende gebruikers gemeenschappelijk benutte computer. Bovendien zal er een toenemend gemeenschappelijk gebruik zijn van de in databases opgeslagen gegevens.
Het ligt voor de hand dat in een dergelijke situatie enige problemen met betrekking tot de beheersbaarheid ontstaan.
Wanneer een computersysteem moet worden beoordeeld op de mogelijkheden terzake van beheersbaarheid, is er behoefte aan een raamwerk in de vorm van een modelorganisatie, zodat afstand kan worden genomen van in de praktijk aanwezige verschillen.
In dit hoofdstuk wordt een dergelijk raamwerk besproken.

Conceptuele bedrijfsorganisatie

Het gebruik van een computer voor de gegevensverwerking van een organisatie leidt tot een behoefte aan specifieke kennis en ervaring. Deze kennis en ervaring zijn relatief schaars. Teneinde optimaal profijt te kunnen trekken, zullen deze kennis en ervaring worden geconcentreerd in afzonderlijke functies. De samenwerking tussen de klassieke bedrijfsfuncties en deze verbijzonderde automatiseringsfuncties wordt gekenmerkt door delegatie.

Sterk gesimplificeerd is er in principe samenwerking tussen de bedrijfsfuncties en de automatiseringsfuncties Systeemontwikkeling (met name Programmering) en Verwerking. Er worden programma's geschreven, gecontroleerd en geaccepteerd volgens geldende procedures. Geautomatiseerde systemen worden, na ontwikkeling door Programmering, aan de bedrijfsfunctie beschikbaar gesteld ter acceptatie. Na acceptatie gaat het systeem over naar Verwerking voor bewaring en uitvoering.

In de situatie waarin bedrijfsfuncties identieke gegevens gebruiken, zal (ondersteund door database-technieken) een tweede vorm van samenwerking ontstaan: de verschillende bedrijfsfuncties zullen gezamenlijk gebruik gaan maken van dezelfde fysieke gegevens. Hieruit vloeit een beheersingsvraagstuk voort, namelijk de toekenning van verantwoordelijkheden ten aanzien van de volledigheid, juistheid en actualiteit van deze gegevens. Beheersing en coördinatie moeten worden uitgeoefend door een afzonderlijke functie: Gegevensbeheer (data administration) (III)*). Om deze functie goed te kunnen uitoefenen heeft Gegevensbeheer in het algemeen behoefte aan een hulpmiddel voor de registratie van gegevens (naam, definitie, eigenschappen) over gegevens en van gegevens over het gebruik van gegevens (wie heeft welke bevoegdheden met betrekking tot welke gegevens en wanneer); dit hulpmiddel staat bekend als data dictionary. De beheersbaarheid kan worden verbeterd, als Gegevensbeheer programmeurs kan dwingen tot het gebruik van bestanden die volgens algemeen geldende definities zijn gecreëerd.

De scheiding tussen de verschillende functies kan slechts bijdragen tot beheersing van het gegevensgebruik indien het computergebruik voor elke functie kan worden beperkt tot een groep bepaalde, nauw omschreven programma- en gegevenssoorten.
Zo een door een bepaalde functie te gebruiken groep programma- en gegevenssoorten wordt aangeduid als domein of omgeving.
Er is behoefte aan verschillende omgevingen voor:
1. Bedrijfsfuncties met operationele toepassingssystemen.
2. Programmering met toepassingen in ontwikkeling.
3. Verwerking.
4. Gegevensbeheer.

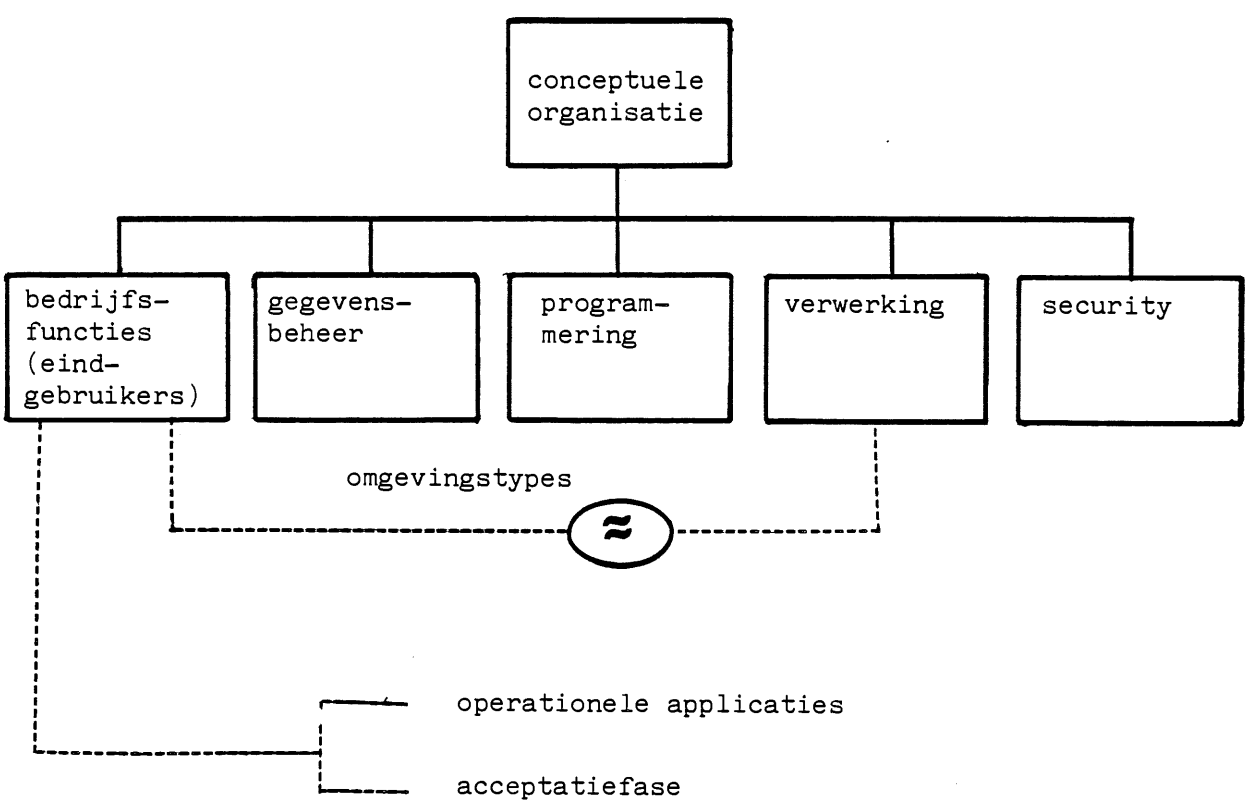
In een situatie met een hoge graad van interactieve computerprocessen, hetgeen in de situatie met een S/38 veelal het geval zal zijn, valt de Verwerkingsfunctie goeddeels weg. De bedrijfsfuncties zullen de produktie-activiteiten in belangrijke mate zelf regelen.

*) Romeinse cijfers verwijzen naar de literatuuropgave aan het einde van het artikel.

Ten aanzien van de gewenste omgevingen geldt, dat geen der functies in staat mag zijn ongevraagd het domein van een ander te "betreden". Hierdoor is er behoefte aan nog een functie, die, refererend aan de S/38 terminologie (security officer), Security zal worden genoemd. (Een betere naam voor deze functie zou zijn Bevoegdhedenbeheer.) Security creëert de omgevingen per functie. Security draagt zorg voor de overdracht van systemen (programma's en bijbehorende bestanden of databases) van de ene omgeving naar de andere. Kritiek punt in de samenwerkingen is de systeemacceptatiefase en de overdracht van geaccepteerde systemen naar een Verwerkingsomgeving. Gedurende de acceptatiefase kan de bedrijfsfunctie niet ook maar enige controle overlaten aan Programmering. De Programmeringsomgeving is derhalve ongeschikt. Ook de Verwerkingsomgevingen zijn niet geschikt voor de acceptatiefase: mogelijk instabiele systemen zouden de werkelijke bedrijfsgegevens ongewenst kunnen beïnvloeden. Een speciale omgeving voor de acceptatiefase is derhalve nodig.

Samenvatting

Noodzakelijke functiescheidingen in de organisatie moeten kunnen worden doorgetrokken tot in het computersysteem:



De sleutelvraag is nu, of en hoe de mogelijkheden die de S/38 biedt, op deze organisatorische functiegebieden kunnen worden afgestemd.

3. Systeem/38

Architectuur

Het gemeenschappelijk gebruik van een computersysteem heeft tot gevolg dat:
- gegevens van verschillende bedrijfsfuncties zich in één en dezelfde machine bevinden;
- verwerkingsprocessen ten behoeve van verschillende gebruikers gelijktijdig plaatsvinden.

Programma's mogen elkaar en elkaars gegevens niet beïnvloeden.
Het hoofdprobleem ligt in het gemeenschappelijk gebruik van geheugens. Er is behoefte aan geheugenbescherming.

Geheugenbescherming wordt doorgaans gerealiseerd door het toekennen van sleutels aan processen. Deze sleutels moeten passen op sloten, die worden geïnstalleerd op geheugendelen die aan het proces zijn toegekend. Het toekennen van sleutels en installeren van sloten gebeurt gewoonlijk door een overkoepelend proces, het operating system, dat daartoe de beschikking heeft over specifieke instructies. Om deze instructies te kunnen uitvoeren, moet de machine in de "privileged state" zijn. Deze status kan ontstaan ten gevolge van een interrupt. In deze situatie is het gehele geheugen toegankelijk voor het operating system.
Een probleem hierbij is, hoe kan worden voorkomen dat "gewone" gebruikers (toepassingsprogrammeurs) hun proces in "privileged state" kunnen laten komen. In vele gevallen biedt de machine-interface (gewoonlijk een assembler) in principe deze mogelijkheid.

Een andere methode om te voorkomen dat processen elkaar beïnvloeden is het gebruik van "capabilities". Een capability omvat een door de machine toegekende unieke naam per programma, bestand of welke entiteit ("object") in de machine dan ook, alsmede toegangsrechten (I, II)*). De entiteiten zijn alleen adresseerbaar door middel van de naam. De naam wordt opgeslagen in beschermd geheugen en kan niet door gebruikers worden gemanipuleerd. Elke poging om een naam, die in wezen een "pointer" is, te wijzigen, moet leiden tot vernietiging van die pointer.
Deze principes zijn toegepast in het Systeem/38. Ze worden uitgevoerd door hardware en/of microcode, en niet door een uit in wezen "gewone" programma's bestaand operating system.

S/38-basisconcepten

Het Systeem/38 is een op objecten gebaseerd systeem, waarin de adressering is gebaseerd op capabilities (namen). Alle entiteiten in het systeem worden gerepresenteerd in de vorm van objecten, bijvoorbeeld een reeks bij elkaar behorende instructies (object type "programma") of een reeks adresseerbare gegevens (object type "bestand"). De start- en eindadressen van een object worden door de machine toegekend en zijn geldig gedurende het bestaan van het object.

*) Literatuuropgave.

Een object wordt gedefinieerd als een benoemde entiteit, die verder wordt beschreven door de functies en bewerkingen die met of op het object kunnen worden uitgevoerd. (Andere namen hiervoor zijn "extended data type" en "abstract data type".)
Op het hoogste niveau zijn er twee types: de systeemobjecten (ondersteund door de machine) en de CPF-objecten (ondersteund door het CPF, Control Program Facility, het operating system van de S/38; het CPF bestaat in wezen uit een aantal objecten). De systeemobjecten worden in dit artikel buiten beschouwing gelaten.
Het CPF ondersteunt 23 (release 4.1) verschillende CPF-object types. Voor elk object type bestaan commando's om objecten te creëren, te onderhouden of te gebruiken.
De CPF-objecten zijn beschreven in bijlage 1 (bron: IBM manual).

Programmeurs zien geen verschil tussen intern en extern geheugen. De machine biedt één geheugen, noodzakelijk voor de realisering van capability adressing.

Van het CPF is geen source-versie beschikbaar voor gebruikers. IBM verschaft slechts een laadbaar operating system in microcode.
Ook is er geen machine-interface beschikbaar. Het laagste niveau van interface is de user interface: de CPF Command Language (CL).

4. Beheersings- en beveiligingsstructuur S/38

User-profiles, menu's, passwords

User-profiles zijn verbonden aan een password voor de aankoppeling en zijn zelf ook beschermd door een password, namelijk dat van de "security officer" (een specifiek user-profile in de S/38).
In elk user-profile kan een initieel programma worden gespecificeerd, dat normaliter automatisch wordt opgestart na aankoppeling door de desbetreffende gebruiker. Dit heeft de intentie de gebruiker in het keurslijf van een menu te dwingen, waarmee hij kan worden beperkt in zijn toegang tot programma's en bestanden.
Menu's behoren echter niet tot de ontworpen beveiligingsstructuur van de S/38. Ze ondersteunen de gebruikersvriendelijkheid.
Om verschillende redenen moet de toepassing van menu's worden aanbevolen, maar de beveiliging moet (anders dan in vele andere situaties, bij voorbeeld met een Systeem/34) hierop niet worden gebaseerd.

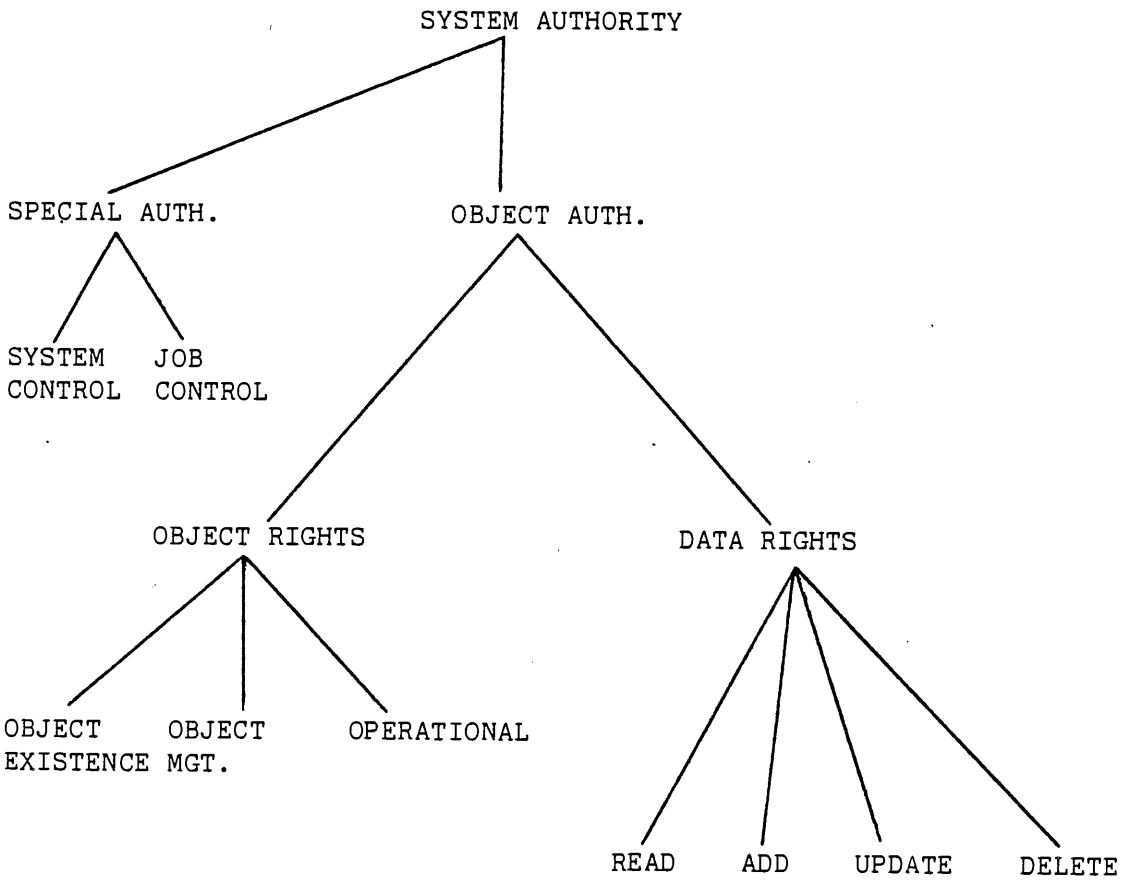
In het systeem bevindt zich standaard een aantal user-profiles:
- security officer (QSECOFR)
- programmer (QPGMR)
- workstation user (QUSER)
- system operator (QSYSOPR)
- IBM programming service representative (QPSR)
- IBM system engineer (QCE).

