AC AZ

compact

COMPUTER EN ACCOUNTANT

UIT DE INHOUD

Klynveld Kraayenhof & Co.
ACCOUNTANTS

Internationaal KMG Klynveld Main Goerdeler

NUMMER 29 9E JAARGANG HERFST 1982

COMPUTER EN ACCOUNTANT

INHOUDSOPGAVE

NUMMER 29 9E JAARGANG HERFST 1982

Automatisering en Controle-groep Redactie Compact

Uw persoonlijk oordeel over de inhoud van Compact
Computer en Accountant nummer 29 9e jaargang herfst 1982

Dit jaargetijde hebben wij het niet gehaald. Het herfstnummer komt u eerst nu op 6 januari 1983 in de winter onder ogen. Was u Compact reeds wachtende? Wij willen dit graag weten.

Wilt u het teken (X) plaatsen in één van deze kolommen

	JA	NEEN
1. Wilt u aan de enquete medewerking verlenen? Zo neen, ga naar vraag 7		

2. Zo ja, uit welken hoofde leest u Compact?

2.1 - behoort u tot KKC/KMG?
zo neen, ga naar vraag 2.2

A.C.-kern		
A.C-part-timer		
Organisatie groep		
Algemene sector		
Binnendienst		
Centrale dienst		

- hebt u het blad aan cliënten laten zien?
Ga naar vraag 3

2.2 bent u

- lid van interne accountantsdienst		
- lid van EDP-audit staf		
- gebruiker van systemen		
- lid van de leiding van uw organisatie		
hebt u		
- een automatiseringsfunctie		
- een documentatiefunctie		
- een secretariaatsfunctie		
- een researchfunctie		
- een regelende functie		
of bekleedt u een andere functie		
- bij het onderwijs		
- elders		

3. Om enig oordeel te vormen over uw kennisniveau:

	bent u	studeert u voor
3.1 registeraccountant		
administratie consulent		
organisatie-adviseur		
administrateur		
raadgevend ingenieur of vergelijkbare discipline		
systeemanalist/programmeur met AMBI		

3.2 - volgde u een "automatiserings- en controlecursus" bij KKC		
- volgde u de "A.C.-opleiding" bij KKC		
- andere opleidingen op gebied van automatisering		
3.3 Leest u regelmatig vakliteratuur op het gebied van automatisering en controle		

Voor het geven van uw oordeel voor de vragen 4 en 5, zowel naar algemeenheid als naar nuance gelieve u gebruik te maken van de volgende symbolen:
G (= goed),B (= bevredigend), M (= matig) en S (= slecht).

	oordeel	nuancering naar aspect			
	in algemeenheid	actualiteit	kwaliteit	diepgang	toepasbaarheid
4. Compact nummer 29 in zijn geheel.					
5. Artikelen en rubrieken:					
5.1 Anticiperen op conversie					
5.2 Interne controle-aspecten bij een systeem voor financiële administratie op een minicomputer					
5.3 Bescherming software tegen ongeautoriseerd copiëren					
5.4 Computer related risks					
5.5 Culprit library of routines: EDP-auditor					
5.6 Boeken					
5.7 Tijdschriften					
5.8 ABC-Nieuws					
5.9 Onderwijs					

6.1 Heeft u tot nu toe onderwerpen gemist in Compact ☐ ☐
Zo ja, welke: 1. .....
2. .....
3. .....
4. .....

6.2 Welke onderwerpen zoudt u in Compact behandeld willen zien
1. .....
2. .....
3. .....
4. .....

7. Wij stellen het op prijs de reden te vernemen waarom u geen medewerking wilt vernemen.
.....

8. Desgewenst kunt u hieronder uw naam vermelden

.....

eventueel uw adres .....

.....

Hartelijk dank voor uw medewerking. Wilt u ons het formulier in gesloten enveloppe met antwoordnummer (bijgaand) toezenden.
De uitkomsten van het onderzoek zullen wij in Compact publiceren.
Dit op een zodanige wijze dat de privacy van de individuele gegevens gewaarborgd blijft. Wij verzoeken u het ingevulde formulier uiterlijk 28 februari 1983 terug te zenden.

compact

Herfst 1982

VAN DE REDACTIE

Geachte lezer,

Reeds geruime tijd hebben wij u Compact toegezonden. Er is ons als redactie, als drager van de eindverantwoordelijkheid voor de inhoud, veel aangelegen dat Compact beantwoordt aan zijn doel. Dit zowel ten aanzien van de actualiteit, de kwaliteit, de diepgang en de toepasbaarheid van de artikelen.

Ten einde een indruk te verkrijgen of de redactie van Compact op de goede weg is, willen wij u ook vragen in welke hoedanigheid u Compact leest.
Bij dit nummer met "Elck wat wils" hebben wij een beoordelingsformulier bijgesloten met het verzoek dit ingevuld aan ons terug te zenden.
Wij stellen uw medewerking zeer op prijs.

De Automatisering en Controle-groep wenst een ieder een Voorspoedig 1983

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

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

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

Redactie:
Drs. J.E. Huizenga,
A.W. Neisingh en
Prof. D. Steeman.

Kopij kunt U inleveren bij de secretaris van de redactie:
H.J.M. van der Wielen.
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 redactie-secretaris, evenwel zolang de voorraad strekt.

ANTICIPEREN OP CONVERSIE

door A. van der Drift

1. Inleiding

In Compact nummer 24, 8e jaargang zomer 1981, verscheen een artikel over de problematiek van conversie van toepassingsprogrammatuur. Onder conversie werd verstaan het wijzigen van bestaande geautomatiseerde toepassingsprogramma's (applicaties), zonder dat het gegevensverwerkend proces en de informatievoorziening voor de gebruiker veranderde; in wezen dus een verandering in de syntax van de applicaties.
Een conversie is vereist indien de omgeving, waarin de applicatie wordt uitgevoerd, verandert. Met omgeving wordt in dit verband bedoeld:

- de hardware;
- het Operating System;
- de bestandsorganisatie;
- de Tele-Processing monitor.

Uit het voornoemde artikel ontstaat terecht de indruk dat conversie tijdrovend, complex en omvangrijk kan zijn. In het artikel is dan ook voor een belangrijk deel ingegaan op de organisatie van conversie.

In dit artikel zal echter voornamelijk worden ingegaan op de betekenis van programmaconversie en op de systeemontwikkeling, waarbij maatregelen kunnen worden getroffen ten einde een mogelijke conversie te vergemakkelijken.

Doordat conversie, zoals hierboven gedefinieerd, geen directe resultaatsverbetering in de gegevensverwerking beoogt (geen andere gegevens voor in- en uitvoer), kunnen conversiewerkzaamheden als belastend worden ervaren door de gebruikersorganisatie. Dit ligt aan de mate van verstoring welke zij ondervinden als gevolg van de conversie in het bestaande te converteren geautomatiseerd proces. Op zijn minst dienen zij ook deel te nemen aan de acceptatietest van de geconverteerde toepassingen. Eventueel dienen zij te leren werken met veranderde hardware zoals bijvoorbeeld terminals, e.d. De mate van inspanning voor zowel de gebruikers- als de automatiseringsorganisatie hangt sterk af van de aard van de verandering in de omgeving en de kwaliteit en opzet van de te converteren applicaties. De veranderingen in de omgeving (daarmee de conversie) kunnen echter in het belang zijn van de gebruikers. De nieuwe produkten (de veranderde hardware en software) zouden onder meer betere mogelijkheden kunnen bieden met betrekking tot:

- De tijdigheid van gegevensverwerking;
  een snellere computer of T.P.-monitor zou bijvoorbeeld een betere performance kunnen bieden aan de gebruiker-achter-de-terminal of de performance kunnen handhaven bij een grotere belasting door het in gebruik nemen van nieuwe applicaties.

- De continuïteit van gegevensverwerking;
  een voorbeeld hiervan is de conversie die de PTT heeft ingezet met betrekking tot het gebruik van invulformulieren in plaats van ponskaarten. Dit omdat de betrokken hardware-leverancier in de toekomst geen ponskaartapparatuur meer zal leveren c.q. onderhouden in geval van storing.
- De uitbreidbaarheid;
  door gebruik van andere hardware of software kan men in staat worden gesteld bepaalde uitbreidingen te doen, bijvoorbeeld het koppelen van computers.
- De integriteit, beveiliging en reconstructie;
  andere produkten zouden hiervoor wellicht betere mogelijkheden kunnen bieden.