Al deze profiles, behalve dat van de security officer, bevatten de naam van een initieel programma. Ze zijn eveneens verbonden aan een initieel password.
Spoedig na installatie van een S/38 dient de security officer deze initiële passwords te wijzigen!

De user-profiles worden beheerd door de security officer, die ook het beheer over de passwords voert. Het beheer van de passwords kan bij de gebruikers zelve worden gelegd, doch de security officer behoudt altijd toegang tot de passwords en derhalve tot alle objecten in het systeem.
De security officer heeft dus toegang (en bevoegdheden) tot alle objecten in het systeem. Dit is een direct gevolg van de in het CPF gerealiseerde hiërarchische beveiligingsstructuur: de "man at the top" heeft nogal wat macht.
De S/38 structuur biedt de mogelijkheid security officer bevoegdheden geheel of ten dele aan andere user-profiles toe te kennen. Dit is in het huidige CPF echter niet opgenomen.
Op dit moment kan de verantwoordelijkheid voor de security officer functie in twee handen worden gelegd door het security officer password in een badge vast te leggen, dat onder dubbele versluiting wordt bewaard (hiertoe dient een badge-reader aan een werkstation te worden gekoppeld), of - eenvoudiger - door het password van de security officer in tweeën te delen, waarbij elk deel door een ander wordt gekend en beheerd.

CPF beveiligingsstructuur

De beveiliging in het Systeem/38 is geregeld door passwordbescherming op de aankoppeling van gebruikers, specifieke toekenning van bevoegdheden met betrekking tot besturingsoperaties en specifieke toekenning van bevoegdheden om objecten (programma's, bestanden, e.d.) te beheren of te gebruiken.
De structuur kan schematisch als volgt worden weergegeven:



Special authority

Indien aan een gebruiker special authority wordt toegekend, wordt dit vastgelegd in zijn user-profile. Er zijn twee soorten special authority:

- save system: save/restore-rechten ten aanzien van objecten;
- job control: rechten ten aanzien van jobqueues, jobs, outputqueues, bestanden in outputqueues.

Deze rechten worden doorgaans alleen aan de operator toegekend, waarbij bedacht moet worden, dat gebruikers vergelijkbare rechten bezitten ten aanzien van de objecten die ze in eigendom hebben.

Een object bestaat uit twee delen: een "description" en een "data part" (de feitelijke inhoud van het object, bijvoorbeeld de records in een file). Bij save wordt het gehele object gekopieerd. Bij restore wordt alleen het data part teruggeplaatst, tenzij het object tussen de save en restore operaties werd uitgewist (delete). In dat geval wordt het gehele object teruggeplaatst.
Als een object door middel van restore wordt teruggeplaatst, kijkt het systeem of de in het object vermelde eigenaar overeenstemt met het in het desbetreffende user-profile vastgelegde eigenaarschap (zie ook de volgende paragraaf). Als dit niet overeenstemt wordt automatisch de security officer als de eigenaar aangemerkt.

Object authority

Een gebruiker die een object creëert, is hiervan de eigenaar en heeft alle bevoegdheden ten aanzien van dat object. De eigenaar kan echter rechten toekennen aan andere gebruikers, bijvoorbeeld op het gebruik van gegevens in bestanden.
Het eigenaarschap wordt vastgelegd in het description-deel van het object. Daarnaast bevat een user-profile een lijst van de objecten waarvan de betreffende gebruiker eigenaar is.

Object authority omvat twee groepen rechten:
rechten op het object als geheel (object rights), bijvoorbeeld een bestand en rechten op het data part van het object (data rights), bijvoorbeeld ten aanzien van het object type bestand: de records in een bepaald bestand.

Objects rights

- existence: delete, save, free storage, restore, overdragen eigendom;
- management: verplaatsen, herbenoemen, bevoegdheden toekennen aan/herroepen van andere gebruikers;
- operational: het kunnen lezen van de beschrijving van het object; het object mogen gebruiken. (Deze rechten variëren per object type; ze kunnen tevens enige data rights omvatten).

Indien het eigenaarschap wordt overgedragen, verdwijnen de hierbij behorende rechten niet automatisch uit het user-profile van de "oude" eigenaar. Deze moeten uitdrukkelijk worden herroepen ("revoke") door de nieuwe eigenaar.

Data rights

- read: het mogen lezen van het data-part, bijvoorbeeld de records in een file;
- update: het mogen wijzigen van de inhoud van het data-part;
- add: het mogen toevoegen aan het data-part;
- delete: het mogen verwijderen uit het data-part.

Zoals gezegd heeft de eigenaar volledige bevoegdheid ten aanzien van zijn objecten. Hierna wordt aangegeven hoe rechten aan andere gebruikers kunnen worden toegekend ("grant").

Toekennen van rechten

Zowel object rights als data rights kunnen aan andere gebruikers worden toegekend. Dit kan expliciet aan individuele gebruikers worden gedaan (private), of aan alle gebruikers (public).

Private rights worden vastgelegd in de desbetreffende user-profiles. Ze worden toegekend door de Grant Object Authority of Grant User Authority commands. Ze kunnen worden herroepen door het Revoke Object Authority command.

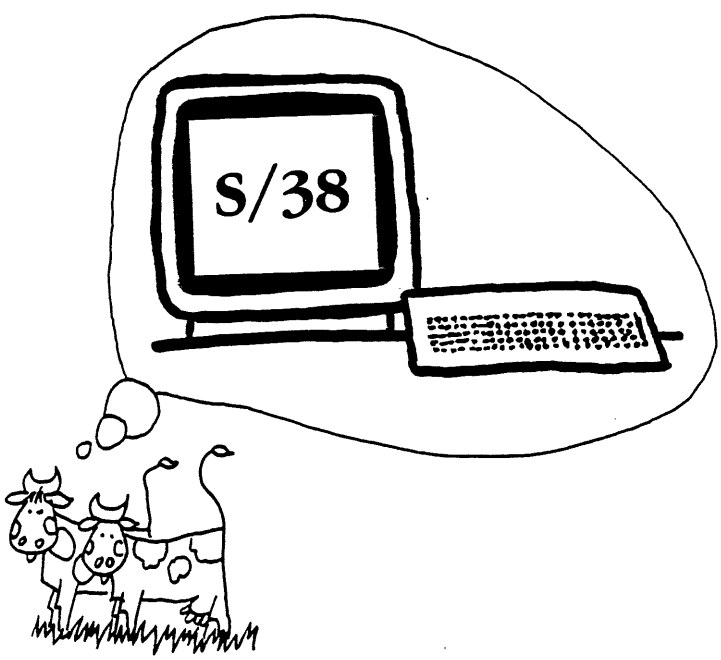
De volgende tabel uit het IBM-manual geeft aan welke data rights automatisch zijn vervat (aangegeven door een "O") in de toekenning van (private) operational rights.

Object Type	Data Rights			
	Read	Add	Update	Delete
Class	O	O	O	O
Command	O	O	O	O
Control unit description	O	O	O	O
Data area	O	O		O
Device description	O	O	O	O
Edit description	O	O	O	O
File				
Forms control table	O	O	O	O
Job description	O	O	O	O
Job queue				
Journal				
Journal receiver				
Library	O			
Line description	O	O	O	O
Message file				
Message queue				
Output queue				
Program		O	O	O
Print image	O	O	O	O
Session description	O	O	O	O
Subsystem description	O	O	O	O
Table	O	O	O	O
User profile				

De toekenning van "public" rechten kan gebeuren bij creatie van het object, of door middel van het Grant Object Authority command. Public authority wordt vastgelegd in de object descriptions.
Public authority kan als volgt worden gespecificeerd:

- normal: alle gebruikers krijgen "normale" bevoegdheden ten aanzien van het gebruik van het object; dit is een combinatie van operational authority en enige of alle data rights, afhankelijk van het object type (zie tabel hierna);
- none: alleen de eigenaar, de security officer en gebruikers die expliciet rechten kregen toegekend (private) kunnen het object gebruiken;
- all: elke gebruiker kan het object als ware hij de eigenaar (dus ook delete!) gebruiken.

Object existence rights en object management rights worden nooit toegekend als onderdeel van "normal public authority".



S/38: een gebruikersvriendelijke computer

De volgende tabel uit het IBM-manual geeft weer welke rechten worden toegekend bij "normal public authority" (aangegeven door een "N"):

	Object Rights	Data Rights			
Object Type	Operational	Read	Add	Update	Delete
Class	N	N	N	N	N
Command	N	N	N	N	N
Control unit description	N	N	N	N	N
Data area	N	N	N	N	N
Device description	N	N	N	N	N
Edit description	N	N	N	N	N
File (see note)	N	N	N	N	N
Forms control tabel	N	N	N	N	N
Job description	N	N	N	N	N
Job queue	N	N	N		
Journal	N	N	N	N	
Journal receiver	N	N			
Library	N	N	N	N	N
Line description	N	N	N	N	N
Message file	N	N			
Message queue	N	N	N		N
Output queue	N	N	N		
Program	N	N	N	N	N
Print image	N	N	N	N	N
Session description	N	N	N	N	N
Subsystem description	N	N	N	N	N
Table	N	N	N	N	N
User profile	N				

Noot: Data rights kunnen niet worden gespecificeerd voor logical files.

Om een CPF-object te kunnen gebruiken, moet een gebruiker zowel bevoegdheden bezitten ten aanzien van het object als ten aanzien van de bibliotheek waarin het object zich bevindt. Bij creatie van het object kan worden opgegeven in welke bibliotheek het moet worden geplaatst (de General Purpose Library, standaard in het CPF, is default, hetgeen wil zeggen, dat deze bibliotheek wordt gebruikt tenzij een andere wordt gespecificeerd), behalve voor de vanuit beveiligingsoogmerk belangrijkste object typen user-profile en bibliotheek, alsmede enige hardware beschrijvingen. Deze objecten worden automatisch in de systeembibliotheek QSYS, geplaatst.

De naam van een object bestaat uit twee delen ("qualified name"): de objectnaam en de bibliotheeknaam. Deze qualified names kunnen worden benut om de verschillende gebruikersdomeinen te creëren en de overdracht van objecten van de ene omgeving naar de andere efficiënt te regelen (zie hoofdstuk 6).

5. Ondersteuning voor Gegevensbeheer en Programmering

Programmering

Het CPF verschaft een uitgebreide ondersteuning voor de programmeurs in de vorm van een Source Entry Utility om interactief programma's te schrijven in RPG III, COBOL of de CPF Command Language (CL), een Data File Utility (DFU) ten behoeve van data entry en updaten van bestanden, een Query-faciliteit en een Screen Design Aid (SDA) voor het creëren van scherm layouts en menuprogramma's.

RPG III is gebaseerd op z'n voorgangers RPG en RPG II, maar kent enige uitbreidingen. In het bijzonder is de Data Description Specification (DDS)faciliteit van belang. Hiermee kunnen alle databases in het systeem worden beschreven, los van de toepassingsprogrammatuur.
Sources van RPG III-programma's en van DDS-gegevensbeschrijvingen worden gebruikt door CPF Commands die uitvoerbare programma's en fysieke of logische bestanden creëren.

Gegevensbeheer

RPG III biedt de mogelijkheid om files binnen een programma te beschrijven (om conversie van programma's in RPG II te vergemakkelijken), of om afzonderlijk (extern, door middel van DDS) gedefinieerde bestanden te gebruiken. In het eerste geval wordt gesproken over "program defined"bestanden, in het laatste geval over "externally defined"-bestanden.
Bij het definiëren van een bestand kan worden gerefereerd naar elders beschreven velden. Dit verschaft de mogelijkheid om centraal een zogenaamde "field reference file" (FRF) te onderhouden, waarin alle velddefinities en formaatbeschrijvingen worden opgenomen. De FRF vormt een belangrijk stuk gereedschap voor de Gegevensbeheer functie. De FRF is een gewone fysieke file, die echter niet wordt gecreëerd met als doel "echte" gegevens te herbergen; het data part wordt gewoonlijk leeg gelaten. Alleen het description deel wordt benut: hierin zit één (grote) recordbeschrijving met daarin alle waar dan ook gebruikte velden; hiernaar kan worden gerefereerd als "echte" bestanden worden beschreven en gecreëerd.

Bij het beschrijven en creëren van bestanden kan echter naar elk ander bestand worden verwezen; bovendien kunnen definities ook in de beschrijving zelf worden opgenomen. De overeenstemming tussen de FRF en de echte bestanden moet derhalve door procedures worden ondersteund, hetgeen een taak vormt van Gegevensbeheer. Gegevensbeheer zal hierin moeten samenwerken met de security officer.

Een zeer sterke eigenschap van de S/38 is de mogelijkheid om op elk gewenst moment de objectbeschrijvingen via een display zichtbaar te maken. De informatie die via een display wordt verstrekt, is dezelfde informatie waarmee het systeem werkt ten behoeve van de verwerking (in wezen is dit een voorbeeld van een "active data dictionary"). Deze eigenschap is van bijzondere betekenis voor ccntroledoeleinden gezien de één op één relatie die bestaat tussen ieder object en de daarbij behorende beschrijving. Deze relatie is niet te doorbreken.

Ook zijn er commands om de volgende informatie zichtbaar te maken:
- welke files worden gebruikt door een bepaald programma;
- welke fysieke files worden benaderd via een bepaald logisch bestand (een logisch bestand vormt ware een "user view" op gegevens; de gegevens in een logisch record kunnen een subset vormen van het fysieke record; het toegangspad - volgorde - kan per gebruiker verschillen);
- via welke logische files wordt een bepaald fysiek bestand benaderd.

6. Realisatie van de conceptuele organisatie met het CPF

In hoofdstuk 2 werden de volgende functies onderscheiden:
- Bedrijfsfuncties (eindgebruikers):
  - produktie
  - acceptatietestfase
- Programmering
- Gegevensbeheer
- Security.

De standaard CPF object typen bieden goede mogelijkheden tot het realiseren van de noodzakelijke gescheiden omgevingen.

De vanuit het gezichtspunt van beveiliging voornaamste object types zijn programma's en bestanden.