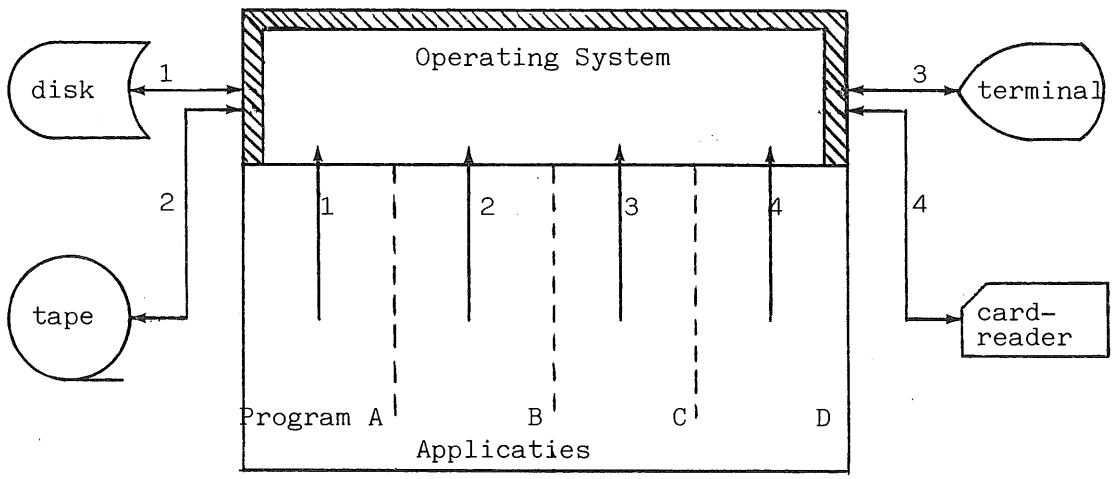
Door de snelle ontwikkelingen van hardware en software - als gevolg waarvan leveranciers ondernemingen dwingen c.q. verleiden tot het veranderen van hun omgeving - is de conversieproblematiek duidelijk een gegeven waarmee geleefd en waarop geanticipeerd dient te worden. Het verdient derhalve aanbeveling toekomstige conversieproblemen te minimaliseren door bij de systeemontwikkeling hiermee rekening te houden. Dit kan enerzijds worden bereikt door een kwalitatief goede bouw in de vorm van gestructureerde en gedocumenteerde applicaties (onderhoudbaarheidsaspect); anderzijds door een mate van onafhankelijkheid te bewerkstelligen tussen de applicaties en de omgeving. Op dit laatste wordt in de navolgende hoofdstukken uitvoerig ingegaan.

2. Hardware

Het streven van een onderneming zal er in het algemeen op zijn gericht om één groeipad te kiezen.
Onder groeipad wordt in dit kader verstaan: een door leveranciers gevolgde produktlijn met groeimogelijkheden inzake hardware en daarop aangepaste software.
Koppelingen tussen hardware van één leverancier zijn vaak gemakkelijker tot stand te brengen dan tussen hardware van verschillende leveranciers. Dit kan betekenen dat, indien ten behoeve van toekomstige ontwikkelingen een koppeling tot stand moet komen, men eerst van hardware zal moeten veranderen als deze niet koppelbaar blijkt te zijn. Dit zou een verandering betekenen in de omgeving van de reeds bestaande applicaties hetgeen kan leiden tot conversie.

In het algemeen functioneert een computer met behulp van een Operating System (O.S.), dat de applicaties o.a. minder hardwaregevoelig maakt. Vele hardware-gebonden functies voert het O.S. op verzoek van applicaties uit. Derhalve vindt communicatie plaats tussen de applicaties en het O.S. en vormt dit O.S. een soort interface tussen de applicaties en de hardware. Een applicatie kan, zonder te worden aangepast, worden uitgevoerd op bijvoorbeeld een IBM 370/125 en een IBM 3033 als ook op een Amdahl, indien op deze computers gebruik wordt gemaakt van hetzelfde O.S.

Figuur 1 geeft de toepassing van het O.S. in schemavorm weer. De hardware wordt aangegeven door middel van de randapparatuursymbolen en het gearceerde gedeelte.



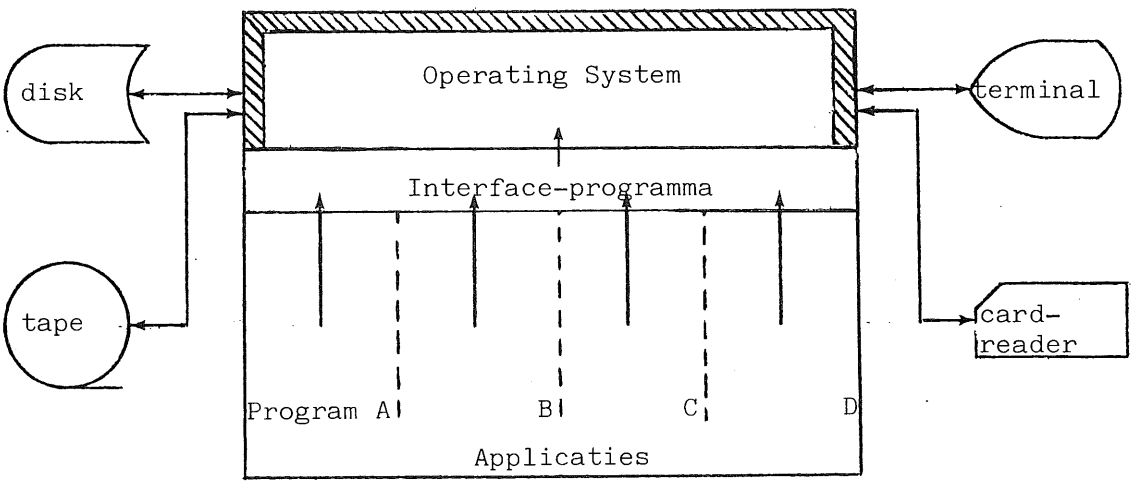
Figuur 1

Door een juiste keuze van programmeertaal wordt de hardware-afhankelijkheid voor de applicatie eveneens verkleind. Het behoeft nauwelijks betoog dat niet een specifiek machinegerichte taal (zoals Assembler), maar juist een algemene, hogere, programmeertaal (zoals COBOL of FORTRAN) deze onafhankelijkheid het meest bevordert. De compatibiliteit van bijvoorbeeld COBOL-applicaties betreft zelfs hardware van verschillende leveranciers.
Ook sommige mini- en microcomputers beschikken tegenwoordig over een COBOL-compiler, waardoor bestaande COBOL-applicaties slechts beperkt behoeven te worden aangepast om ook op deze computers te kunnen worden uitgevoerd.
Het American National Standards Institute heeft o.a. standaards uitgeschreven voor de taal COBOL ten einde een grote mate van compatibiliteit te bereiken tussen de hardware van verschillende leveranciers, welke die standaards hebben geïmplementeerd in hun COBOL-compiler (het zogenaamde ANSI-COBOL). Het verdient derhalve aanbeveling bij het gebruik van een programmeertaal afwijkingen van een algemene standaard te vermijden.

3. Het Operating System (O.S.)

De applicaties zijn weliswaar door gebruik van het O.S. minder hardware-afhankelijk geworden, maar doordat zij daarvoor in de plaats door middel van een bepaalde syntax communiceren met het O.S., wordt onwillekeurig een mate van afhankelijkheid ten opzichte van dit O.S. gecreeerd. Ook hierbij geldt dat hogere programmeertalen een syntax gebruiken, die geschikt is voor meerdere O.S.'s, waardoor de afhankelijkheid wordt verkleind.

Toch wordt bij gebruik van hogere programmeertalen nauwelijks ontkomen aan het aanpassen (converteren) van applicaties bij verandering van O.S.
Om het aanpassen tot het minimum te beperken zou de communicatie tussen het O.S. en de applicaties vermeden moeten worden. Dit kan in bepaalde mate worden bereikt door gebruik te maken van een soort Interface-programmatuur (I-programmatuur). De communicatie tussen applicaties en het O.S. betreft voor het merendeel lees- en schrijfverzoeken (I/O's). Indien nu niet elke applicatie afzonderlijk direct aan het O.S. een I/O-verzoek doet, maar daarvoor in de plaats aan een zelf ontwikkeld I-programma, waarna vervolgens dit I-programma dit verzoek doorgeeft aan het O.S., behoeft bij verandering van het O.S. slechts dit algemene I-programma te worden geconverteerd.
Figuur 2 heeft het gebruik van zo'n I-programma weer.



Figuur 2

De syntax voor het I/O-verzoek van de applicaties aan het I-programma kan bepaald worden binnen de syntaxregels van de programmeertaal van de applicaties. De syntax voor het verzoek aan het O.S. vanuit het Interface-programma is daarentegen O.S.-afhankelijk.

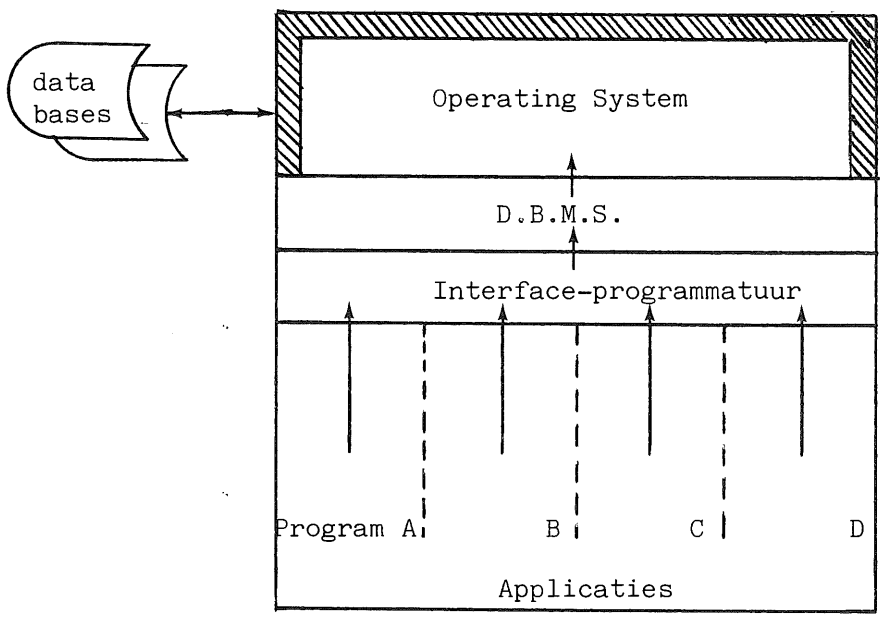
4. Data base

Onder Data base wordt hier verstaan elke vorm van gegevensopslag al dan niet beheerd door een Data Base Management System (DBMS).

Indien gebruik wordt gemaakt van een I-programma, zoals beschreven in het vorige hoofdstuk, zou de bestandsorganisatie kunnen wijzigen

zonder dat applicaties hierop behoeven te worden aangepast. De applicaties verzoeken slechts om data aan het I-programma. Hoe dit I-programma deze data via het O.S. ter beschikking krijgt is niet bekend aan en niet relevant voor de applicatie. Indien bijvoorbeeld een sequentieel bestand zou worden gewijzigd in een Indexed-sequentieel bestand, zou zonder gebruik van het I-programma elke bestaande applicatie, voor zover het dat bestand gebruikt, hierop moeten worden aangepast. Bij gebruik van een I-programma behoeft slechts dit ene programma hierop te worden aangepast.

Een D.B.M.S. vormt in wezen zo'n I-programma als interface tussen de applicaties en het O.S. Het vereist echter in de applicaties ten behoeve van de communicatie een bepaalde syntax waardoor weer afhankelijkheid ontstaat in de applicaties ten opzichte van het D.B.M.S. Ook bij gebruik van een D.B.M.S. kan I-programmatuur gebruikt worden, waardoor de applicaties niet meer direct met het D.B.M.S. behoeven te communiceren en derhalve daardoor D.B.M.S.-onafhankelijk worden.
Figuur 3 toont het gebruik van I-programmatuur ten behoeve van D.B.M.S.-onafhankelijkheid.



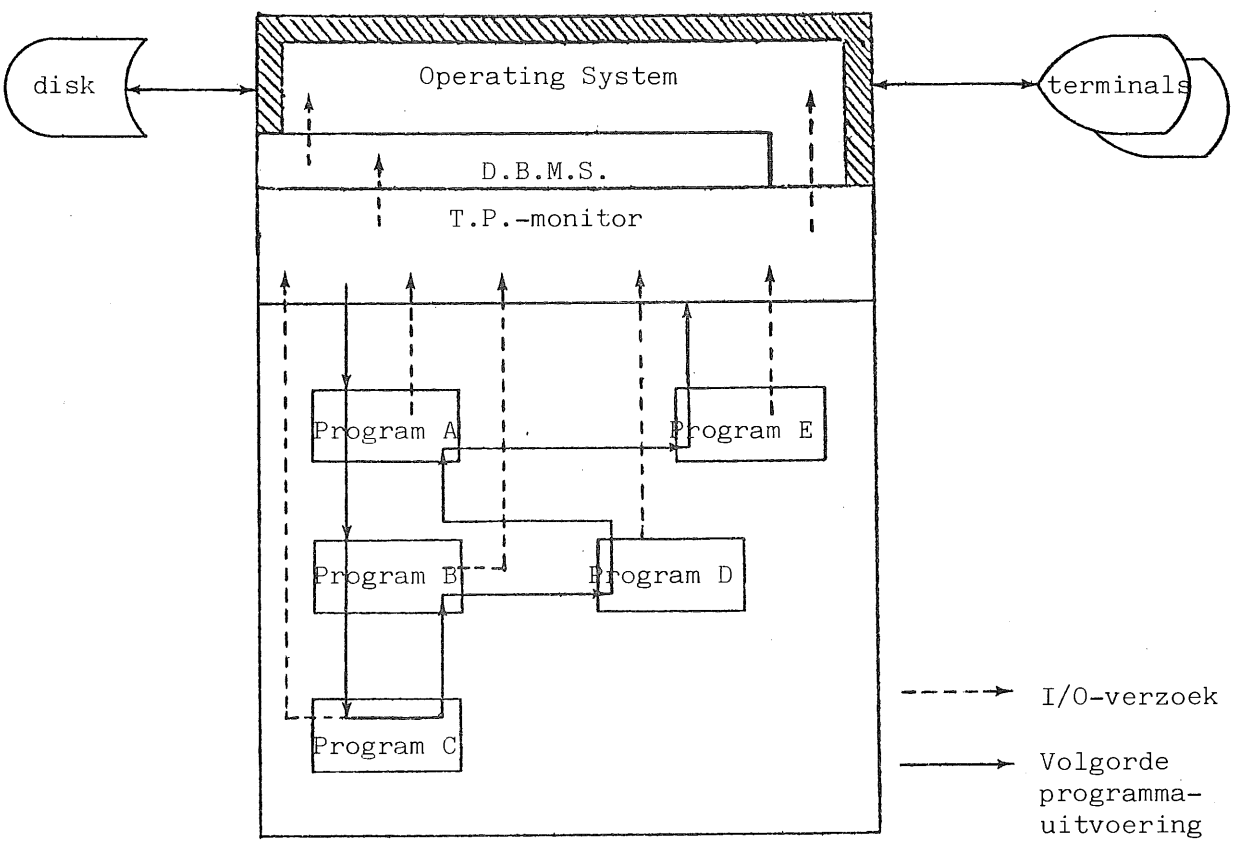
Figuur 3

In het algemeen bestaan door het gebruik van I-programmatuur ten behoeve van Data base-onafhankelijkheid beperkingen in het wijzigen van de bestandsorganisatie en -opslag. De datastructuur zal, afhankelijk van het functioneren van het I-programma, niet onbeperkt kunnen

worden veranderd. De applicaties zullen aan het I-programma vaak in een mate van detaillering aangeven hoe de data door het I-programma zullen moeten worden behandeld. Een bepaalde volgorde of relatie tussen records kan voor de applicaties informatie bevatten. Derhalve moeten de applicaties wel werken met deze karakteristieken van informatie-opslag en als zodanig ook het I-programma instrueren wat met welke data moet worden uitgevoerd. Dit betekent dat een volledige Data base-onafhankelijkheid, al dan niet bij aanwezigheid van een D.B.M.S., voor de applicaties door middel van het gebruik van I-programmatuur in de praktijk niet of nauwelijks te verwezenlijken zal zijn.

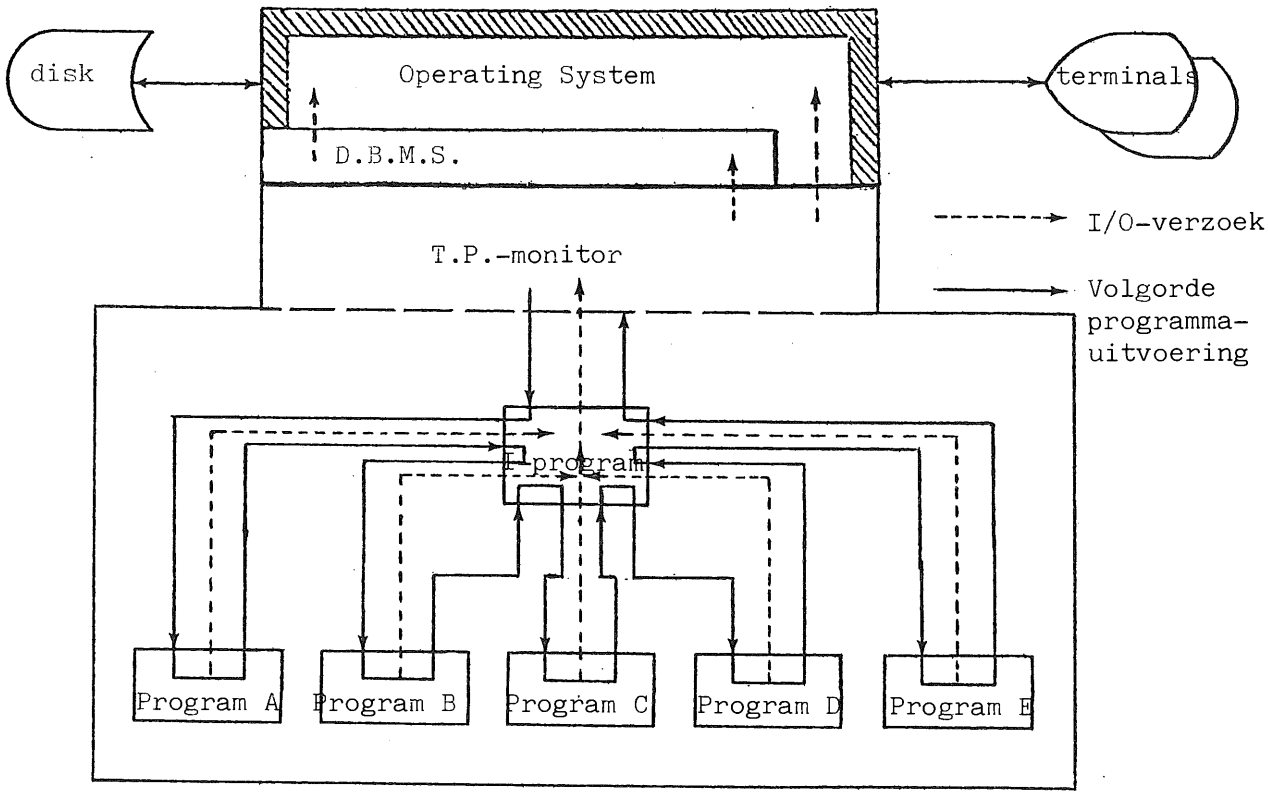
5. Teleprocessing-monitor (T.P.-monitor)

Een T.P.-monitor is ondersteunende software, waardoor online-applicaties kunnen worden uitgevoerd. Deze applicaties doen verzoeken aan de T.P.-monitor inzake I/O naar disk en terminals en het starten van vervolg-applicaties.
Figuur 4 geeft dit schematisch weer.