Enkele kerndoelstellingen zijn:
- Gegevensbeheer wil er zeker van zijn dat in operationele systemen de regels met betrekking tot het gebruik van gegevens worden nageleefd;
- Eindgebruikers willen er zeker van zijn, dat geaccepteerde systemen ongewijzigd blijven;
- Security wil dat de afzonderlijke omgevingen in stand worden gehouden.

Twee principes kunnen worden toegepast:
- om een object te kunnen gebruiken, moet de gebruiker de vereiste bevoegdheden hebben ten aanzien van dat object alsmede tenminste operationele bevoegdheid ten aanzien van de library waarin het object zich bevindt;
- overdrachten van de ene omgeving naar de andere worden beheerst door Security.

Voorbeeld van de realisatie van een beheersings- en beveiligingssysteem

1. Security creëert bibliotheken van 4 typen: Gegevensbeheer, Programmering, Acceptatie, Eindgebruikers-produktie.

2. Teneinde alle bibliotheken te kennen, reserveert Security het Create Library command voor zichzelf; ten gevolge daarvan is Security eigenaar van alle bibliotheken.

3. Teneinde op de hoogte te zijn van alle bevoegdheden van alle gebruikers zal Security in principe slechts operationele bevoegdheid ten aanzien van bibliotheken toekennen aan gebruikers. Operationele bevoegdheid impliceert het data right "read".

4. Gebruikers krijgen voor de bibliotheken binnen hun eigen omgeving ook de data rights "add" en "delete".

5. Databases worden alleen als extern beschreven bestand gecreëerd:
   5.1 Gegevensbeheer creëert in zijn bibliotheek een field reference file (FRF); elk gegevenselement wordt daarin één maal beschreven.
   5.2 Voor iedere database wordt, refererend naar de FRF, een sourcefile gecreëerd. Deze sourcefiles bevatten met RPG-source programma's vergelijkbare bestandsdefinities die worden gebruikt bij de creatie - vergelijkbaar met compileren - van de "echte" bestanden.
   5.3 Vanuit deze sourcefile wordt de fysieke file gecreëerd.
   5.4 Eveneens via sourcefiles worden over de fysieke files logical files gedefinieerd.
   5.5 Beide filetypen worden gecreëerd met de opties LVLCHK(*YES) en PUBAUT(*NONE). Levelcheck (LVLCHK) heeft tot gevolg dat, telkens wanneer de betreffende file wordt verbonden aan een actief programma, wordt gecontroleerd of de file-definitie nog hetzelfde is als ten tijde van de creatie van het programma. PUBAUT is de public authority parameter.
   5.6 Beide filetypen moeten, tijdens de ontwikkelingsfase, beschikbaar zijn voor de programmeur; Gegevensbeheer plaatst de files daartoe tijdens creatie in de programmeursbibliotheek. Hiertoe moet Gegevensbeheer operationele en add bevoegdheden hebben ten aanzien van deze bibliotheken. Gegevensbeheer creëert de databases en is hiervan derhalve eigenaar.

6. Programmeurs ontwikkelen sourceprogramma's in database sourcefiles in hun eigen bibliotheken.

7. Uitvoerbare programma's worden door de programmeur gecreëerd vanuit de sourcefiles met het create RPG/COBOL/CL-programma command. Dit geschiedt met de optie user-profile "*OWNER". De creator moet operationele bevoegdheid ten aanzien van alle gerefereerde objecten (in het bijzonder de te benaderen bestanden) hebben. Deze bevoegdheid alsmede de voor het testen benodigde data rights, wordt door Gegevensbeheer toegekend.

8. Indien de programma's gereed zijn voor acceptatie, brengt Security de programma's over naar een Acceptatiebibliotheek. De namen van de objecten blijven gelijk voor wat het eerste deel betreft, de qualifier (de library naam) maakt de naam als geheel uniek. Ook alle objecten die in de programma's worden gebruikt, moeten in deze overdracht zijn betrokken:
   8.1 Security stelt vast welke bestanden door de programma's worden gebruikt door middel van het DSPPGMREF command (display program references).
   8.2 Gegevensbeheer controleert deze informatie en zet de bestanden over naar de Acceptatiebibliotheek. Hiertoe kent Security op deze bibliotheek operationele en add bevoegdheid toe aan Gegevensbeheer.
   8.3 Gegevensbeheer maakt de bestanden schoon, zodat hierin de testgegevens kunnen worden opgebouwd (CLRFM command);
   8.4 Doordat de programma's werden gecreëerd met de optie user-profile "*OWNER" (zie stap 7), vindt uitvoering van de programma's plaats met de bevoegdheden uit zowel het user-profile van de eindgebruiker als die uit het profile van de eigenaar (de programmeur); hierdoor heeft de eindgebruiker de bevoegdheid om de betrokken bestanden te benaderen "geadopteerd" van de programmeur.
   8.5 De eigenaar van de programma's, de programmeur, heeft geen bevoegdheden ten aanzien van de Acceptatiebibliotheek: hij kan de acceptatietest niet beïnvloeden.
   8.6 De optie LVLCHK(*YES), zie stap 5.5, die bij creatie van de bestanden werd gehanteerd, draagt er zorg voor dat de gegevensdefinities zoals die naar het programma werden gecopieerd, overeenstemmen met de definities in de extern gedefinieerde file zelf (in het description deel). Level checking wordt bij elke "open" van het bestand uitgevoerd.

9. Na formele acceptatie worden de programma's en bestanden overgezet naar de eindgebruikers produktiebibliotheken. Deze procedure is gelijk aan die onder 8.

10. Indien wijzigingen moeten worden aangebracht, kan de procedure op gelijke wijze in omgekeerde richting worden uitgevoerd.
    Bij wijzigingen van een database echter, zal de betreffende fysieke file operationeel moeten blijven. De fysieke file zal gedupliceerd moeten worden door Gegevensbeheer (CPYF command); deze functie kan er eveneens voor zorg dragen, dat vertrouwelijke gegevens bij dit dupliceren worden weggefilterd.

7. Het gebruik van het Systeem/38 in de controle

Uit het voorgaande komt naar voren, dat de structuur van de S/38 uitstekende mogelijkheden biedt voor interne en externe controle. In dit hoofdstuk wordt die betekenis nader uitgewerkt voor de externe controle die zich richt op de financiële verantwoording (financial audit). Daarmee zal het tevens duidelijk zijn dat de S/38 ook van betekenis is voor de controle op de organisatie (operational audit).

Doelstelling van een financiële controle is het verkrijgen van een oordeel over een financiële verantwoording. De principiële controlemiddelen zijn het onderzoek van de organisatie waarin de gegevens zijn verzameld en verwerkt en, mede gebaseerd op conclusie uit het onderzoek van de organisatie, het onderzoek van het cijfermateriaal (pag. 52).

Onderzoek van de organisatie (compliance testing)

Indien de accountant besluit de handhaving en naleving van functiescheidingen te controleren, zal hij eerst vaststellen hoe de organisatie van de beveiliging en van het (gemeenschappelijk) gebruik van gegevens is opgezet. Hiertoe zal hij in contact treden met de Security en Gegevensbeheer functies. De CPF Command Language verschaft mogelijkheden om de beveiliging zoals die is geïmplementeerd, zichtbaar te maken. Een dergelijke controle verschaft vanzelfsprekend niet meer dan momentopnamen, waardoor het van belang is de controle zonder voorafgaande aankondiging uit te voeren. De controle is als zodanig een optimaal middel om een partieel of integraal beeld van de gehanteerde bevoegdheidsstructuur op een bepaald moment te kennen en te toetsen.

Terwille van de efficiency zal de accountant enige geautomatiseerde procedures voor het produceren van de momentopnamen moeten ontwikkelen. De controleprocedure bestaat voor een groot deel uit het zichtbaar maken van de relaties tussen gebruikers, bevoegdheden en objecten. Eveneens om redenen van efficiency zal de accountant een keuze moeten maken welke object typen, en binnen het type eventueel welke specifieke objecten, hij in zijn controle wil betrekken. Er is namelijk al gauw een groot aantal objecten in een S/38.

Stappen bij het gebruik van de computer in de controle

A. Voorbereiding

1. Kennis nemen van het beleid ten aanzien van beveiliging en het gemeenschappelijk gegevensgebruik.
2. Kennis nemen van het ontworpen systeem ten aanzien van beveiliging en het gemeenschappelijk gegevensgebruik.
3. Evalueren van beleid en systeem.
4. Voorbereiden controleprocedures.

B. Uitvoering

5. Aankoppelen onder het password van de security officer.
6. Nagaan hoe de verwerkingsomgeving eruit ziet.
7. Creëren bibliotheken, programma's, bestanden.
8. Uitvoeren CPF-commands en programma's.
9. Output en joblogs (van de batchjobs) naar de gewenste printer sturen.
10. Afkoppelen en creëren joblog interactive job.
11. Print joblog interactive job.
12. Save de bibliotheek en delete de bibliotheek.
13. Print historylog over de periode.
14. Laat security officer zijn password wijzigen.
15. Controle output en joblogs.
16. Evaluatie.

Stap 5

Sign-on onder het password van de security officer is nodig om bevoegdheid ten aanzien van alle aanwezige objecten te verkrijgen. Elk ander password verschaft een onvolledig beeld, doordat het slechts toegang verschaft tot de objecten die in het betreffende user-profile zijn vermeld (dat zijn de objecten in eigendom en de objecten waarvoor de gebruiker specifieke - private - bevoegdheden heeft gekregen) en tot de "public" objecten. Vanzelfsprekend vereist deze voorwaarde de medewerking van de security officer en instemming van de hogere leiding.

Stap 6

De accountant gaat hier na welke subsystemen hij ter beschikking heeft, welke jobdescriptions toepasbaar zijn, welke queues aanwezig zijn en naar welke printer hij het beste zijn output kan sturen.

Stappen 7/8

De accountant zal beginnen een eigen library te creëren door middel van het CRTLIB command, waarbij de public authority parameter de waarde *NONE krijgt. Vervolgens zal hij in zijn library de nodige source en data-bestanden creëren; hiervoor is het CRTPF commando (create physical file) beschikbaar: type *SRC voor de programma source-bestanden (met de standaard recordlengte 92) of type *DATA.
Sourcefiles kunnen ook zeer eenvoudig worden gecreëerd als met de Source Entry Utility wordt gewerkt (optie 8 van het programmeursmenu; het programmeursmenu kan worden bereikt door het commando CALL QPGMMENU in te toetsen op het command entry scherm; dit menu maakt het ook mogelijk op eenvoudige wijze CPF commands en programma's te laten uitvoeren, programma's naar een batch-subsysteem te sturen, in outputfiles te kijken, e.d.).

Vervolgens worden de controleprocedures ontwikkeld, waarbij gebruik wordt gemaakt van CPF commands, Command Language programma's of hogere programmeertalen (COBOL, RPG III). Indien de CPF-release CL commands bevat waarmee files kunnen worden gelezen, is het gebruik van een hogere programmeertaal niet meer nodig.

Voorbeeld

De accountant wil inzicht krijgen in de bevoegdheden ten aanzien van alle bibliotheken.
Eerst zal hij moeten weten welke bibliotheken in het systeem aanwezig zijn. Dit is mogelijk door middel van het commando "display object description":

```
DSPOBJD  OBJ(*ALL)  OBJTYPE(*LIB)
```

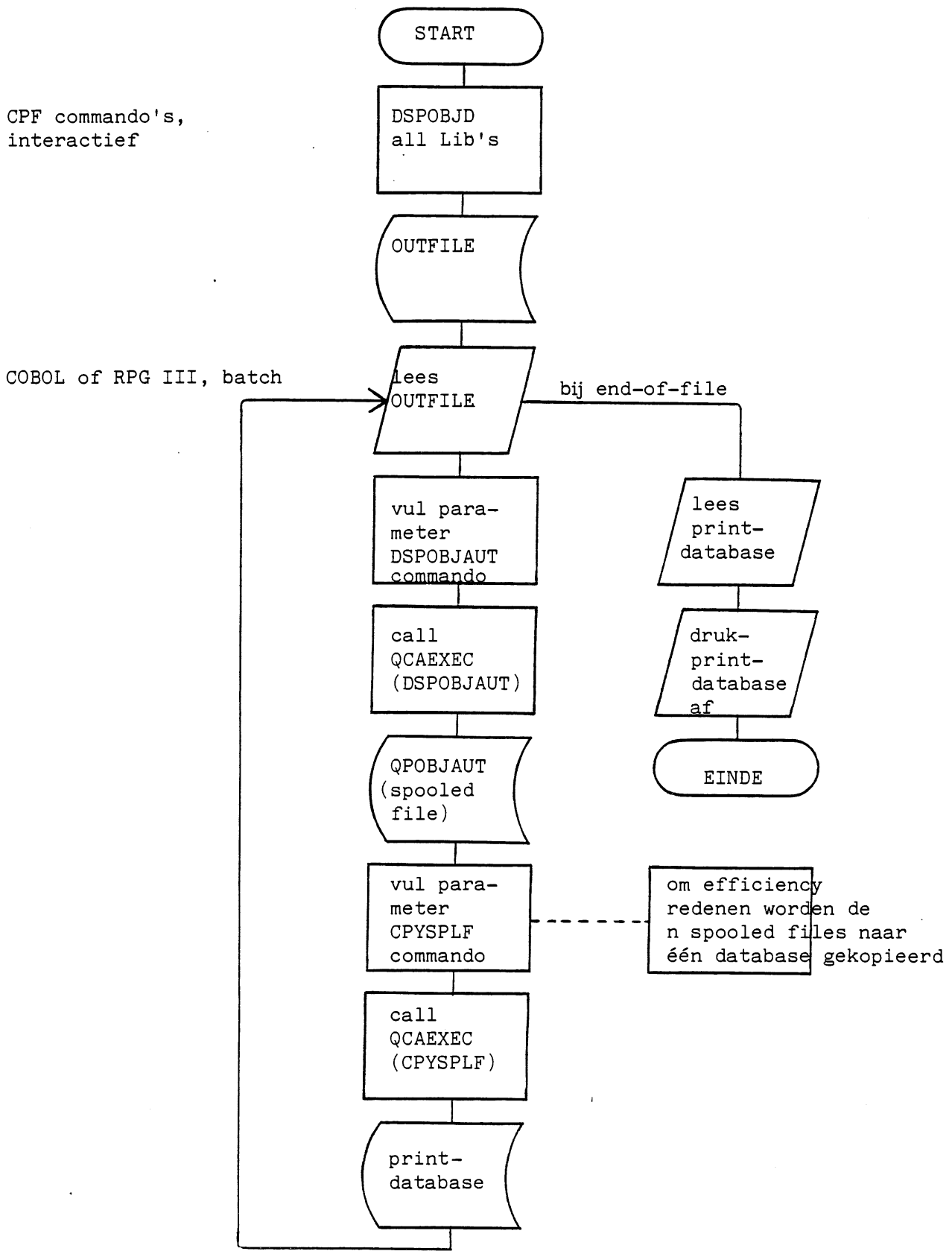
De output verschijnt naar keuze op papier of op het scherm. Daarnaast is het mogelijk de output (die de namen van alle bibliotheken bevat) in een database op te slaan, die door een COBOL, RPG III of CL-programma verder kan worden verwerkt (OUTFILE parameter).