Figuur 4

De programma's A tot en met E zijn applicaties die achtereenvolgens worden uitgevoerd. Programma A wordt door de T.P.-monitor op verzoek van een gebruiker achter de terminal opgestart.
Gedurende de uitvoering verzoekt dit programma aan de T.P.-monitor om tussentijds programma B op te starten en uit te voeren.
Bij beëindiging van programma A verzoekt deze aan de T.P.-monitor om programma E op te starten. Programma B verzoekt tussentijds om programma C en bij beëindiging om programma D.
Hierdoor krijgen de genoemde programma's in de volgorde A.B.C.B.D.A.E. de besturing van de T.P.-monitor (zie doorgetrokken pijl). De T.P.-monitor vormt in wezen een bepaalde interface tussen de applicaties en het O.S.
Alle programma's in figuur 4 verzoeken de T.P.-monitor om I/O op disk en terminal (onderbroken pijlen).
De programma's B tot en met E worden door verzoeken van applicaties aan de T.P.-monitor opgestart en uitgevoerd.
Alle voornoemde verzoeken zijn aan een bepaalde syntax gebonden ten behoeve van de communicatie tussen applicaties en de T.P.-monitor. Indien de T.P.-monitor wordt vervangen of op dit punt wordt gewijzigd, betekent dit een aanpassing c.q. conversie van alle online-applicaties.
Teneinde in bepaalde mate T.P.-onafhankelijk applicaties te ontwikkelen kan ook hier gebruik worden gemaakt van een online I-programma. Alle verzoeken van de applicaties worden gericht aan het I-programma, dat deze vervolgens in de gewenste T.P.-afhankelijke syntax zal doorgeven aan de T.P.-monitor. Figuur 5 toont dit.



Figuur 5

Voor de volledigheid wordt opgemerkt dat gelijktijdig verschillende programmareeksen, zoals programma's A tot en met E, door de T.P.-monitor en het I-programma kunnen worden bestuurd. De hoeveelheid gelijktijdig uitgevoerde programmareeksen komt overeen met de hoeveelheid actieve aangelogde gebruikers.

Voor elke gebruiker wordt door de T.P.-monitor automatisch het I-programma opgestart en uitgevoerd. Dit I-programma krijgt in het voorbeeld van figuur 5 van de gebruiker op, dat programma A moet worden uitgevoerd. Het I-programma verzoekt aan de T.P.-monitor om achtereenvolgens programma's A tot en met E op te starten en uit te voeren. De applicaties (programma's A tot en met E) verzoeken dus niet meer zelf aan de T.P.-monitor om vervolg-applicaties uit te voeren. Evenzo worden geen I/O-verzoeken direct aan de T.P.-monitor gedaan. Indien de T.P.-monitor wordt vervangen of gewijzigd behoeft slechts het I-programma hierop te worden aangepast.

Een volledige T.P.-onafhankelijkheid zal door het gebruik van I-programmatuur echter niet kunnen worden bereikt, omdat elke applicatie bijvoorbeeld zijn beëindiging wel direct aan de T.P.-monitor zal moeten mededelen. Na beëindiging zal de T.P.-monitor immers de besturing van de applicatie moeten overbrengen naar het I-programma. Het gebruik van het I-programma stelt wel een bepaalde structuur in de applicaties om praktische en technische reden verplicht, hetgeen hier, gezien de doelstelling van dit artikel, niet verder wordt toegelicht.
Wel dient te worden vermeld dat de plaats en toepassing van het I-programma in figuur 5 slechts ter illustratie is. Het is evenwel mogelijk dat (een deel van) het I-programma op een andere plaats, dan aangegeven, kan worden geïmplementeerd. Conceptueel heeft dit echter nauwelijks invloed op de betekenis van het gebruik van online I-programmatuur.

Wat in wezen door het gebruik van het I-programma wordt bereikt is geen T.P.-onafhankelijkheid maar een afhankelijkheid door een communicatie met een veel eenvoudiger en beperkter syntax, hetgeen een T.P.-conversie zal vergemakkelijken.

Het gebruik en functioneren van het I-programma blijft in bepaalde mate afhankelijk van de structuur en werking van de T.P.-monitor. Derhalve kan niet met zekerheid worden gesteld dat door het gebruik van het I-programma zal kunnen worden overgegaan op elke andere T.P.-monitor zonder dat daarvoor alsnog ingrijpende conversiewerkzaamheden moeten worden uitgevoerd. Nochtans bestaat de mogelijkheid dat door dit gebruik conversiewerkzaamheden worden gereduceerd.

6. Interface-programmatuur

Zoals in de inleiding is gesteld, wordt met conversie van applicaties bedoeld: het aanpassen van de syntax waarin de applicaties geschreven zijn.

Syntax ten behoeve van de communicatie met de omgeving (het O.S., het D.B.M.S. of elke andere vorm van bestandsorganisatie en de T.P.-monitor) wordt verwijderd uit (en/of vereenvoudigd in) de applicaties en samengevoegd in interface-programmatuur met het doel de applicaties meer onafhankelijk te maken ten opzichte van de omgeving.
De communicatie met de I-programmatuur geschiedt met behulp van eenvoudige uniforme syntax, die meer wordt bepaald door de programmeertaal dan door de omgeving. De omgeving kan derhalve worden gewijzigd zonder dat de applicaties hiervoor behoeven te worden aangepast (geconverteerd). Slechts de I-programmatuur zal hiervoor moeten worden gewijzigd. In deze ideaalsituatie betekent dit een zeer geringe conversie, waarvan de gebruiker nauwelijks iets behoeft te merken. In dit verband kan de benaming "interface-programmatuur" wellicht beter worden vertaald naar "omgeving-aanpas-programmatuur".

Hoe meer omgevingafhankelijke eigenschappen (syntax) gecentraliseerd worden in de I-programmatuur, des te groter wordt het voordeel van deze toepassing ten behoeve van toekomstige conversie.
Overigens dient vermeld te worden dat het gebruik van I-programmatuur niet alleen ten behoeve van conversie voordelen kan bieden en derhalve door een onderneming ook om andere redenen kan worden gebruikt. Een en ander hangt af van de geïmplementeerde functies binnen de I-programmatuur.
Als verdere voordelen van het gebruik van I-programmatuur kunnen worden genoemd:

- Geringere werkzaamheden inzake nieuwbouw en onderhoud; de I-programmatuur voert tenslotte een aantal standaardfuncties uit die niet in elke applicatie afzonderlijk behoeven te worden geprogrammeerd of onderhouden.
- I-programmatuur dwingt voor de applicaties standaardisatie af inzake O.S./D.B.M.S./T.P.-verzoeken.
- Mogelijkheid tot het gebruiken van additionele integriteits- en autorisatiemaatregelen binnen de centrale I-programmatuur ten behoeve van de gegevens (een soort D.B.I.O.C.- of D.B.Proc.-functie).

Als nadelen kunnen worden genoemd:

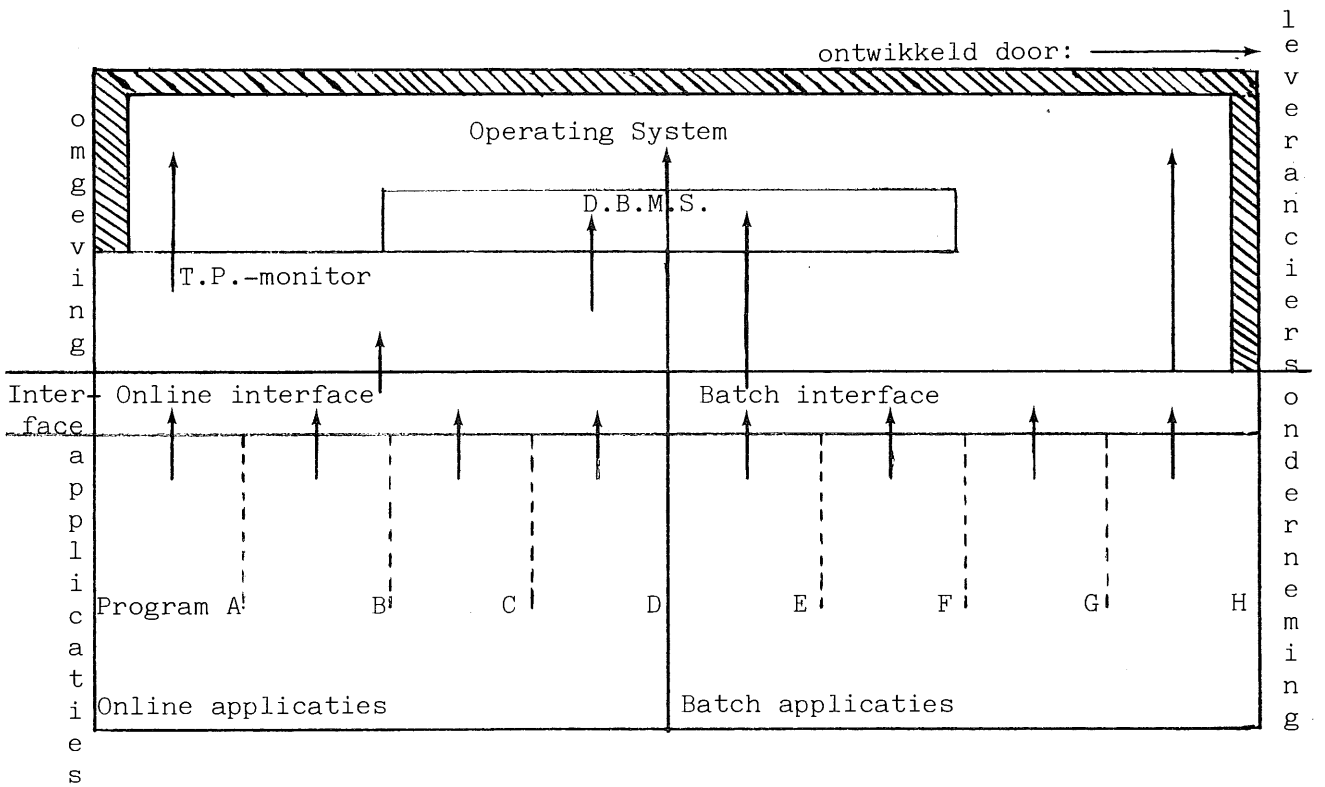
- Overhead (soms moeilijk te kwantificeren).
  De I-programmatuur bevat functies die niet voor elke applicatie afzonderlijk noodzakelijk zijn. Derhalve is de omvang en wellicht ook de werking groter dan specifiek noodzakelijk.
- Mogelijk toch een grote conversie vereist door structurele veranderingen in de omgeving, waarvoor de bestaande I-programmatuur ongeschikt is, (datastructuur en T.P.-werking).
- Indien programmafouten aanwezig zijn in de I-programmatuur ondervinden alle applicaties daarvan hinder.
- Beperkingen in mogelijke verzoeken aan de omgeving, namelijk tot die welke zijn opgenomen in de I-programmatuur.
- Beperkingen in de structuur van online-applicaties.

') D.B.I.O.C. = Data Base Input Output Controller (I.M.S.) = Data Base Procedure (I.D.M.S.)

- Mogelijkheid tot het doorbreken van de door de omgeving geboden beveiligingsmaatregelen. Voor het D.B.M.S. bijvoorbeeld, zal het I-programma tot alle data toegang moeten hebben. Het D.B.M.S. ziet slechts één gebruiker namelijk dit I-programma. Hierdoor is het D.B.M.S. niet meer in staat ten opzichte van de applicaties/gebruikers controle uit te oefenen op de bevoegdheid.
- Mogelijke overname van de in de omgevingbepalende software aanwezige functies (wordt dubbel uitgevoerd/moet eveneens geconverteerd worden).

Het is - wat ook uit de opsomming van nadelen mag blijken - geenszins de bedoeling van dit artikel om een pleidooi te houden voor het gebruik van I-programmatuur. Een onderneming zal afhankelijk van een aantal eigen criteria moeten vaststellen of en met welke functies gebruik zal worden gemaakt van de zelf te ontwikkelen I-programmatuur.
Indien echter wordt gekozen voor bepaalde I-programmatuur, dient deze voor de hierin opgenomen functies door alle applicaties volledig te worden gebruikt, anders suggereert de aanwezigheid een mate van onafhankelijkheid en/of standaardisatie, die niet of niet-volledig wordt benut.

Figuur 6 geeft een samenvatting van de omgeving, interfaces en applicaties.



Figuur 6

I-programmatuur zal in de praktijk op verzoek van, respectievelijk ontwikkeld worden door:

- de Ontwerp/Analyse- en Programmeringsafdeling, die hiervoor eisen en wensen zullen specificeren;
- de Systeemprogrammeringsafdeling, die de I-programmatuur zal bouwen. De I-programmatuur zal uit oogpunt van performance en werking veelal gebouwd worden in een meer machine-gerichte taal (Assembler). De hiervoor benodigde kennis en specialisme bevindt zich meestal bij deze afdeling. Een van de functies van de afdeling is het beheren en onderhouden van de ondersteunende, omgevingbepalende software (O.S., D.B.M.S., T.P.-monitor, etc). De I-programmatuur behoort zeker niet gerekend te worden tot de applicaties maar tot deze ondersteunende software. Derhalve verdient het aanbeveling deze afdeling de bouw van de I-programmatuur te laten uitvoeren ten behoeve van het latere beheer en onderhoud. Voor zover additionele integriteits- en autorisatiemaatregelen binnen de I-programmatuur zijn opgenomen dient het beheer hiervan niet zonder meer bij deze afdeling te worden ondergebracht.

Indien belangrijke taken/functies van het D.B.M.S. en de T.P.-monitor zullen worden overgenomen c.q. doorbroken door het gebruik van de I-programmatuur dienen de T.P.-beheerder en data base administrator bij de ontwikkeling hiervan te worden betrokken.

Het ontwikkelen van I-programmatuur kan afhankelijk van de te implementeren functies en de bereikte mate van efficiëntie, complex zijn. De ontwikkeling wordt niet alleen bemoeilijkt door deze complexiteit maar ook door de navolgende punten:

- Ten behoeve van de toekomstig te ontwikkelen applicaties dienen alle soorten verzoeken te kunnen worden gehonoreerd door de I-programmatuur. Het inventariseren van deze verzoeken in een vroegtijdig stadium is vaak moeilijk;
- De I-programmatuur dient volledig te functioneren alvorens de eerste applicatietests kunnen aanvangen.

7. Programmeertalen

Al eerder is de invloed van de programmeertaal op de conversieproblematiek aan de orde geweest. In dit hoofdstuk zal hierop dieper worden ingegaan mede omdat het gebruik van een taal zelf aanleiding kan zijn tot conversie.

Goed gedocumenteerde applicaties, die gestructureerd en leesbaar zijn gebouwd, zijn hierdoor beter onderhoudbaar en converteerbaar. Deze kwaliteiten vormen een ideaalsituatie, die vooral bij verouderde en te converteren applicaties in de praktijk nauwelijks wordt aangetroffen. Dit wordt nog eens verergerd indien de ontwikkeling van de applicaties niet in een hogere programmeertaal (die veelal beter leesbaar is) maar in een machine gerichte taal heeft plaatsgevonden. Verhoudingsgewijs beschikt een onderneming in steeds mindere mate over applicatieprogrammeurs, die voldoende kennis en ervaring hebben om deze applicaties in machine gerichte taal te onderhouden.

Dit kan binnen de onderneming leiden tot probleemsituaties inzake de continuïteit van de gegevensverwerking indien noodzakelijkerwijs onderhoud moet worden uitgevoerd op de bestaande, in deze taal geschreven applicaties. Het zal derhalve ook moeilijk zijn dergelijke applicaties te converteren, terwijl juist conversie in verband met het genoemde continuïteitsprobleem meer en meer vereist wordt.

Het verloren gaan van kennis met betrekking tot de te converteren applicaties en de programmeertaal vormt ook voor de toekomst een mogelijk probleem ten aanzien van conversie.
Soms wordt hiervoor hulp geboden door de leveranciers. De IBM 4300- en 3000-computers simuleren nu nog met de door IBM geleverde emulatieprogrammatuur een IBM 1400-computer voor de toenmalig ontwikkelde applicaties. Hierdoor behoefde men ondanks de verandering van hardware nauwelijks te converteren. Burroughs heeft in het verleden als oplossing software ontwikkeld om voor een groot deel automatisch Cobol-applicaties draaiend op een andere hardware te converteren naar Cobol-applicaties, die kunnen worden vertaald en uitgevoerd op de Burroughs-computers.

Totaal ongevoelig voor de omgeving wordt een applicatie pas als een onderneming zijn eigen compiler (programmavertaler), generator (software, die uit parameters een applicatie in een bepaalde taal genereert) of interpreter (software, die toepassingsfuncties uitvoert op grond van parameters) bouwt. De onderneming programmeert dan in zijn eigen (parameter-)taal. Indien de omgeving nu verandert behoeft men "slechts" zijn compiler, generator of interpreter hierop aan te passen, waarna vervolgens de in eigen taal geprogrammeerde applicaties vertaald of geinterpreteerd kunnen worden zonder dat deze behoeven te worden geconverteerd. Het is echter bijzonder moeilijk om deze eigen software ten behoeve van de totale gegevensverwerking zelf te (laten) ontwikkelen en onderhouden. Toch worden op dit gebied vergaande ontwikkelingen gedaan, met name in combinatie met het gebruik van data dictionaries.
Gezien het interessante concept wordt hier een recent op de markt verschenen toepassing nader toegelicht. In deze toepassing wordt gebruik gemaakt van een data dictionary, waarin beschrijvingen van datastructuren, toepassingsfuncties en documentatie worden opgeslagen. Door speciale generators worden vanuit de dictionary de programma's gegenereerd in bijvoorbeeld de programmeertaal Cobol of PL/1. Bij een verandering van omgeving behoeven slechts de generators hierop te worden aangepast, waarna alle programma's vanuit de dictionary opnieuw kunnen worden gegenereerd. Ontwikkeling en onderhoud vindt derhalve uitsluitend plaats in deze dictionary, waarna de generators de nieuwe of aangepaste programma's genereren.
Helaas is dit concept nog onvoldoende uitgewerkt omdat enerzijds de dictionary niet voldoet aan de daaraan redelijkerwijs te stellen eisen inzake integriteit en beveiliging; anderzijds het vullen of aanpassen van de inhoud van deze dictionary nog te veel op instructieniveau, overeenkomstig de te genereren programma's, moet plaatsvinden.

Toch toont deze toepassing wellicht de ontwikkeling van het automatiseren in de toekomst. Hierbij wordt gedoeld in de richting van een situatie waarbij op het logische/conceptuele niveau de gewenste toepassing, eventueel door de gebruiker zelf, beschreven wordt, waarna speciale software deze beschrijvingen gebruikt voor het automatisch ontwikkelen van de vereiste applicaties zonder arbeid van systeemanalisten en programmeurs.