De bevoegdheden voor libraries kunnen zichtbaar worden gemaakt door het commando "display object authority":

```
DSPOBJAUT  OBJ(library naam)  OBJTYPE(*LIB)  OUTPUT(*LIST)
```

De namen kunnen gelezen worden uit de database die met het eerste commando werd gecreëerd. Dit houdt in, dat het DSPOBJAUT commando n keer moet worden uitgevoerd, waarbij n het aantal bibliotheken is.
Om deze reden is een programma nodig dat de database leest en n keer een loop uitvoert; de loop bevat het DSPOBJAUT commando; de waarde voor de library naam in de OBJ parameter wordt op grond van de informatie in de database, steeds gewijzigd.
De loop kan vanuit een COBOL of RPG-programma worden gerealiseerd door de routine QCAEXEC aan te roepen. Deze routine stelt in staat tot het dynamisch creëren en uitvoeren van CPF commands.

Schematisch kan een en ander als volgt wordenweergegeven:



Stap 9

Na uitvoering van de geautomatiseerde procedures moet de accountant er voor zorg dragen, dat de printuitvoer naar een printer wordt gestuurd die hij onder visuele controle heeft.

Stappen 10/11

De joblog wordt gecreëerd door het SIGNOFF commando de parameter *LIST mee te geven. Joblogs zijn van belang als bewijsmateriaal terzake van wat de accountant aan commando's en programma's heeft uitgevoerd.

Stap 13

De historylog is van belang om vast te stellen dat niemand anders onder het security officer profile actief is geweest, daar in dat geval een risico van beïnvloeding heeft bestaan.

De hier vermelde controleprocedure zal als nevenvoordeel kunnen hebben, dat verwatering in de handhaving en naleving van beheersings- en beveiligingsprocedures wordt tegengegaan.

Onderzoek van het cijfermateriaal (substantive testing)

Het beoordelen en verifiëren van het cijfermateriaal kan veelal efficiënt en effectief worden ondersteund door het inschakelen van de computer in de controle. Er zijn globaal 2 mogelijkheden voor de verwerking: verwerking op de computer van de accountant en verwerking op de computer van de gecontroleerde. De eerste situatie is mogelijk door middel van fysieke bestandsoverdracht op diskette en soms ook op tape. De tweede mogelijkheid plaatst de accountant in principe in een situatie met het risico dat de gecontroleerde de verwerkingen van de accountant op ongewenste wijze beïnvloedt.

Zoals eerder is gesteld, vereisen verschillende functies in een organisatie afzonderlijke omgevingen; dit geldt eens te meer voor de onafhankelijke accountant.
De beheersings- en beveiligingsmogelijkheden zoals die werden beschreven in hoofdstuk 4, te zamen met de suggesties ten aanzien van de wijze waarop de functiescheidingen binnen de computer kunnen worden geëffectueerd in hoofdstuk 6, zullen duidelijk maken dat de accountant de S/38 van de gecontroleerde kan benutten voor het doen uitvoeren van zijn controleprogrammatuur, met voldoende garanties voor het behoud van zijn onafhankelijkheid. Hij zal echter moeten vaststellen dat de security officer niet tijdens de zelfde periode actief is geweest; dit is mogelijk door middel van de "history log" waarop alle sign-on's en sign-off's zijn vermeld.
Vanzelfsprekend moet de accountant de S/38, het CPF en de beveiligingsstructuur goed doorgronden. Een groot voordeel van de S/38 is echter, dat deze kennis op alle S/38 computersystemen toepasbaar is, omdat er slechts één CPF is; een gebruiker moet het volledig implementeren, waardoor de accountant altijd met hetzelfde operating system in aanraking komt.

Literatuur

I Linden T.A., Operating system structures to support security and reliable software, Computing Surveys Volume 8, no. 4 December 1976.

II Houden M.E. e.a., IBM System/38 support for capability based addressing, Proceedings 8th annual symposium on computer architecture 1981 (ACM, IEEE).

III A.H.C. Koedijk, De organisatie van gegevensbeheer, Compact winter 1981/1982.

IV A.W. Neisingh/A.H.C. Koedijk, Het gebruik van de computer in de Accountantscontrole, Deel I, Handboek Accountancy III, 50.

Lente 1983

Bijlage 1

OBJECT TYPES

Objects are the basic units upon which commands perform operations. For example, programs and files are objects. Through objects you can find, maintain, and process your data on System/38. You need only know what object and what function (command) you want to use; you do not need to know the storage address of your data to use it.

There are 23 types of objects on System/38. Each type has unique purpose within the system and has associated with it a set of commands with which to process that type of object. The following lists the 23 types of objects, the abbreviations used as parameter values for object type parameters, and the definition of the object belonging to that type:

- Class (* CLS). An object that contains the execution parameters for a routing step.

- Command definition (* CMD). An object that contains the definition of a command (including the command name, parameter definitions, and validity checking information) and identifies the program that
- performs the function requested by the command.

- Control unit description (* CUD). An object that contains a description of the features of a control unit that is either directly attached to the system or attached to a communications line.

- Data area (* DTAARA). An object that contains a description of an area used to communicate data such as CL variable values between the programs within a job and between jobs.

- Device description (* DEVD). An object that contains a description of a device that is attached to the system.

- Edit description (* EDTD). An object that contains a description of a user-defined edit code.

- File (* FILE). An object that contains a description of a set of related records treated as a unit and, optionally, those records.

- Forms control table (* FCT). An object that designates the special processing requirements for specific printer or punch output streams received by an RJEF (Remote Job Entry Facility) session from a host system.

- Job description (* JOBD). An object that contains the attributes of a job.

- Job queue (* JOBQ). An object on which entries for batch jobs are placed when they are submitted to the system and from which they are selected for execution by CPF.

- Journal (* JRN). An object through which the changes made to a data base file are recorded. These changes are recorded in a journal receiver.

- Journal receiver (* JRNRCV). An object that contains entries, called journal entries, generated when a change is made to a data base file being journaled.

- Library (* LIB). An object that serves as a directory to other objects. A library is used to group related objects and to find objects by names when they are used.

- Line description (* LIND). An object that contains a description of a communications line to the system.

- Message file (* MSGF). An object that contains message descriptions.

- Message queue (* MSGQ). An object on which messages are placed when they are sent. A message queue can be associated with a person, program, work station, or job.

- Output queue (* OUTQ). An object that contains a list of output files that are to be written to an output device by a writer.

- Print image (* PRTIMG). An object that contains a description of the print belt or print train on a printer.

- Program (* PGM). An object that contains a set of instructions that tell a computer where to get input, how to process it, and where to put the results. A program is created as a result of a compilation.

- Session description (* SSND). An object that contains a description of the operating characteristics of an RJEF session.

- Subsystem description (* SBSD). An object that contains the specifications that define a subsystem and that CPF uses to control the subsystem.

- Table (* TBL). An object that contains a set of hexadecimal characters used to translate one or more bytes of data.

- User profile (* USRPRF). An object that contains a description of a particular user or group of users. A user profile contains a list of the objects and functions the user is authorized to.

(Source: IBM-manual)

compact

Lente 1983

DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE

door H. Veenman

Nieuws van het audit-micro front

Planningsysteem operationeel.

In de maand mei 1983 is een geautomatiseerd planningsysteem, genaamd "plens" in gebruik genomen op de microcomputer van kantoor Deventer, waar het, onder leiding van B. Koldewey, op de proef zal worden gesteld. Plens is ontwikkeld door een lid van de audit-micro-groep en is geënt op de wijze van plannen, zoals deze binnen KKC wordt gehanteerd.

KKC audit pakket.

Reeds tweemaal is een demonstratie gegeven van de audit-micro-computer; eenmaal voor de collega's van kantoor Brussel, en eenmaal voor de A.C.-kernleden, de A.C.-part-timers, steekproefconsulenten en enkele andere genodigden.
Tijdens deze gezamenlijke demonstraties is men in de gelegenheid gesteld een bestandsonderzoek uit te voeren met behulp van een eerste versie van het zogenaamde "KKC audit pakket".
Dit pakket, dat in de toekomst aanwezig zal zijn op de portable-audit-micro, stelt de algemene controlesector in staat om op relatief eenvoudige wijze een bestandsonderzoek uit te voeren op een bestand, dat op enigerlei wijze door de betreffende cliënt ter beschikking is gesteld.

Er is begin juni een aantal microcomputers aangeschaft (IBM personal computer), die onder andere worden gebruikt om de algemene sector met dergelijke apparatuur vertrouwd te maken.

Nieuwe ontwikkelingen.

Gedurende de zomermaanden zal door de audit-micro-groep het lopende onderzoek worden geïntensiveerd naar de verschillende mogelijkheden van datacommunicatie tussen de audit-micro en andere computers; tevens zullen de mogelijkheden van het KKC audit pakket worden uitgebreid.

Hierna volgt het tweede deel van de speech van Mr. Raymond H. Healey. De aandacht wordt nu gericht op de huidige ontwikkelingen van de "audit-micro".
Het derde en laatste deel van de voordracht zal worden opgenomen in het komend nummer van Compact.

CURRENT DEVELOPMENTS FOR FUTURE THINKING

Speech regarding microcomputers presented by
Raymond H. Healey (part II) november 1982 ')

This imaginary day (see part I in Compactnumber 30, 83/1) has been based on the use of a multi-function workstation to assist in a wide variety of professional and management tasks.
This workstation combines the attributes of the state of the art EDP microtechnology, data communications, word processing, text editing and data storage. The work station is user friendly and connects to large and small EDP functions. It has the capacity and function to stand alone or to be interconnected to distributed networks, both locally and internationally.

The workstation was used by KM to obtain access to a variety of support systems that ranged from direct audit support, to engagement management and administrative support functions, office management, special services such as convenience computing and the use of the firm's data bank or data base. All of these computer based support functions are linked together by the combined resources of communication, data processing hardware, software/office equipment, and related training.

A review of some key trends in computer technology will help illustrate the nature and speed of change in information processing. I would like to show some headlines from a few recent newspaper and magazine articles, to demonstrate that the scenario that I've just presented is not only plausible but gradually taking place.

First of all, the portable briefcase computer is a reality; a modern manager's tool kit, engineered and produced in Japan. It is the forerunner of newer and more powerful units that will combine the newest micro chip developments with space age miniaturization.

Another Japanese invention is this pocket computer that has a four colour printer built in and can produce graphs and charts in addition to normal text output.

New generations of computers are appearing every few months. Each claims superiority over preceeding generations and each offers more features and better performance for lower prices.
This system is designed to grow with the user, with an expansion factor of up to 800%.

And not satisfied with displaying data, there are more and more colour graphics packages available on micros.

Even the mainframe manufacturers are feeling the competition and reaction to the price/performance push in order to retain their share of the market.

') Raymond Healey is a partner of The Canadian KMG Member Firm Thorne Riddell. He is also chairman of the computer audit subcommittee within KMG.

And of course there are the usual inflated claims such as our ambitious accounts clerk, buried under paper -- a condition that is easily resolved by use of EDP technology.

If even a very small number of all of these predictions come true, we are going to have some adjusting to do. Many forecasters suggest that even our KM scenario is conservative and that the "electronic cottage" and the integrated electronic office will be realized and indeed form a major part of business operations. We as KMG members are in a highly influential position to soften and manage the impact of these changes, which could be turned into opportunities for our clients and our respective firms. Next I'd like to emphasize on the very dramatic changes in computer technology that have occurred in only the last few years.
The emerging technology and the resultant cost/performance gains resulting from dramatic improvements such as circuit sizes being cut in half each year, costs cut in half every two years and new thresholds in computing power and function are driving the micro evolution forward.

Components per circuit have increased from 16 in 1964 -- the function necessary to run a clock radio or automatic coffee percolator -- to 4 million in 1982.

Circuit costs will have dropped from 12c per bit in 1979 to 2c in 1983.

The physical size of computers has seen them shrink from requiring room size, air conditioned block houses to circuit boards or even chips -- with more functions. The dramatic reduction in the size of the computer has largely been a result of computer chip technology. In 1965 it was possible to store about 1,000 memory bits on a chip.

Now we routinely store more than 65,000 bits per chip and within a year, as many as 1 million bits per chip is considered a feasible target.

To illustrate the storage capacity of these chips, a page from a telephone book requires about 20,000 characters of memory -- well below the capacity for most contemporary chip designs.

Costs have also dropped dramatically. In 1964 1,000 characters of computer memory had a cost of $2,000. In 1973 that memory cost dropped to $300, in 1979 to about $15, and now to about $8.

Similarly, the cost of mass data storage has dropped. In 1964 the cost per million characters of storage was $ 3,333. In 1973 that same storage capacity cost was $188 and that storage capacity can now be purchased for about $40.

By way of contrast, staff costs, particularly for office workers, have doubled from 1969 to 1979 with a material decline in productivity. The same kind of trend can be applied to personnel in the data processing profession, especially the more experienced systems analyst and programmer. One reason for this is found in the value of the capital investment made per employee which ranges from a low level of between $2,000- 4,000 for an office worker to $18,000 in agriculture, $25,000 in manufacturing and over a million in an oil refinery.

However, much of the activity and excitement is not coming from the traditional computer area at all. The real impact is already being made by the microcomputer which is destined to accomplish in the technological evolution what steam did for the industrial revolution.

The attitude of many business persons to a personal mainframe means wider use and acceptance of data processing as everyone's business tool.
Micros represent the imaginative use of cheap technology to achieve a simple, user friendly operation.

These features have already led to an incredible proliferation of small personal computers with many of the capabilities of the large office computer -- and that is only the effect of the first generation. What are these revolutionary catalysts -- the foot soldiers of the technological evolution.

Some typical and popular examples of micros that are becoming more business oriented are Tandy, IBM, Apple, Commodore, DEC, HP, etc. The price range varies from $700 to $10,000.

The impact on number of units delivered is an illustration of the growth and change in market share of small computers. From 1980 to 1990 it is forecasted that they will increase in number of units sold from 70% until they dominate the market at 95% of units delivered.

However, much lower unit costs will mean that sales value will comprise only about 50% of an $8,3 billion market (but that's still $4,2 billion).

In terms of processing power, small computers will greatly increase their share from about 15% to greater than 75%. These are optimistic forecasts perhaps, and serve the interests of the micro producers but now let's look at examples of what's really happening.

First of all we have perhaps the lowest price unit of all -- the Sinclair $99.95 ZX 81 personal computer conceived and built by Clive Sinclair -- considered to be one of the Beatles of personal computers.

But let's start instead with Adam Osborne, at 44 the other Beatle of micro-land who designed and produces the Osborne. This ugly duckling of the micros, sold 11,000 units in the first 8 months on the market and has now reached total sales of greater than 150,000 units for a sales value of $175 million. He has earned more than $25 million after tax already on this unlikely product. His production cost is about $425 per unit.

It takes a worker about 68 minutes to assemble this 24 lb portable briefcase computer from several components using 40 screws. His 38 workers produce about 200 daily and are up to a production level of 25,000 per month. How much does it cost -- about $1,795 for a basic unit. A computer-printer combination with several widely used software packages costs about $2,900.

Now we will return to Clive Sinclair, the 42-year-old electrical engineering genius who with his 30 employees at Kings College, Cambridge turns out the ZX 81, a descendant from the original ZX 80 personal computer. It sells at $99.95. This happy band of workers can produce 50,000 units per month and sold 250,000 units in their first ten months in the market. First year sales were $38 million, producing an after-tax profit of $13,3 million. Market forecasts for the Sinclair are 2,25 million units.