In het verleden heeft men ook getracht software te ontwikkelen om applicaties automatisch te converteren. Deze software heeft tot dusver in beperkte mate gefunctioneerd. Bij genoemd voorbeeld van Burroughs werd uitsluitend binnen een zelfde taal geconverteerd. Veel moeilijker is het om van de ene programmeertaal automatische conversie te plegen naar een andere taal. Zeker als de structuren van de talen duidelijk verschillend zijn, zoals bij Assembler en Cobol het geval is. In de toekomst valt op dit gebied geen spectaculaire verbeteringen in deze conversiesoftware te verwachten, waardoor voor een belangrijk deel de programmeertaalconversie manuale handelingen zal blijven vereisen.

8. Samenvatting

Gelet op de ontwikkelingen bij leveranciers van hard- en software zal ook in de toekomst conversie nauwelijks kunnen uitblijven, aangezien deze ontwikkelingen sneller zullen worden ingevoerd dan dat de bestaande informatiesystemen (applicaties) aan vernieuwing toe zullen zijn.

De hulpmiddelen om conversiewerkzaamheden te reduceren zijn tot op heden nog onvoldoende. De interface-programmatuur dient zelf geconverteerd te worden en voorkomt niet altijd inspanning om wijzigingen aan te brengen in de applicaties ten behoeve van de conversie. Ook andere hulpmiddelen staan hiervoor nog in de kinderschoenen waarbij het nog de vraag is of deze er ooit zullen uitgroeien.

Gezien het gegeven "conversie" is het dus raadzaam hierop te anticiperen in zowel het Automatiseringsplan van een onderneming als ook in vooronderzoeken van te ontwikkelen informatiesystemen, waarbij verwachtingen moeten worden uitgesproken inzake:
- De handhaving van de omgeving;
- De levensduur van informatiesystemen;
- De geaccepteerde mate van omgevingafhankelijkheid.

Het automatiseringsbeleid dient er derhalve mede op gericht te zijn aandacht te schenken aan de conversieproblematiek bij systeemontwikkeling.

Herfst 1982

INTERNE CONTROLE-ASPECTEN BIJ EEN SYSTEEM VOOR FINANCIELE ADMINISTRATIE OP EEN MINICOMPUTER

door H. Weerd

1. Inleiding

Op grond van een praktijkervaring bij de participatie in een projectgroep voor de ontwikkeling van een systeem voor financiële administratie op een minicomputer, wordt in dit artikel een uiteenzetting gegeven van de wijze waarop maatregelen van interne controle in een systeem voor financiële administratie op een minicomputer kunnen worden opgenomen.
Het ontwikkelen van geautomatiseerde systemen omvat een aantal van de werkelijkheid losgemaakte activiteiten waaraan nog een extra dimensie wordt gegeven, omdat reeds in een vroeg stadium dient te worden aangegeven op welke wijze maatregelen van interne controle in de organisatie dienen te worden opgenomen.
Met name de wijze waarop de invoerprocedure en de daaruit voortvloeiende rapportage wordt opgezet, is een kritiek moment in de ontwikkelingsfase. Op het juiste moment advies geven bij de ontwikkeling, dit is in de logisch ontwerp-fase, voordat een technische oplossing wordt gerealiseerd, is een belangrijke factor die bepalend is voor het uiteindelijke resultaat. Hierbij dient te worden geanticipeerd op het functioneren van de toepassingen op een minicomputer in een gebruikersorganisatie.
In de gebruikersorganisatie is in de meeste gevallen niet voldoende kennis en begrip ten aanzien van automatisering aanwezig, zodat ingeval er verkeerde beslissingen zijn genomen in een foutsituatie, het tijdig onderkennen van eventuele onregelmatigheden, door maatregelen in toepassingen dienen te worden gesignaleerd.

2. Uitgangspunten

Bij de invoerprocedure voor een systeem voor financiële administratie op een minicomputer is het van belang dat op doelmatige wijze kan worden vastgesteld dat de ingevoerde mutaties op correcte wijze hun weerslag hebben gevonden in de saldi van de rekeningen. Met name in de situatie dat boekingen door verschillende personen in het systeem worden ingevoerd is het van belang dat een ieder dit voor zijn ingevoerde mutaties kan vaststellen.
Om hierin te voorzien kan gebruik worden gemaakt van de aloude techniek van het chronologisch vastleggen van primaire aantekeningen en de daaruit voortvloeiende boekingen in dagboeken. Indien de nodige voorzieningen in het systeem worden opgenomen, biedt de computer hiervoor uitstekende mogelijkheden.
Uitgangspunt hierbij vormt het feit dat de debet/credittotalen van de proefbalans - als de beginbalans ook als mutatie wordt ingevoerd gelijk dienen te zijn aan de som van de debet/credittotalen van de via de dagboeken ingevoerde mutaties.

De voorzieningen betreffen:
a. lay-out van de invoerverslagen;
b. geprogrammeerde controle voor omspannende totaalaansluiting;
c. effectueren van gewenste functiescheiding.

In dit artikel wordt aan de hand van deze indeling een uiteenzetting gegeven van een oplossing voor de wijze van invoervastlegging en de daarbij behorende geprogrammeerde controles, voor een systeem voor financiële administratie op een minicomputer. Ter afsluiting wordt op enige consequenties gewezen voor de accountantscontrole bij toepassing van een dergelijk systeem.

3. Lay-out van de invoerverslagen

Voortvloeiend uit die hiervoor beschreven uitgangspunten dient het resultaat van de per dagboek ingevoerde transacties van elke terminalsessie (de invoering en verwerking van een hoeveelheid transacties met behulp van een terminal) informatie te bevatten, die een oordeel mogelijk maakt over de juistheid van de ingevoerde transacties en de volledigheid van de verwerking van de hieruit voortvloeiende boekingen in de saldi van de rekeningen. Eventuele onregelmatigheden dienen tijdig te kunnen worden gesignaleerd.

Om dit te bereiken dienen de invoerverslagen een overzicht te bevatten van de transacties (primaire aantekeningen). Deze dienen te worden gevolgd door een recapitulatie van de uit de transacties voortvloeiende grootboekmutaties.
Het totaal van deze grootboekmutaties dient debet/credit gescheiden te worden gecumuleerd. Vervolgens dient een telling te worden afgedrukt van het debet/credittotaal van de in voorgaande verwerkingsgangen (sessies) via het dagboek ingevoerde grootboekmutaties (dagboektotaal oud); bij dit totaal dient het totaal van de via de terminalsessie ingevoerde mutaties te worden geteld. De som vormt het dagboektotaal nieuw van alle via het dagboek ingevoerde mutaties (ingang in het grootboek) tot dat moment. Dit totaal dient in het systeem te worden vastgelegd, zodat dit voor een volgende sessielijst kan worden gehanteerd. Voor het systematisch archiveren kunnen de sessielijsten tevens van een volgnummer per dagboek worden voorzien.
De sessielijst komt vrijwel direct na het intoetsen van de transacties beschikbaar, zodat de complete verwerking van de transacties in een aaneenschakeling van activiteiten kan worden afgehandeld.

Voor de uitvoering van de activiteiten met betrekking tot intoetsen en verificatie, kan op de sessielijst worden geparafeerd.
De paraaf voor de verificatie dient onder andere te staan voor de uitvoering van de volgende handelingen:
- aansluiting vaststellen van nummervolgorde van de verslagen per dagboek;
- aansluiting vaststellen van oude en nieuwe stand van de dagboektotalen;
- vaststellen dat de mutaties zijn ingetoetst door degene die hiervoor heeft geparafeerd;

- beoordelen van het juiste gebruik van de grootboekrekeningen;
- visuele detailcontrole met brondocumenten.

Ter ondersteuning van de controle op juistheid van de ingevoerde transacties kan worden overwogen om bij de invoerprocedure met voortellingen te werken, indien een visuele detailcontrole met de brondocumenten niet doelmatig wordt geacht. Voor de uitvoering van de invoerprocedure dient bij voorkeur de sessielijst te worden geparafeerd, zodat achteraf kan worden vastgesteld door welke personen de werkzaamheden zijn uitgevoerd.
In het hierna volgende schema is een overzicht gegeven van de hierboven beschreven lay-out van een sessielijst voor een financieel dagboek.

Voorbeeld sessielijst financiële dagboek AMRO

SESSIE VOLGNUMMER: XX

STUKNR.	PERS.NR.	FAKTNR.	DATUM	PERIODE	GROOT-BOEK-REKENING	DEBET	CREDIT	
001001	1234563	401234	020182	0182	150000		3.000,00	(1)
001001	1234563	401237	020182	0182	150000		2.000,00	(1)
001002	4321222	012002	020182	0182	160000	3.420,00		(2)
001003			020182	0182	004000	7.200,00		(3)
001003			020182	0182	140000		5.620,00	(4)
						10.620,00	10.620,00	

RECAPITULATIE

150000	DEBITEUREN		5.000,00	(posten 1 en 2)
160000	CREDITEUREN	3.420,00		(post 2)
140000	AMRO		5.620,00	(sluitpost)
	OVERIG GROOTBOEK	7.200,00		(post 3)
	SESSIETOTAAL	10.620,00	10.620,00	
	DAGBOEKTOTAAL OUD	100.000,00	100.000,00	
	DAGBOEKTOTAAL NIEUW	110.620,00	110.620,00	

D.D. PARAAF

INTOETSEN:

VERIFICATIE:

Met behulp van de hiervoren beschreven lay-out en voorzieningen voor de invoerverslagen zijn de administratieve medewerkers in staat greep te houden op de door hen in het systeem ingevoerde transacties en de daaruit voortvloeiende grootboekmutaties.

4. Geprogrammeerde controle voor omspannende totaalaansluiting

Door dagelijks en op afroep een overzicht te vervaardigen waarop de dagboektotalen nieuw per dagboek worden afgedrukt en getotaliseerd kan vervolgens met een geprogrammeerde controle een debet/credittotaal van de grootboekrekeningen uit het grootboek-saldibestand worden geformeerd. Dit totaal dient gelijk te zijn aan het debet/credittotaal van de dagboeken. Ingeval van ongelijkheid dienen gebruikersinstructies beschikbaar te zijn voor de te nemen actie, alvorens de transactieverwerking wordt voortgezet.

Met name ingeval van onzekerheid na een storing (stroomuitval, lees/schrijffouten, etc.) kan deze geprogrammeerde controle van nut zijn om vast te stellen of de ingevoerde transacties op correcte wijze zijn verwerkt.
Ook ingeval een restore-procedure niet op correcte wijze is uitgevoerd kan deze onregelmatigheid tijdig worden gesignaleerd, mede met behulp van de sessieverslagen door na de restoreprocedure de debet/credittotalen opnieuw te laten formeren.

5. Effectueren van gewenste functiescheiding

Bij gebruik van een systeem voor financiële administratie op een minicomputer kunnen de volgende functies worden onderscheiden:
- het voorbereiden en dagelijks verwerken van boekingen door administratieve medewerkers (met het verdelen van de verschillende activiteiten in brede zin);
- het incidenteel toekennen van bevoegdheden voor transactieverwerking met behulp van terminals aan administratieve medewerkers;
- het periodiek aanbrengen van wijzigingen en aanvullingen op de programmatuur.

Het is van belang dat de hierboven genoemde functies gescheiden zijn zodat een persoon uit hoofde van zijn functionele bevoegdheid niet meer dan één van de hierboven genoemde functies krijgt toegewezen.
Bij gebruik van een minicomputer kan voor het realiseren van een beoogde functiescheiding in de meeste gevallen geen gebruik worden gemaakt van een automatiseringsorganisatie waarbij een verdeling van activiteiten over een ontwikkelingsorganisatie, verwerkingsorganisatie en gebruikersorganisatie kan plaatsvinden.

Een minicomputer heeft de mogelijkheid om gebruik te maken van passwords waarmee het gebruik van de functies van de minicomputer via keuzemenu's kan worden beperkt. In de keuzemenu's kunnen zowel programmanamen voor transactieverwerking als programmanamen voor het gebruik van hulpprogrammatuur, waarmee wijzigingen en aanvullingen op de programmatuur worden aangebracht, worden opgenomen.

In de ideale situatie kan een password van een terminalgebruiker door hemzelf op elk gewenst moment worden gewijzigd.
Door gebruik te maken van deze mogelijkheden en door voldoende geheimhouding rond het gebruik van de passwords te realiseren, wordt het ten uitvoer brengen van een scheiding van functies met behulp van deze techniek ondersteund.

Het toewijzen van bevoegdheden tot transactieverwerking en het gebruik van hulpprogrammatuur aan personen dient in overleg met de directie te worden bepaald en schriftelijk te worden vastgelegd. De technische uitwerking van het toekennen van de bevoegdheden kan worden gedelegeerd aan een ter zake deskundig medewerker.

6. Consequentie voor de accountantscontrole

Door de accountant kan achteraf op eenvoudige wijze worden vastgesteld:

a. de opeenvolging van de dagboektotalen oud/nieuw van de sessielijsten;
b. de aansluiting van het totaal-generaal van de dagboektotalen met het totaal-generaal van de proefbalans.

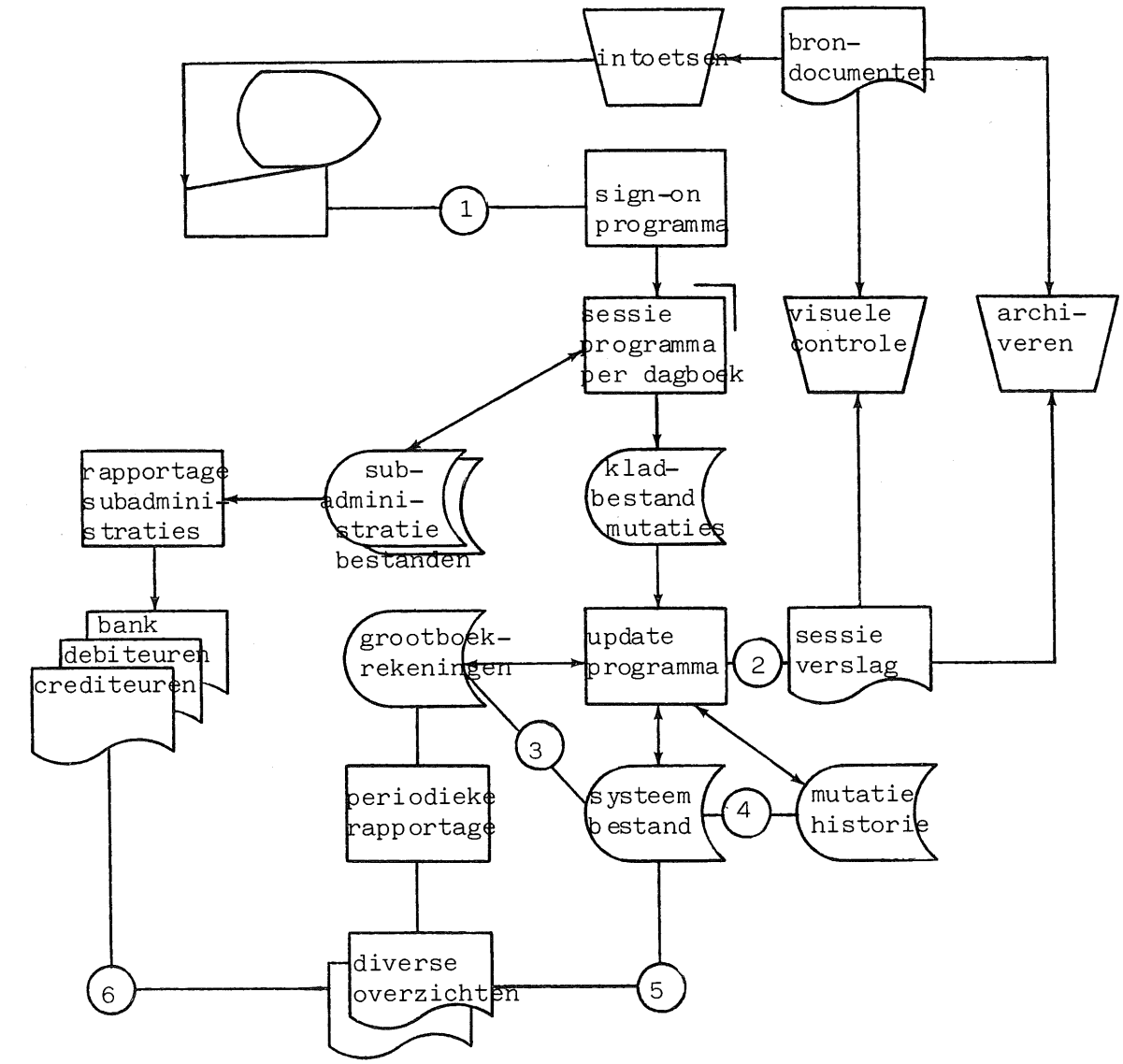
Indien de sessielijsten en de daarbij behorende brondocumenten per dagboek worden gearchiveerd, kan een gewenste verificatie van uitgevoerde boekingen op efficiënte wijze reeds in de loop van het boekjaar in de dagcontrole plaatsvinden. Door de hiervoor beschreven archiveringsprocedure zal een gewenste verificatie van uitgevoerde boekingen aan de hand van een historisch overzicht per grootboekrekening op minder efficiënte wijze kunnen plaatsvinden. Hierbij dient aan de hand van de bij de post vastgelegde verwijzing naar dagboek/terminalsessie de betreffende stukken te worden geraadpleegd.

Met behulp van de schriftelijke vastlegging van de bevoegdheidsregeling en de parafen op de sessielijsten kan achteraf worden vastgesteld of de beoogde functiescheiding over een periode is geëffectueerd.

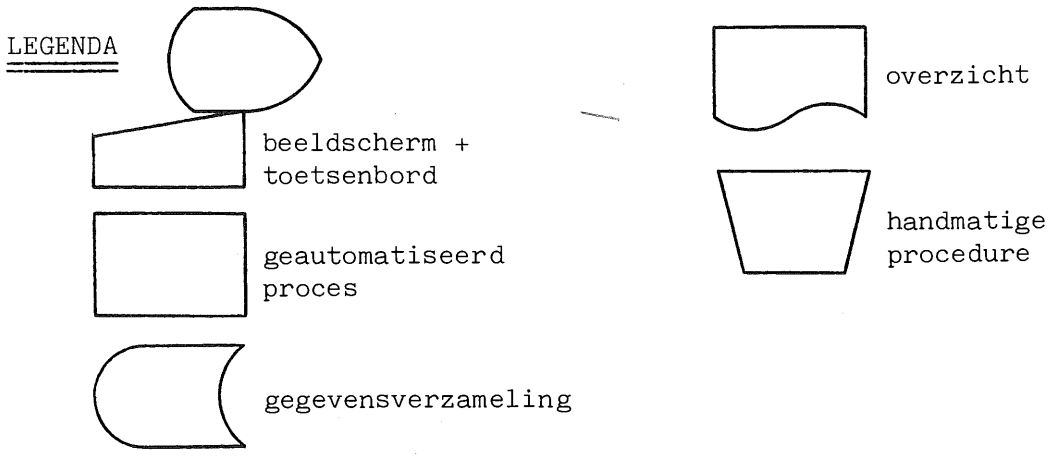
7. Slot

In het hiernavolgend schema is voor de geïnteresseerde een globaal overzicht gegeven van programma's en procedures voor een systeem van financiële administratie.