This computer which sells at under $200 costs less than $70 to produce. Recently, a partnership arrangement has been concluded with Timex -- the gigantic watch distributor to take over the marketing and distribution of Sinclair computers. Their objective is quite simple -- they want everyone to have one and they expect to make more money from computers than from watches. They expect to reach the $1 billion level per year in sales producing $50 million in royalties for Mr. Sinclair. So much for mid-life crisis.

Recent forecasts suggest U.S. micro processor sales for office use will increase from 1981 figure of about 500,000 to nearly 7 million in 1990.

Home computers will proliferate even faster, growing from 710,000 to 34 million.

In the past three years, for instance, the average price range for office installed mini computers has fallen from between $35,000 and $200,000 to between $10,000 and $140,000, and by 1990 the base price may be as low as $2,200. Home computers will similarly go the way of the digital watch and the pocket calculator, falling from today's $600 to $1,500 to around $400.

A comparison is very revealing -- if the automobile industry had done what the computer industry has done in the last 30 years, a Rolls Royce would cost $2.50 and get 2 million miles per gallon.

-- or, if you are continental in your measures, 700,000 kilometres per litre.

Is it any wonder that even giant IBM, who were very slow to react and quite late into the micro computer industry has already sold a quarter of a million of their new Personal Computers in the first year it has been available in scarce quantity and against long waiting lists. They announced their entry into the market in August, 1981 - following 18 months development, and has sparked not only interest but the weight of the name has greatly increased the micros credibility for business use. This new legitimacy has been followed by a host of imitators - of which 5 are on the market and 10 more are planned, including 6 major Japanese producers.

So far the most interesting is the COMPAQ, produced in Houston, Texas - and announced in the Wall Street Journal, November 4, 1982.

It is priced at $2,995 - about $1,600 less than the IBM PC. It is portable, at 28 lbs. and runs all major IBM programs without modification. It has a 9" screen, two disk storage units and boasts 128K - random access memory. It even beats the IBM PC - in another area - it has graphics display software.
The COMPAQ is targeted at a $1 billion market.

The long-awaited Japanese invasion of the micro computer market has begun and not only appears to follow their approach to automobiles, that is, do the same but better, but also a complete re-thinking of the computer itself. They will be based on IBM like machines - and go far beyond them. Their home market is growing so rapidly that they can't meet local demand - and can't plan to seriously go after the Western market until well into 1983 or 1984. From abacus to micros in one generation - after everything else they have accomplished in the last 30 years, the mind boggles. One other message is clear from the Japanese also - IBM compatibility is absolutely necessary for companies getting into the personal computer market and there is no doubt the Japanese machines will take this approach in their designs.

Even the term personal or convenience computing is losing its meaning. Estimates are that between 25 and 40 percent of these computers are finding their way into corporate offices, primarily to aid managers. In 1981, large corporations accounted for 11 percent of the micro market and this year it has grown to 25 percent. The unassuming micros are being purchased in batches for use by individual managers.

Where are micros going? They are certain to deliver more power and more function at an even lower cost. Programming languages such as COBOL and application programs such as general ledger and payroll systems will be programmed onto chips. By doing so, software and opera-

ting system can function under greater security and control. The rapid advances in software development will make them more user friendly with voice recognition and answer. They will become prime candidates to support special purpose business and accounting systems and will almost certainly become an integral part of business activities to such an extent that the once clear division between micro and mainframe processors will become blurred and even disappear. The best definition to date to separate the two is that a micro can be purchased with a credit-card at the local electronic shop.

How soon will this happen - very. The November 12, 1982 issue of the Economist carried an article on user-friendly - touch sensitive screens. The first is likely to be Apples - Lisa - due to be launched in January, 1983 at $3,000. At the touch of a finger, the user will be able to indicate which command on the screen he wants carried out - or draw a picture - which just might be a way to flowchart out accounting systems in the future.

The November British Airways magazine - High Life - talks about push button artists - using CGI or computer generated imagery - to produce graphics or computer paintings. The computer engineers have invented the electronic paintbox which uses an electric pen to paint images on a screen and reproduce them in a tidy, perfect form. A rough square becomes a perfectly regular square, after using the tidy up software. It's hard to know where the super smart computer now takes over from man.

These changes will have an impact not only on how we manage and carry out our professional responsibilities but on the way we live in a society where there will be almost universal computer literacy. I would like to conclude this segment with several direct quotations which have appeared in print in the last two years -- quotes that refer to several sides of the micro issue.

1. The first is from the Wall Street Journal, quoting a big 9 firm partner.

   "Here come the minicomputers -- and right behind them, here come the crooks ... the rapid proliferation of minicomputers, and their ease of operation by nonspecialist personnel from vice presidents down to secretaries, is creating a massive new potential for embezzlements and other frauds ... There are going to be a lot of shocks and horror stories out there."

2. The second is from a technical paper on computer fraud and countermeasures, by a well known security consultant.

   "We are fast approaching the time when one out of every ten people in the work force will have a direct working relationship with computers. With the number of installed computers approaching the half-million mark on the scale and proliferating more rapidly as a result of minicomputers and micro processors, there is not much doubt that computer fraud will grow proportionately."

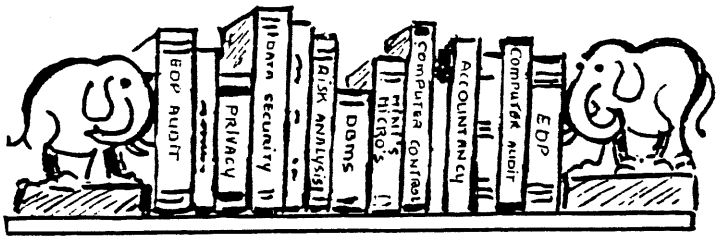
3. "Many data processing executives have been very concerned about the proliferation of microcomputers... The message of the day is: you ain't seen nuthin' yet. If minis have proliferated, micros will explode. Control will become more and more difficult ..." written by two leading minis/micros EDP consultants in an international magazine on data processing.

4. IBM correctly states that the time is not long in coming (and in many enterprises is already here) when establishing the adequacy of accounting controls will be inseparable from establishing the adequacy of controls built into and surrounding the computer, its programs and data. This is quite a radical statement from the usually moderate and measured big blue machine.

5. Technological developments (e.g., large scale integration circuits) have increased performance to the point that "it is almost impossible to define a minicomputer anymore and the boundary between minicomputers and microcomputers is getting hazy". Our concern is not with technical specifications, but rather the control problems inherent in an environment in which a mini or micro computer is used by a small firm.

   From a feature article in a leading EDP publication.

6. Perhaps the most incisive quote is from the venerable Captain Grace Hopper (U.S. Navy), well known in internal audit circles, commenting on the development of microcomputers versus maxicomputers who put it all in focus when she said, "Just remember, it wasn't the dinosaurs who survived; it was the lizards."



Boeken

Titel: De organisatorische voorwaarden voor automatisering van de informatieverzorging
Serie: Studierapporten nr. 11
Auteurs: Werkgroep "Voorwaarden voor automatisering van de informatieverzorging"
Uitgave: Nederlands Instituut van Registeraccountants
AC-Bibliotheeknummer: AC 439, code A14
Aantal bladzijden: 52
(toevoeging boekbespreker); (C) = commentaar

Het studierapport is een weloverwogen weergave van een gedegen studie. Het laat zich eenvoudig lezen. Het bestaat uit:

- de inleiding (4 pag.)
  - 1.1 Doelstelling en inhoud van het rapport; doelgroep, afbakening van de probleemsituatie
  - 1.2 Kort overzicht met aanduiding van de in het rapport behandelde punten
- de studie verdeeld in 6 hoofdstukken (20 pag.)
  - 2 De beleidsvorming in de organisatie.
  - 3 Het klimaat in de organisatie en de houding van de betrokkenen
  - 4 De structuur en het functioneren van de interne organisatie
  - 5 De informatieverzorging
  - 6 De kennis en vaardigheden van de leden van de organisatie
  - 7 Enkele organisatorische facetten van de aanpak van de automatisering

Het rapport is tot stand gekomen onder auspiciën van de Commissie Advies inzake Automatiseringsvraagstukken (CAV).
Voor de samenstelling van de werkgroep, die onder leiding stond van prof.drs. H.B. de Mare, verwijzen wij u naar het Ten Geleide van het studierapport.

Karakteristiek

Zoals u kunt lezen in de inhoudsopgave is het rapport niet specifiek gericht op "Automatisering en Controle", maar heeft het er wel alles mee te maken.

Het rapport geeft een beschrijving van de "ambiance" waarin automatisering en controle eerst goed tot zijn recht kan komen. Op een aantal plaatsen in de tekst worden betrouwbaarheid en continuïteit, efficiency en effectiviteit genoemd, aangeduid of als vanzelfsprekend verondersteld. Fysieke beveiliging en grensoverschrijdend gegevensverkeer worden niet genoemd. Het woord "privacy" verschijnt in de laatste zin van het rapport.

Het is de functie van de boekbespreker om het rapport kritisch te lezen en eventueel opmerkingen te maken. Wij doen dit juist bij dit rapport ongaarne, omdat het mogelijk afbreuk doet aan de sfeer die het oproept.

Het is duidelijk dat het rapport weergeeft wat de leden van de werkgroep belangrijk vinden. Wij kunnen u adviseren het rapport vooral nauwkeurig te lezen, woord voor woord, en zien welke wereld er achter schuil gaat.

Het rapport kent een 3-tal beperkingen:

1. Op pagina 5:
   "Attentiepunten met betrekking tot de opzet en aanpak van een automatiseringsproject komen slechts beknopt aan de orde. Hierover is in ruime mate elders gepubliceerd."
2. Op pagina 10:
   "De controleproblematiek in het kader van de automatisering - waarbij in het bijzonder interne controle-aspecten een belangrijk aandachtsveld vormen - en de functie van de controlerend accountant vallen buiten het bestek van dit rapport."
3. Op pagina 29:
   "Het literatuuroverzicht is afgesloten in het voorjaar van 1981". (Blijkbaar is de studie in 1978 beëindigd, gezien de vermelding van het copyright.)

   Het merkwaardige nu is dat bij het lezen deze toch niet geringe beperkingen niet storend zijn.

In hoofdstuk 3 op pagina 13 wordt de betrokkenheid van de leiding bij de automatisering beschreven. In dit verband zou ook iets van de betrokkenheid van de accountant bij het ontwikkelen van projecten gezegd kunnen worden. Zijn bemoeienis met de ontwikkelfunctie wordt sterk bepaald door filosofie van de aanpak van de accountantscontrole en door de mogelijkheden van de cliënt om zelf tot een toereikende opzet van de interne controle te geraken. Als minimum eis kan gesteld worden dat hij kennis zou moeten kunnen nemen van de paragraaf waarin in het ontwerp de aanpak van de interne controle wordt beschreven. Gewenst is dat de accountant voordat het systeem in exploitatie wordt gebracht, gelegenheid krijgt om de definitieve opzet van de controle te leren kennen en de mogelijkheid krijgt daarop zonodig te kunnen reageren.

Op pagina 14 wordt ingegaan op de gebruikersopleiding:
"Het effectueren van een gebruikersvriendelijke opzet van de automatisering."

> Gebruikersvriendelijk moet tevens inhouden dat de gebruikers de werking en de resultaten van de automatisering moeten kunnen beoordelen en controleren. Dit is noodzakelijk wil de gebruiker zijn verantwoordelijkheid kunnen dragen.

Op pagina 15 wordt de term "Procedurebewust" gebruikt. Wij merken hierbij op dat geen melding wordt gemaakt van nieuwe technieken. Wij noemen in dit verband:

> Prototyping, op het gebied van de systeemontwikkeling een nieuwe methodiek. Alhoewel ook hierbij het aanhouden van procedures noodzakelijk is, ligt hierop niet de nadruk. Prototyping maakt gebruik van de methodiek om een model te maken van de werkelijkheid zoals dat in de analyse door de toekomstige gebruiker wordt opgeroepen. Het model kan effectief en efficiënt worden aangepast na verificatie met de gebruiker. Hierdoor wordt de betrokkenheid van de gebruiker vergroot. Tevens ontstaan met een kortere doorlooptijd systemen die leiden tot een snellere acceptatie.

"Inzake het aanbrengen van verbeteringen/aanpassingen" (pag. 17 merken wij op dat voor een flexibel verloop daarvan in geautomatiseerde systemen het noodzakelijk is de programmatuur op te bouwen uit een groot aantal relatief zelfstandige onderdelen van een beperkte omvang (modulair programmeren).

Bij het punt "De informatieverzorging" (pag. 19) tekenen wij aan dat in de literatuur een nieuwe functie is geïntroduceerd, te weten de Informatiemanager. Hij is degene die namens de leiding een coördinerende en controlerende functie heeft met als doel te komen tot een verantwoorde en evenwichtige informatieverzorging.

Ook de accountant heeft een functie aldus het rapport op pag. 19:
"In principe gaat de accountant ten behoeve van (- als onderdeel van) de controle van de jaarrekening de opzet, (het bestaan) en de werking na van de administratieve organisatie, waarbij het accent ligt op de informatieverzorging in het kader van de financiële verantwoording.
Vanuit deze betrokkenheid zal de accountant in het algemeen na een aanvullend onderzoek een oordeel kunnen geven over het huidige systeem van informatieverzorging. Ook bij de beoordeling van de gewenste informatievoorziening kan de accountant een belangrijke inbreng hebben."

Het is duidelijk dat hier de rol van de accountant wordt beschreven in zijn attestfunctie voor de jaarrekening. Daarnaast komen speciale onderzoeken voor. Wij verwijzen naar NIVRA 26 Automatisering en Controle deel IV "Mededelingen door de accountant met betrekking tot de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking".

Bij de pagina's 22 en 23, het hoofdstuk "Gebruikers", merken wij ten opzichte van het vereiste kennisniveau het volgende op.

> De gebruiker dient de eindverantwoordelijkheid voor de systemen te kunnen dragen en te blijven aanvaarden. Hierbij is de noodzaak tot interne controle aanwezig. Op bepaalde punten zal algemene kennis bepaald onvoldoende zijn. Met name is specifieke kennis vereist voor (zie pag. 24) bestandsbeveiliging, programmatuurbeveiliging, controle op alsmede gebruikerstest van programma's en bestanden. Het systeem als geheel dient in elk geval centraal beheersbaar en controleerbaar te zijn (pag. 26).

Al met al een goed rapport, waard om gelezen en toegepast te worden. Wanneer aan de voorwaarden die in het rapport worden gesteld is voldaan, is de voltooiing van een adequaat controle- en beveiligingsplan niet zo moeilijk en tijdrovend meer.

TIJDSCHRIFTEN

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

Information systems curriculum recommendations.
Tijdschrift: Communications of the Association for Computing Machinery (ACM) vol 25, nr. 11.

De publicatie bevat een uitgebreid exposé met betrekking tot de totstandkoming van een concept-leerplan voor personen werkzaam in de informatica. De basisfilosofie van het leerplan is dat de afgestudeerden zich hoofdzakelijk zullen gaan bezighouden met administratieve automatisering. De verschillende richtingen waarin afgestudeerden zich verder kunnen ontwikkelen zijn:

- definiëren en plannen van informatiesystemen;
- formuleren van informatiebehoeften voor toepassingen en assisteren in het ontwerp van de systemen;
- implementeren van informatiesysteemtoepassingen;
- leiding geven aan ontwikkeling en produktie-activiteiten.

Naast deze "kunnen"-vereisten zijn drie belangrijke "kennis"vereisten gedefinieerd:

1. kennis van de technologie met betrekking tot informatiesystemen;
2. kennis van "concepts and processes";
3. kennis van organisatie- en management theorie.

De voornoemde vereisten worden in het artikel uitgewerkt naar de volgende gezichtspunten:

1. Mensen

De betrokkenen zullen vooral in staat moeten zijn om in groepsverband samen te werken en bepaalde elementen van het (toekomstige) individuele of van het groepsgedrag te onderkennen.

2. Modellen

Kennis op het gebied van operations research en het kunnen hanteren van de juiste modellen in bepaalde situaties is noodzakelijk.

3. Systemen.

De informatici zullen in staat moeten zijn om de systeemleer toe te passen in specifieke situaties (bedrijfstypen).
Voorts worden eisen gesteld op het gebied van (project-)rapportage, welke als uitgangspunt dient voor het nemen van beslissingen door het management of over de (technische) realisatie van bepaalde systemen.

4. Computers

De belangrijkste eisen liggen op het gebied van hardware, software en bestandsorganisatie.
Verder zal men in staat moeten zijn om alternatieven aan te dragen op het gebied van gegevensverwerking, gegevensopslag en communicatie-structuren.
Deze alternatieven dienen onderbouwd te zijn door zowel economisch als niet-economisch gerichte analyses.

5. Organisaties

Met betrekking tot dit gezichtspunt wordt met name gesproken over eisen welke liggen op het kennisgebied van de bedrijfskunde.
Tevens zal men in staat moeten zijn om informatiebehoeften en de invloed van toekomstige informatiesystemen op de organisatie te onderkennen.
Uitgaande van de specifieke situatie dient men in staat te zijn informatiebehoeften systematisch te verzamelen en alternatieven te ontwikkelen die in deze behoeften kunnen voorzien.

6. Maatschappelijke factoren

Van mensen, die werkzaam zijn in de informatica, wordt verwacht dat zij kunnen doorzien wat de invloed is van de informatie-technologie en informatiesystemen op het maatschappelijk leven.
Voorts dient men de hiermee verband houdende positieve en negatieve factoren te kunnen verwerken in toepasbaarheidsanalyses.

Conclusie

Uitgaande van de basisfilosofie van het concept-leerplan lijken de "kennen"- en "kunnen"-eisen, die in dit artikel worden behandeld, reëel. Echter dient te worden afgevraagd of alle personen, die werkzaam zijn in de informatica, aan deze eisen moeten voldoen.
Gezien de doelgroep van het voornoemde concept-leerplan komt het ons merkwaardig voor dat geen kenniseisen worden gesteld met betrekking tot het omgaan met facetten van interne controle en beveiliging.

Lente 1983

TWEE PRIEMGETALLEN VAN HONDERD CIJFERS: VIER MILJARD JAAR REKENEN

Bron: Elseviers Weekblad 29 mei 1983
mei 1982, S886, trefwoord B43

Alle vercijferingstechnieken die tot voor kort werden toegepast, maakten gebruik van een bepaalde manier van door elkaar husselen van letters en cijfers (het algoritme) en een sleutel, die voor iedere vercijfering apart bepaalde hoe het vercijferde bericht er uiteindelijk kwam uit te zien. Als een afluisteraar het vercijferde bericht wil ontcijferen, dan moet hij eerst uitvissen welke vercijferingstechniek (algoritme) is toegepast, en vervolgens welke sleutel is gebruikt.
Het eerste probleem is meestal vrij snel op te lossen en vaak al op voorhand bekend. In de praktijk staat het vinden van de sleutel meestal gelijk aan het zoeken naar een speld in een hooiberg. Zo is het DES-algoritme (Data Encryption Standard) algemeen bekend, alsmede ook wie het gebruiken. Maar daar heeft een afluisteraar niet zoveel aan, want voor het vercijferen heeft hij de keuze uit een quadriljoen sleutels (een 1 met 24 nullen). Ga er maar aan staan.
Toch heeft een systeem als DES een zwakte: als iemand de sleutel kent waarmee is vercijferd, kan hij het bericht ontcijferen. Dat noemt men een symmetrisch vercijfersysteem, omdat voor het vercijferen en ontcijferen dezelfde sleutel moet worden gebruikt. Daarom moet de sleutel geheim blijven. Dat geeft allemaal problemen, omdat de kwetsbaarheid van het berichtenverkeer dan wordt verplaatst naar de kwetsbaarheid van het centrale punt, waar de geheime sleutels worden bewaard en verdeeld. Een aardig voorbeeld van de wet van behoud van ellende.
In deze onbevredigende situatie is in 1976 verandering gekomen dank zij de Amerikanen Ralph Merckle, Whitfield Diffie en Martin Hellman van de Universiteit van Stanford. Zij kwamen tot een opzet waarbij de sleutel, die wordt gebruikt voor het vercijferen van de berichten openbaar kan zijn: het "public key system". Van deze vercijferingstechniek bestaan nu twee varianten. Het "valluik/rugzak"-systeem en het RSA-systeem. De afkorting RSA is afgeleid van de eerste letters van de achternamen van de mensen die het systeem hebben uitgedacht. Ronald Rivest, Adi Shamir en Leonard Adleman. Ze zijn alle drie afkomstig van het Massachusetts Institute of Technology (MIT).

Enen en nullen

Om uit te leggen hoe een "public key system" werkt, zullen wij het RSA-systeem als voorbeeld nemen. Stel dat je een bericht met dit systeem wilt vercijferen. Eerst ken je aan ieder karakter (letter, cijfer of leesteken) een getal toe. Hoe je dat doet, kun je met zijn allen afspreken. Zo bestaat er onder andere de ASCII-code, een internationale standaard voor het omzetten van alfa-numerieke tekens in binaire getallen voor het verwerken van gegevens in de computer en het versturen van gegevens via kabels en ether.

Ieder karakter wordt dan weergegeven door een serie van zeven enen en nullen. Een stuk tekst levert aldus een lange sliert enen en nullen op. Deze hak je in stukken. Hoe, kun je ook met elkaar afspreken. Vervolgens neem je een tamelijk willekeurig hulpgetal, waarmee je de getallen, die zijn ontstaan uit de sliertjes enen en nullen, tot die macht verheft. Bijvoorbeeld: is het getal dat een gedeelte van de boodschap voorstelt gelijk aan vijf en het hulpgetal twee, dan is het resultaat vijf tot de macht twee, of wel vijfentwintig. Tot zover niets ingewikkelds of geheimzinnigs aan de hand, want het hulpgetal mag iedereen weten. Nu komt de truc. Het nieuwe getal (bij ons 25) wordt gedeeld door een bijzonder getal. Na de staartdeling blijft er een restgetal over. Het getal waardoor wordt gedeeld, is de sleutel. Dat is een bijzonder getal, omdat het het produkt is van twee grote priemgetallen. Een priemgetal (zoals drie en vijf) is alleen door een en zichzelf deelbaar.
De twee priemgetallen kunnen bijvoorbeeld uit 98 en 101 cijfers bestaan. Het produkt van deze twee priemgetallen bestaat dus uit zo'n 200 cijfers en is de openbare sleutel. Ook die is aan iedereen bekend. Het uiteindelijk vercijferde bericht is het restgetal van de staartdeling. Wat is nu het geval? De afluisteraar pikt het restgetal op, kent het hulpgetal, kent de sleutel, weet precies hoe het oorspronkelijke bericht is vercijferd, maar is toch niet in staat het vercijferde bericht te ontcijferen. Daarvoor is namelijk een andere sleutel (de geheime ontcijfersleutel) nodig. Deze sleutel kun je berekenen via een bekende wiskundige vergelijking, de stelling van Fermat uit 1640. Voor deze berekening moet je echter wel beschikken over de twee priemgetallen, die als produkt de openbare vercijfersleutel hebben opgeleverd. Nou en? zou je zeggen, dan bereken je toch even die twee priemgetallen. Je kent immers hun produkt? En dàt lukt nou juist niet.
Met de huidige stand van de computertechnologie en de wiskundige theorie duurt het vinden van de priemgetallen (het ontbinden in factoren) uit een produkt van tweehonderd cijfers ongeveer vier miljard jaar. En dat is lang, te lang. Als je het bericht wilt ontcijferen lukt dat dus niet met het hulpgetal en de vercijfersleutel, die daarom beide openbaar kunnen zijn.
In de praktijk werkt het "public key"-vercijfersysteem als volgt. Iedereen, die wil dat berichten aan hem vercijferd kunnen worden verstuurd, geeft in een soort telefoonboek aan wat zijn hulpgetal en vercijfersleutel is. Hijzelf berekent via de stelling van Fermat de bijbehorende ontcijfersleutel en houdt die geheim. Het resultaat is, dat iedereen aan hem vercijferde berichten kan versturen en dat hij de enige is, die de berichten kan ontcijferen.

Waterdicht

Voor het vercijferen en ontcijferen zijn dus twee verschillende sleutels nodig. Daarom is dit een asymmetrisch vercijfersysteem. Dit systeem is waterdicht, doordat het niet mogelijk is het produkt van de twee priemgetallen binnen redelijke tijd uit elkaar te rafelen. Stel dat de computers zo veel sneller worden, dat die vier miljard jaar rekentijd voor het berekenen van beide priemgetallen uit de openbare vercijfersleutel, verschrompelt tot vier uur. Geen nood, want dan kan vrij eenvoudig de lengte van de priemgetallen en dus het produkt (de openbare vercijfersleutel) worden vergroot.

compact

Lente 1983

ESTABLISHING AN EDP AUDIT FUNCTION

EDP auditor oktober 1982

Lynn G. Good

In dit artikel wordt ingegaan op een aantal punten die van belang zijn alvorens over te gaan tot de invoering van een EDP-audit-functie.

Naarmate de automatiseringsgraad in een organisatie toeneemt, wordt deze steeds meer geconfronteerd met gevaren die de betrouwbaarheid en de continuïteit van de gegevensverwerking bedreigen. Dit noodzaakt de aanwezigheid van een EDP-audit-functie die het verantwoordelijke management moet voorzien van de nodige gegevens om de omgeving die technologisch steeds complexer wordt, te kunnen beheersen.
Het topmanagement is immers veelal onvoldoende deskundig om de gevolgen te onderkennen die de automatisering heeft ten aanzien van de eisen die gesteld moeten worden teneinde een betrouwbare gegevensverwerking, alsmede een effectief en efficiënt gebruik van de computer mogelijk te maken.

Vooral in de afgelopen jaren is veel aandacht besteed aan de noodzaak van een EDP-audit-functie. Met name werd dit veroorzaakt door het feit dat de automatiseringsmensen onvoldoende in staat waren om het verantwoordelijke management te verzekeren dat de geautomatiseerde systemen betrouwbaar waren. Immers de meeste programmeurs en systeemanalisten hebben over het algemeen een onvoldoende controle-achtergrond.

Voorafgaand aan de invoering van een EDP-audit-functie dient het hierna volgende in beschouwing te worden genomen.

Ten behoeve van een effectieve functievervulling is het van belang dat het topmanagement deze EDP-audit-functie in voldoende mate erkent en ondersteunt. De werkzaamheden dienen onafhankelijk van de automatiseringsafdeling te worden verricht en de rapportage dient rechtstreeks gericht te zijn aan een audit committee of aan de directie (topmanagement).
Evenals dit het geval is voor de werkzaamheden in de algemene controle moeten controlestandaarden en controledoelstellingen worden opgesteld. Deze controledoelstellingen hebben onder andere betrekking op het ondernemingsbeleid, de systeemgebruikers, gegevensbeveiliging, testen, performance en backup.
Voorts is het van belang om, voorafgaande aan de invoering van de EDP-audit-functie, overleg te plegen met de automatiseringsafdeling, de systeemgebruikers en met de interne controle-afdeling. Dit overleg vermindert de kans op weerstand en dient betrekking te hebben op de doelstellingen van de EDP-audit-functie.
In het kader van het vaststellen van de controledoelstellingen dienen tevens de specifieke controleverantwoordelijkheden te worden afgebakend tussen EDP-auditing, de automatiseringsafdeling, het management en de gebruikersafdelingen.

Ook zal aandacht besteed moeten worden aan de opleiding van en de eisen die men wil stellen aan mensen die betrokken worden bij de vervulling van de EDP-audit-functie.
De betreffende eisen zijn:
- kennis van de organisatie;
- kennis op het gebied van controle;
- kennis op het gebied van automatisering;
- de vaardigheid om met mensen samen te werken;
- audit-instinct.

Lynn G. Good komt tot de conclusie dat de EDP-audit-functie een waardevol "tool of management" zal worden, maar dat men bij de invoering ervan op zijn hoede moet zijn voor oppositie en conflictsituaties. Deze zijn namelijk het gevolg van veranderingen in organisaties.

N.B. Opgemerkt wordt dat binnen het NIVRA reeds enige tijd de werkgroep "opleidingseisen EDP-audit" bezig is de opleidingseisen te formuleren.

Voor u gelezen in Computable van 10 juni 1983.

Drankproblemen in Nederland

Het Medical Information Bureau (MIB) neemt het niet zo nauw met de privacy-wetgeving in de Verenigde Staten. Dit blijkt uit een onderzoek van de Amerikaanse federale handelscommissie. De MIB is een organisatie van de levensverzekeringsmaatschappijen in de VS en verzamelt persoonlijke gegevens van potentiële klanten. Zaken als hoge bloeddruk, zelfmoordneigingen of drankproblemen worden onverbiddelijk in een enorme databank vastgelegd.

De verzekeraars - niet minder dan 750, die 98 procent van alle levensverzekeringen in de VS en Canada afsluiten - gebruiken de MIB om te voorkomen, dat nieuwe cliënten worden verzekerd die hebben gelogen over hun gezondheidstoestand. Vorig jaar werd het MIB 19 miljoen keer geconsulteerd.

Dit alles gebeurt onder het motto dat de maatschappijen gerechtigd zijn zich tegen fraude te beschermen. De assuradeurs denken zelf op deze manier veertig tot vijftig keer de twaalf miljoen dollar te besparen die ze jaarlijks kwijt zijn aan de MIB.

Een loze kreet, want er zijn geen betrouwbare gegevens over hetgeen de fraude de verzekeringsindustrie kost.

De handelscommissie is overigens van mening, dat het voor het publiek te moeilijk is om achterhaalde gegevens te wijzigen. Zo wordt geweigerd medische gegevens direct aan de betrokkenen te verstrekken; de informatie wordt alleen aan artsen gegeven. Ook worden gegevensbestanden te traag bijgewerkt. Daarnaast zijn er beweringen van belangenorganisaties, dat de MIB zich niet tot alleen 'medische bewezen feiten' beperkt, maar dat ook door omwonenden of collega's van de te verzekeren persoon verstrekte informatie in de databank wordt opgenomen. De MIB heeft gegevens van twaalf miljoen Noordamerikanen opgenomen.

Komt een dergelijke situatie in Nederland ook voor?

Lente 1983

NIEUWS
Automatisering
Beveiliging
Controle

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

Automatisering

NIEUWE FUNCTIE IN DE AUTOMATISERING

Sinds 8 februari 1983 kent men in de automatiseringswereld de functie van makelaar in programmatuur. Op deze dag werd de eerste makelaar door de Arrondissementsrechtbank te Amsterdam in deze functie beëdigd.

De desbetreffende makelaar zal zich, binnen de daartoe opgerichte onderneming Eerste Nederlandse Software Makelaardij (ENSM) in Naarden gaan bezighouden met de bemiddeling bij aan- en verkoop van software alsmede de taxatie daarvan.

Bij de bemiddeling tussen koper en verkoper van software staat wat ENSM betreft voorop dat beide partijen na advies door een software-makelaar contractueel goed worden beschermd. Dit wordt onder andere bereikt - aldus ENSM - door de notariële overdracht van software bij akte.
Software-taxaties zullen voornamelijk verricht worden op twee gebieden:
a. financiële taxaties waarbij in een aantal gevallen toepassingsprogrammatuur geactiveerd zal kunnen worden en
b. operationele evaluatie van programmatuur waarbij ook het auditing-facet naar voren komt.

Uit: Financieel en Administratief Management, 17 februari 1983 (gewijzigd)

IBM systeem 38

In dit nummer van Compact wordt door A.H.C. Koedijk al de nodige aandacht aan dit systeem besteed. Ook in Computable van 11 maart 1983 werden enkele kolommen aan dit systeem gewijd. Het volgende lijstje met tips voor toekomstige gebruikers van Systeem 38 hieruit willen wij u niet onthouden.

1. De toepassing opnieuw ontwerpen en herschrijven.
2. Goede studie van de mogelijkheden van het systeem maken.
3. Goede standaards aanleggen.
4. Zorgen voor goed opgeleide mensen.
5. Eerst programmeringsgereedschap maken.

6. Veel 'default' waarden nemen.
7. Niet te veel in één keer willen doen.
8. Alle fysieke 'files' extern definiëren.
9. 'Source achieve' pakket gebruiken.
10. Bomp-files (Bill of material processor files).
11. Beveiligingsplan maken.
12. In het eerste jaar een vaste systeemprogrammeur nemen.
13. Gebruik de ervaringen van anderen.
14. Bij gebruik van een 3370-schijfgeheugen ook een magneetbandeenheid gebruiken.
15. Zoveel mogelijk interactief overdag en 'batch' 's nachts.
16. Direct een magneetbandsysteem aan de configuratie toevoegen.

Met betrekking tot enkele punten ontvingen wij aanvullend commentaar van A.H.C. Koedijk.

a. Ad 1. Dit zal niet altijd haalbaar zijn als gevolg van beperkte ontwikkelingscapaciteit en/of financiën. Het gevolg als je het niet doet is wel, dat goede features van de 38 voor recht-over geconverteerde applicaties buiten gebruik blijven (met name extern gedefinieerde files).

b. Ad 2, 3 en 4. Hieruit blijkt, dat de complexiteit van de 38 wordt onderkend.

c. Ad 5. Is in niet geringe mate standaard aanwezig.

Gedragscode voor registerinformatici

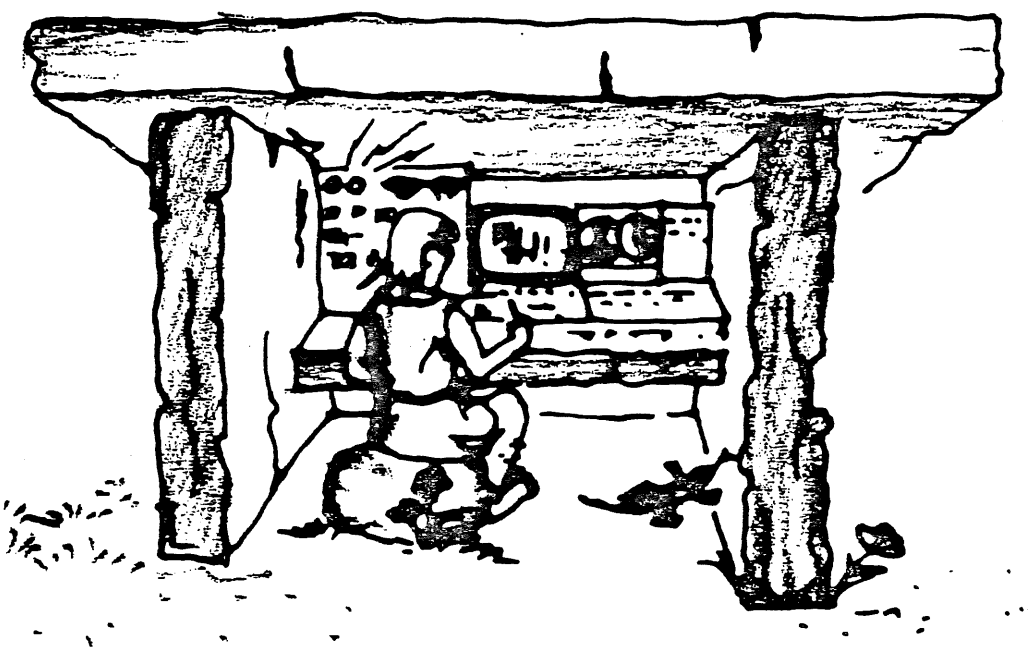
In 1978 werd door het bestuur van het Nederlands Genootschap voor Informatica (NGI) een Commissie Gedragscode ingesteld, die ruim een jaar geleden een tweede concept van een gedragscode voor informatici aan het NGI-bestuur heeft aangeboden. In dit concept zijn reacties en opmerkingen verwerkt op het eerste concept alsmede op een beschouwend artikel over een gedragscode, dat verschenen is in het maandblad Informatie van november 1980. Inmiddels is een Invoeringsgroep geformeerd, die de verdere activiteiten van de invoering van de code moet coördineren. Pogingen van de Invoeringsgroep om een discussie over de gedragscode onder een grote groep informatici op gang te brengen leverden niet het gewenste resultaat. Door publicatie van de gedragscode met toelichtingen in het blad Computable van 18 maart 1983 samen met een oproep aan informatici die bereid zijn om zich als register-informaticus te laten inschrijven hoopt men de belangstelling voor de gedragscode te peilen. Tevens zullen ontvangen commentaren op de gedragscode in Computable worden gepubliceerd.

Uit: Computable, 18 maart 1983
(samenvatting)

Beveiliging

In het nummer van 2 maart 1983 besteedt het blad De Computerkrant aandacht aan de bouwkundige facetten van het computercentrum in het artikel met de volgende titel:

"OOK UW GEBOUW BEHOEFT AANDACHT"



Uitgangspunt voor het desbetreffende artikel was een advertentie waarin de vraag werd gesteld: "Is uw gebouw net zo up to date als uw computer?". De Computerkrant stelt dat EDP-managers andere zorgen hebben dan zich te bekommeren om de huisvesting van hun computercentra. Deze dagelijkse beslommeringen betreffen de produktie, het onderhoud en de renovatie van bestanden en informatiesystemen, alsmede de uitbreidingen van de programmapakketten. Pas bij erkende problemen als gevolg van explosieve groei, stagnerende verwerking, calamiteiten, e.d. wordt het zoeklicht op de huisvesting gericht.

Ons inziens mag het bovenstaande niet zo algemeen worden gesteld. Uit ervaring blijkt dat er gunstige uitzonderingen zijn. Desondanks dient men steeds alert te zijn op interne en externe factoren die eisen aan de bouwkundige voorzieningen van computercentra stellen dan wel wijzigen. Om deze reden lijkt het ons nuttig door middel van een uittreksel uit bovengenoemd artikel een aantal facetten onder uw aandacht te brengen.

Veelzijdigheid van eisen

Aan het computercentrum als gebouw worden een aantal eisen gesteld die ver uitgaan boven die voor andere gebouwen, zoals kantoren. Markante voorbeelden zijn:

. Eisen aan de infrastructuur.
Niet alleen de routing van de werkzaamheden is van belang, maar ook de aanvoer van de gegevensdragers, het bekabelingsverloop, de ventilatievoorziening, etc.

. Eisen aan het klimaat.
De relatief hoge temperatuur en de daarbij geëiste en heersende vochtigheid hebben hun repercussies op de bouwfysische opbouw van de omhulling zoals akoestiek, licht, warmte, ventialtie. Bovendien moet voldaan worden aan eisen van water-, wind- en stofdichtheid.

. Eisen met betrekking tot of voortkomend uit de geïnstalleerde apparatuur. Noodzakelijke ruimte rond de eenheden, maximaal toegestane lengtes van signaal- en voedingskabels, etc. zijn vaak een zaak van computerleveranciers.
Anders ligt dit bij eisen ten aanzien van stofhinder, trillingen, temperatuurfluctuaties, etc.
Daarnaast spelen technische eisen als vloerbelasting, statische elektriciteit een rol.

. Eisen aan de veiligheid.
Deze eisen dienen ingebed te zijn in een veel ruimer organisatorisch kader. Procedures, instructies, etc. betreffen met name de gebieden:
  . Brandbeheersing.
    Vluchtwegen; moeilijk ontvlambare materialen die bij ontvlammen geen corrosieve/giftige gassen afscheiden.
    Brandwerendheid van constructies, signalering, doormelding, blussing direct bij de brandhaard zijn hierbij hot-items.
    Overigens is dit wel één van de gebieden waarvoor normen gelden. De NPR 3900 "Brandbeveiliging van gebouwen - computerafdelingen" heeft hiertoe een aanzet gegeven.
  . Toegangsbeheersing in samenhang met brandbeheersing en inbraakveiligheid.
  . De inbraakveiligheid sec.
  . Het beheer, de opslag van de backup van bestanden en informatiedragers.

De mate waarin en de wijze waarop aan bovengenoemde eisen voldaan zal worden, dient met behulp van een risico-analyse te worden bepaald. Het is gewenst dat in deze analyse naast de fysieke beveiliging ook de volgende deelgebieden geïntegreerd zijn:

1. Betrouwbaarheid van de systeemprogrammatuur.
2. Betrouwbaarheid van de applicatieprogrammatuur.
3. Kwaliteit van de automatiseringsorganisatie.
4. Kwaliteit van de gebruikersorganisatie.

De uit de risico-analyse voortkomende eisen met betrekking tot de fysieke beveiliging moeten vervolgens in overleg met een veelheid aan betrokken partijen in het bouwproces worden gerealiseerd. Daarbij dient men bovendien rekening te houden met een uitgebreid scala van wetten en verordeningen. Het komt daarom nog wel eens voor, dat goed bedoelde maar in feite gebrekkige oplossingen worden gerealiseerd.
Het artikel geeft enkele sprekende praktijkvoorbeelden:

- Een niet voor water gevrijwaarde computerzaal:
  - Geen waterkoeling onder computervloer ten behoeve van waterkoeling CPU's.
  - Hemelwaterafvoer door computerzaal, riolering boven kluis.
  - Geen voorzieningen ten behoeve van lekwater van bovengelegen verdiepingen.
  - Condensatie op de ruiten.

- Brandveiligheid:
  - Wandbekleding op basis van pvc.
  - Brandwerendheid constructie kluis minder dan 1 uur.
  - Geen brandkleppen, geen dichtgezette sparingen in brandscheidingen.

- Lay-out:
  - Onvoldoende hoogte.
  - Ongelukkige airflow.
  - Foutieve sluisprincipes in ringbeveiliging.

- Constructies:
  - Trillingsgevoelige vloer.
  - Foutieve bouwfysische gevelopbouw.

- Uitvoering:
  - Het niet aanbrengen van stofschermen tijdens de uitvoering.
  - Trilling veroorzakende sloop- en heiwerken (niet afgeschermd in bestek).

- Organisatie:
  - Geen gebruikersgids van geïnstalleerde systemen ter behoeve van huishoudelijke dienst, opdrachtgever, etc.
  - Ongeautoriseerde toegang van een gedeelte van het personeel tot informatie- en bestandsopslag.

Vervolgens wordt een tweetal hulpmiddelen aangereikt om bovengenoemde situaties te voorkomen.

- Het opstellen van een Programma van Eisen (PvE).
  Zonder een PvE komt geen goed project tot stand. Het PvE zal het totaal van wensen en verlangens van de opdrachtgever moeten omvatten. Een goede lay-out met optimale verbindingen en adequate ruimtelijke indeling (zoals de verschillende ruimten) vormen het resultaat van een goed uitgewerkt programma van eisen.

- Een installatie-ontwerp.
  Een goed installatie-ontwerp komt tot stand door de wisselwerking: gebouw ontwerp-bouwfysica-installatie-ontwerp. Nog te veel komt het voor dat installaties stiefmoederlijk in de ontwerpfase worden behandeld; letterlijk en figuurlijk moet men zich in bochten wringen om de installaties in het gebouw te doen integreren.

Wij merken hierbij nog op dat de gebruiker c.q. opdrachtgever over deskundigheid op een aantal terreinen zal dienen te beschikken, wil hij tot een evenwichtig en goed doordacht plan van eisen respectievelijk installatie-ontwerp komen. In veel gevallen zal hij zich daarom moeten laten bijstaan door specialisten uit meerdere disciplines.

PAKKET VOOR UITBREIDING CICS TOEGANGSBEVEILIGING

Oxford Software Corporation recently announced the release of a package called COSS (CICS On-Line Security System). This interactive security package, designed to work on IBM mainframes, provides for improved levels of data security in a CICS environment. COSS can be divided into four main areas:

Protected Resources

It can be used to protect all CICS resources, including resources and events defined by the user.

Installation/Implementation

It can be installed in less than one hour. It requires no modifications of CICS or the operating system. It can be tested without disrupting existing on-line operations.
Further, it should not cause any noticeable effect on CICS response time.

Administration/Management

It operates in an on-line mode. All changes in the security environment can be made through an on-line terminal. Terminal operation is menu-driven and designed to be user friendly. The security system was also designed to enforce a separation of operator functions.

Enforcement/Reporting

A combination of eight classes of operator restrictions coupled with multi-level password security gives COSS the capability for preventing unauthorized access. The system also provides:

- An automatic audit trail of all security modifications
- Immediate reporting of security violations
- Comprehensive logging of activities
- Monitoring of critical resources
- Day/time constraints on users or processing
- Automatic terminal sign-on/sign-off
- Encryption of all profiles, packages, passwords.

Uit: Edpacs, februari 1983

Controle

In De Accountant van maart 1983 werd door Prof. L.C. van Zutphen, R.A. uitgebreid aandacht besteed aan de IFAC ontwerprichtlijn nr. 17 over Computer-Assisted Audit Techniques (CAAT's). Uit onze praktijk is gebleken, dat CAAT's bij het samenstellen van controleprogramma's vaak niet die aandacht krijgen die zij verdienen.
Zo wordt onvoldoende of in het geheel niet onderzocht of door het toepassen van CAAT's de effectiviteit en de efficiency van de controleprocedures kunnen worden verbeterd. Ook komt het voor, dat wanneer CAAT's moeten worden benut voor het verzamelen van bewijsmateriaal, de mogelijkheden van de CAAT's niet ten volle worden benut.

Door overname van gedeelten uit het bovengenoemde artikel willen wij de aandacht weer eens op de CAAT's richten.

In het ontwerp worden (slechts) twee meer algemeen bekende en toegepaste vormen van CAAT's behandeld, te weten controleprogrammatuur (audit software) en testgevallen (test data). Hoewel het aanvankelijk wel in de bedoeling lag werd afgezien van de bespreking van andere, vaak minder bekende en toegepaste vormen van computergebruik door de accountant zoals:
- Review of program logic.
- Program comparison.
- Parallel simulation.
- Gebruik timesharing.
- Gebruik van job accounting data.
- Embedded audit modules.

Controleprogrammatuur wordt omschreven als een samenstel van computerprogramma's dat door de accountant kan worden gebruikt als onderdeel van zijn controleprogramma, teneinde gegevens uit het (financiële) systeem van de huishouding, die in het kader van de controle van betekenis worden geacht, met behulp van de computer te kunnen verwerken.
In nr. 17 worden drie soorten controleprogrammatuur onderscheiden en omschreven:
- standaardprogramma's (package programs)
- speciaal geschreven programma's (purpose written programs)
- hulpprogramma's (utility programs).

Testgevallen worden omschreven als een controleprocedure waarbij gegevens (bijvoorbeeld een selectie van transacties) in het computersysteem van de huishouding worden ingevoerd en de verkregen verwerkingsresultaten worden vergeleken met vooraf bepaalde uitkomsten.

Voorbeelden van deze CAAT zijn:

- Testgevallen die door de accountant worden ontwikkeld om de werking van bepaalde geprogrammeerde controles te toetsen; bijvoorbeeld een geautomatiseerde autorisatieprocedure bij on-line-systemen.

- Ook uit de reeds door de huishouding verwerkte transacties kan een selectie van testgevallen worden gemaakt om de goede werking van bepaalde computerprogramma's of van specifieke deelroutines te controleren; bijvoorbeeld de berekening van afschrijvingen, kortingen, e.d.

- In de hiervoor genoemde voorbeelden worden de testgevallen in het algemeen in een aparte verwerkingsgang doorgevoerd. Daarnaast kunnen testgevallen ook tijdens de normale computerverwerking van de huishouding worden ingevoerd met behulp van een geïntegreerde testfaciliteit (Integrated Test Facility).
  Bij deze - ook in ons land al lang bekende maar nog weinig toegepaste - techniek wordt een zogenaamde "dummy unit" (bijvoorbeeld een afdeling of een werknemer) gecreëerd waarop mutaties worden verwerkt met behulp van de tijdens de computerverwerking actieve versies van het toepassingsprogramma.
  Het is bij toepassing van ITF noodzakelijk dat de accountant ervoor zorgt dat de door hem ingevoerde testmutaties direct na afloop van de controleprocedure uit het informatiesysteem worden verwijderd.

Gebruik van CAAT's

Waar kunnen CAAT's in het proces van accountantscontrole nu een zinvolle toepassing vinden? in paragraaf 7 van de guideline worden hiervan de volgende voorbeelden gegeven:
- het verifiëren van mutaties en saldi - met behulp van CAAT's kunnen posten in een computerbestand worden gecontroleerd op bepaalde condities (bijvoorbeeld ouderdom, grootte) en/of voor nader onderzoek worden afgedrukt;
- het verrichten van cijferbeoordeling - CAAT's kunnen bijvoorbeeld behulpzaam zijn bij het opsporen van bijzondere posten of fluctuaties in bepaalde tijdreeksen;
- controle op de goede werking van toepassingsgerichte controles; bijvoorbeeld het testen van een geprogrammeerde controle.

Overwegingen bij het gebruik van CAAT's

Maar liefst negen paragrafen van draft nr. 17 zijn gewijd aan factoren en overwegingen die de keuze van het al of niet gebruiken van CAAT's - in combinatie met niet geautomatiseerde controleprocedures - bepalen. De volgende zes punten worden ter beantwoording van deze vraag naar voren gebracht:

- de automatiseringskennis, de -deskundigheid en ervaring van de accountant;
- de beschikbaarheid van de benodigde computerfaciliteiten (configuratie en capaciteit);
- de praktische (on)uitvoerbaarheid van handmatige controleprocedures;
- mogelijke verbeteringen van effectiviteit en efficiency van de controlewerkzaamheden door toepassing van CAAT's;
- de tijdplanning, rekening houdend met de geldende bewaartermijnen van bestanden;
- de kostenafweging.

Een enkele opmerking ter toelichting.
Een praktische omstandigheid, die de accountant welhaast forceert tot het gebruik maken van CAAT's, is het ontbreken van voldoende controle-informatie in voor de mens direct leesbare vorm. Enkele voorbeelden:

. Orderformulieren kunnen ontbreken bij on-line invoer van verkooptransacties.

. Controleerbare vastleggingen (audit trails) kunnen voor een belangrijk deel slechts in machinaal leesbare vorm aanwezig zijn.

. Eenmaal ingevoerd kan "matching" van inkoopfacturen en goederenontvangstbonnen door de computer plaatsvinden.

. Van door de computer uitgevoerde controles op invoer en verwerking zoals bestaanbaarheid of kredietwaardigheidscontroles worden slechts de door de computer geconstateerde fouten, afwijkingen of uitzonderingen afgedrukt.

In al deze gevallen ontbreekt voor de accountant direct zichtbare informatie waaruit blijkt dat alle transacties ook volledig, juist en tijdig zijn verwerkt.
In het algemeen wordt de efficiency van het controlewerk door de toepassing van CAAT's opgevoerd.
Eenmaal geprogrammeerd kunnen veel meer posten en in een veel hoger tempo worden gecontroleerd dan met behulp van handmatige methodes mogelijk zou zijn.
Ook wat de effectiviteit van de controle betreft wint de computer het bij grotere volumes van de mens qua accuratesse.

Echter voor beoordelingswerk gebaseerd op kritisch en associatief vermogen kan men bij de computer (nog) niet terecht.

In de kostenafwegingen dienen alle kostenelementen van de CAAT-toepassing te worden betrokken. Bij nadere beschouwing kunnen de totale kosten en vooral het initiële deel daarvan nogal oplopen.

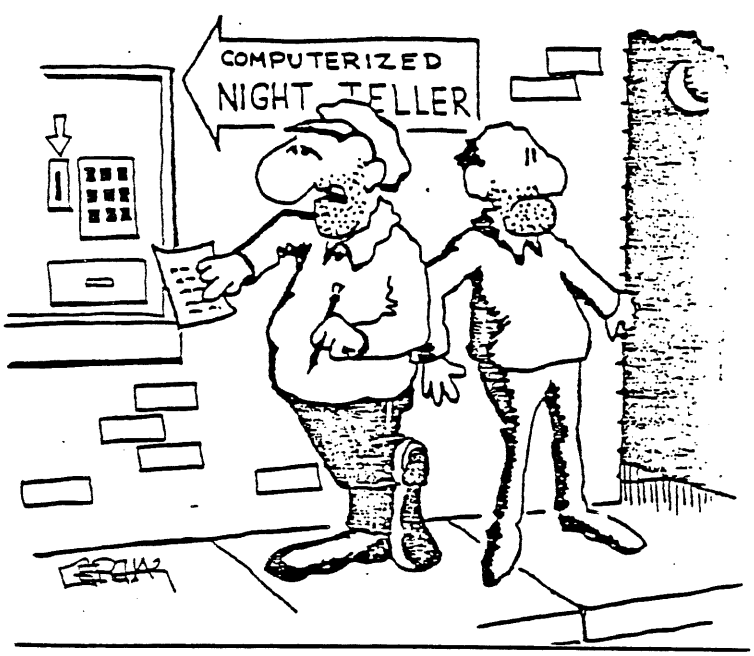
Kosten kunnen ontstaan door:
- tijd benodigd voor planning, ontwerp en uitwerking van de CAAT;
- uren voor technische review van en assistentie bij het CAAT-ontwerp;
- ontwerp en drukken van computerformulieren (bijvoorbeeld saldo-biljetten);
- invoerpreparatie en -controle;
- benodigde computertijd.

Anderzijds kunnen hoge ontwikkelingskosten bij herhaald CAAT-gebruik in vergelijking tot de kosten bij handmatige uitvoering van bepaalde controleprocedures snel worden terugverdiend.

Reactie van lezers van Compact op de inhoud van rubriek ABC

Op de inhoud van Compact nr. 30, blz. 79/80 is een reactie van de heer F. Schwarz binnengekomen. Het betreft de bespreking van het artikel "The Perils of accepting packages in source code" door Thomas A. Browdy. F. Schwarz geeft in overweging om de software te beschermen als volgt:

> Source-code bij de notaris deponeren.
> Wel zorgen dat de programmatuur steeds wordt bijgewerkt.



'Hey, Fred . . . How Do You Spell "Hold-Up" in Cobol?'

ONDERWIJS

Cursussen 83/84

1. In maart 1983 is de brochure voor externe cursussen ter beschikking gekomen. Het betreft het cursusseizoen mei 1983 tot en met januari 1984. De cursusbrochure is speciaal samengesteld ten behoeve van onze cliënten. U kunt extra exemplaren aanvragen bij:
   Klynveld Kraayenhof & Co.
   Bureau Opleidingen, tel. 020 - 5461243,
   waar u kunt vragen naar mw. Pien Schepel,
   eventueel schriftelijk
   Postbus 7137, 1007 JC AMSTERDAM

   Cliënten en niet-cliënten van KKC kunnen zich ook rechtstreeks tot ons Bureau Opleidingen wenden.
   De brochures worden u gaarne toegezonden.

2. De cursussen Administratieve Organisatie en Controleleer verheugen zich als regel in een grote belangstelling. De cursussen zijn steeds volgeboekt. Het is derhalve raadzaam tijdig uw aanmelding in te zenden.

   Kleinschalige automatisering is door KKC ontwikkeld en wordt ook door het NIVRA gegeven. Via dit instituut hebben inmiddels 500 cursisten deze cursus gevolgd.

   Voor de succesvolle cursus uit het verleden Computer Controls zijn momenteel weinig aanmeldingen.
   Het is echter een cursus die inmiddels ten opzichte van de oorspronkelijke cursus is uitgebreid met een aantal nieuwe onderdelen zoals lezingen over testen gevolgd door uitvoeren van de test, conversie, operatingsystems, bibliotheeksystemen, programmabeheer, beveiliging, risico-analyse, programmeerbare controles, check digits, alsmede korte inleiding over Cobol. De cursus vormt een grondige aanzet voor de cursussen data-entry/batch en zeker voor de cursus geïntegreerde gegevensverwerking.

   Data-entry/batch is geheel nieuw van opzet.
   Slechts enkele delen herinneren aan de vroeger bekende zogenaamde batchmodule.

   De cursus accountantscontrole bij Geïntegreerde Gegevensverwerking is steeds vol bezet: moeilijk maar met dankbare cursisten.

   Vervolgens:
   - Workshop samenwerken in projecten.
   - Managen van datacenters.

Deze beide opleidingen worden geheel of gedeeltelijk gegeven met behulp van docenten van KKC. Het belang van deze cursussen in het kader van automatisering en controle is gelegen in het feit dat in deze opleidingen van dezelfde denktrant respectievelijk woordkeuze gebruik gemaakt wordt als bij de daarop aansluitende A.C.-cursussen.

De overige cursussen (Inkomstenbelasting, Vennootschapsbelasting, Internationaal Belastingsrecht en Pensioenen) zijn voor dit seizoen voor het eerst als open cursus aangeboden. Daarvoor zijn zij als regel meerdere malen als in-house-cursus gepresenteerd. Ook over deze laatste vorm is overleg mogelijk, waarvoor verwezen wordt naar de nieuwe brochure.

3. In de cursusbrochure vindt u de automatiseringscursussen in opklimmende graad van moeilijkheid. Om u te helpen met het maken van de juiste keuze hebben wij enige vragen opgesteld:
Gesteld u ontvangt de vraag van een cliënt om (bij)scholing. De volgende vragen zouden dienstig kunnen zijn.

Vraag 1: Heeft u enige opleiding gevolgd in automatisering?
zo ja: zie vraag 2
zo neen: hebt u overwogen een cursus bij uw computerleverancier te volgen zoals bijvoorbeeld de geprogrammeerde cursus van IBM, respectievelijk heeft u "Basiskennis Informatica" van P. Overkleeft nagelezen?.

Vraag 2: Heeft u enige scholing op het gebied van administratieve of interne organisatie?
zo ja: zie vraag 3
zo neen: cursus AO is voor u zeer geschikt.

Vraag 3: Heeft u een beeld van de hoofdlijnen accountantscontrole met het daarbij behorende instrumentarium van controlemiddelen en/of methoden?
zo ja: zie vraag 4
zo neen: inleiding controleleer in 5 dagen.

Vraag 4: Op welk gebied wenst u verdere bekwaamheid?
Onze opleiding houdt een 3-tal richtingen in:
a. Meer kennis op het gebied van automatisering zoals:
   - workshop samenwerken in automatiseringsprojecten
   - het managen van datacenters.
b. Meer kennis op het gebied van automatisering en controle:
   - computer controls
   - data-entry/batchverwerking
   - kleinschalige automatisering
   - geïntegreerde gegevensverwerking.
c. Meer kennis op het gebied van leiding geven:
   - management
   - management en organisatiebeschrijvingen
   - financieel management.

Het is niet noodzakelijk om alle cursussen direct achter elkaar te volgen. Indien u het gewenst acht de cursussen in 1 jaar te volgen kan dat. De data zijn zodanig gekozen, dat een verantwoorde scholing met voldoende tussenruimten kan plaatsvinden.
Welke richting kiest u?

Tenslotte

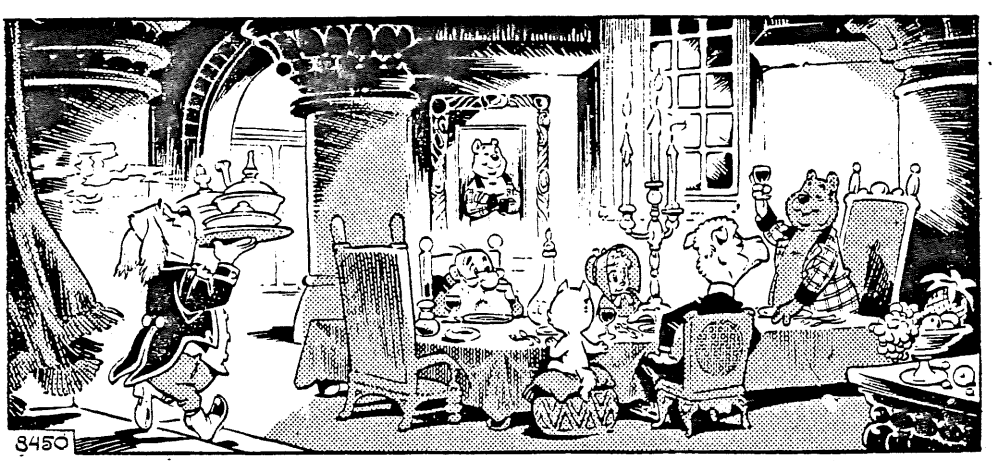
Wat niet in de cursusbrochure staat zijn de zeer specifieke automatisering en controle-opleidingen:

a. Opleiding tot EDP-auditor; hiervoor is slechts een uiterst beperkt aantal plaatsen beschikbaar in de zogenaamde A.C.-opleiding.

b. Aparte cursussen gericht op een specifiek gebied. In 1982 werden de volgende cursussen gehouden:
Data Base Management System IMS (1x);
Operating system MVS (2x).
Bij voldoende belangstelling kunnen ook op andere specifieke deelgebieden cursussen gegeven worden, respectievelijk seminars gehouden.

De cursusbrochure 1983/1984 geldt voor het cursusseizoen mei 1983 tot en met januari 1984.

Inlichtingen bij de Redactie van Compact.



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