SCHEMA mutatie-invoer en verwerkingsprocedures



LEGENDA



Toelichting op het schema

In het schema zijn cijfers opgenomen, Deze cijfers verwijzen naar de hierna volgende punten.

1. Toegang tot het systeem

Ten behoeve van de terminalgebruikers dienen door een systeembeheerder passwords te worden toegekend. Aan deze passwords, waarmee de terminalgebruikers zich kenbaar moeten maken aan het systeem, worden keuzemenu's gekoppeld.
Per keuzemenu kunnen bepaalde transacties (sessies per dagboek) worden geselecteerd. De aard van de te selecteren transacties kan per terminal worden beperkt.

2. Sessieverslagen

De organisatie van de invoervastlegging is gebaseerd op dagboeken. Van ieder dagboek - in casu ingang in het grootboek - wordt in een systeembestand een totaaltelling bijgehouden (debet/credit) van alle via het desbetreffende dagboek ingevoerde mutaties. Van iedere toevoeging van mutaties (terminalsessie) wordt een overzicht in journaalvorm afgedrukt, dat is voorzien van het vorige totaal, de mutaties en het nieuwe totaal van de via het dagboek ingevoerde mutaties.

3. Totalen per dagboek en totaalsaldo grootboekrekeningen

Periodiek en op afroep kan een geprogrammeerde totaalcontrole worden uitgevoerd waarmee wordt vastgesteld en zichtbaar gemaakt dat de som van de totalen per dagboek gelijk is aan de som van de totalen van de grootboekrekeningen.

4. Totalen van de mutatiehistorie

Periodiek en op afroep kan een geprogrammeerde totaalcontrole worden uitgevoerd waarmee wordt vastgesteld en zichtbaar gemaakt dat de som van de totalen van de dagboeken gelijk is aan de som van de totalen van de mutatiehistorie.

5. Proefbalans

Het totaal-generaal van de proefbalans dient gelijk te zijn aan het totaal van de som van de dagboektotalen. Dit kan handmatig worden vastgesteld.

6. Subadministraties

De totalen van de subadministraties kunnen uiteraard op eenvoudige wijze handmatig worden aangesloten met de desbetreffende rekening in het grootboek.

BESCHERMING SOFTWARE TEGEN ONGEAUTORISEERD COPIËREN

door L.N.M. Straathof

1. Inleiding

In dit artikel wordt ingegaan op de problemen bij en de mogelijkheden van bescherming van eigendomsrechten van software.
De belangstelling voor deze bescherming is toegenomen door de sterke uitbreiding van personal computing-systemen.
De gebruikers van deze systemen houden zich op ruime schaal bezig met het onbevoegd copiëren van computerprogramma's.
Dit vermenigvuldigen is op zich geen nieuw probleem, het doet zich reeds jaren voor op het gebied van muziek, film, boeken en tijdschriften.
Het is van belang dat de eigendomsrechten van programmatuur op een adequate wijze beschermd worden, daar de veelal hoge ontwikkelingskosten anders in onvoldoende mate worden terugverdiend, hetgeen remmend werkt op het gebied van de software-ontwikkeling.
De protectie dient zich zowel te richten op het onzichtbare concept wat schuil gaat achter het programma als op de fysieke manifestatie ervan (source-listing, flow-charts, programmabeschrijving, enz.).

2. Problemen bij bescherming van software

Het ontwikkelen van een sluitend geheel van beschermingsmaatregelen wordt bemoeilijkt door de steeds in beweging zijnde automatiseringstechnologie, de internationale verschillen op het gebied van de betreffende wetgeving gepaard gaande met een intensief grensoverschrijdend gegevensverkeer.
Daar geen algemeen aanvaarde, uniek identificerende, programmakenmerken aanwezig zijn, ontstaat met betrekking tot de bescherming van software veelal verwarring onder automatiseringsmensen en bij de rechterlijke macht, zodra men een programma wil definiëren.
Hierdoor ontstaan problemen als: worden de eigendomsrechten van een source-module aangetast bij conversie naar een load-module?
Er wordt onvoldoende rekening gehouden met het feit dat naast de fysieke presentatie van programmatuur ook de daarachter liggende innoverende ideeën beschermd moeten worden.
Het voorafgaande heeft ertoe geleid, dat in Amerika een rechterlijke uitspraak gedaan is, waarin de source-code wel en de daarvan afgeleide objectcode niet onder het copyright viel, omdat de objectcode fysiek verschilt van de source-code.

3. Beschermingsmogelijkheden

Bij het beschermen van software tegen onbevoegd copiëren kan gedacht worden aan de volgende mogelijkheden:
- wetgeving;
- technische faciliteiten.

Op het gebied van de wetgeving spelen de auteursrechten, octrooiwet en trade secrecy een rol.
Op het einde van dit hoofdstuk zal nader worden ingegaan op de mogelijkheid om van een bepaald programma unieke kenmerken vast te stellen.

3.1 Auteursrechten

De auteurswet is gericht op de bescherming van auteurs tegen ongeoorloofd aanmaken van meerdere exemplaren en wijziging van literaire of artistieke werken. Voor software betekent dit, dat auteursrechten slechts een beperkte protectie tegen ongeautoriseerd copiëren bieden, daar alleen de fysieke manifestatievorm van een programma (bijvoorbeeld stroomschema's) beschermd wordt en niet de achterliggende ideeën.
Bovendien wordt het gebruik van een computerprogramma door onbevoegde derden onvoldoende beschermd.
Op het gebied van auteursrechten zijn twee internationale conventies opgericht, teneinde een internationale context voor auteurswetgeving te scheppen.
De bedoelde conventies zijn:
. Berner Conventie (B.C.);
. Universele Auteursrecht Conventie (U.A.C.).

In alle landen die onder de B.C. vallen, worden de auteurs zonder enige formaliteiten van rechtswege beschermd.
De mate van bescherming is echter afhankelijk van de reikwijdte van de betreffende nationale wetgeving.
De landen op welke de U.A.C. van toepassing is kunnen bepaalde formele voorschriften opstellen, waaraan voldaan moet zijn wil de auteur beschermd worden.
Ondanks het bestaan van deze conventies zijn de verschillen tussen de nationale auteursrechten niet gering. Voorts ontbreken duidelijke definities van begrippen, zoals bijvoorbeeld de omschrijving van een programma.

3.2 Octrooiwet

De octrooiwet beschermt uitvindingen, belichaamd in een voortbrengsel of een werkwijze, tegen namaak.
Voordat een octrooi wordt toegekend in een bepaald land moet een octrooionderzoek plaatsvinden welke gericht is op het vaststellen van de nieuwheid van het produkt, in dit geval het programma.
Voorts dient het programma enig nut te hebben op het gebied van handel en nijverheid.
Mr. A. Boers stelt in een van zijn artikelen dat het nieuwheidsvereiste in vele gevallen een blokkade kan opleveren voor octrooiering, daar een computerprogramma in verreweg de meeste gevallen wel een bepaalde inventiviteit in zich heeft, maar deze is slechts zelden zodanig dat gesproken kan worden van een innovatie.
In tegenstelling tot de auteurswetgeving biedt een octrooi bescherming van zowel de fysieke presentatie als van de innoverende ideeën.

Bovendien wordt bescherming geboden tegen de ontwikkeling en verspreiding van soortgelijke programma's, die onafhankelijk van het beschermde programma ontwikkeld zijn.
Het aanvragen van een octrooi in een bepaald land brengt echter wel met zich mee, dat de nieuwe toepassing bekend gemaakt moet worden, waardoor de kans groot is dat kopieën in omloop komen, waarin kleine wijzigingen zijn aangebracht ten opzichte van het beschermde programma. Het octrooi is namelijk niet van toepassing op het gewijzigde programma.

3.3 Trade secrecy

Onder trade secrecy wordt verstaan het beschermen van bedrijfsgeheimen (waaronder ontwikkelde programmatuur) in het geval deze zouden worden doorgespeeld, aan concurrenten door (ex-)werknemers, leveranciers of afnemers of via bedrijfsspionage van concurrenten.
Ten opzichte van voorafgaande wettelijke regelingen biedt trade secrecy het voordeel, dat men de reikwijdte van de bescherming tot op zekere hoogte zelf kan bepalen door allerlei contractuele bedingen en dat men de inhoud kan laten evalueren met veranderde situaties en technologieën.
Toch komt mr. A. Boers tot de conclusie dat deze oplossing slechts een aanvulling kan zijn op de octrooi- of auteurswetgeving, daar slechts in beperkte mate buitenstaanders erbij betrokken zijn. Een absoluut rechterlijke bescherming ontbreekt daar men geen verhaalmogelijkheid heeft bij een eventuele mislukking. De kans hierop neemt toe naarmate het programma een grotere bevoegde gebruikerskring krijgt.

3.4 Samenvatting wettelijke beschermingsmogelijkheden

Indien wij een en ander samenvatten dan krijgen wij het volgende overzicht, welke ontleend is aan de artikelenserie van mr. A. Boers (zie literatuuroverzicht).

	Octrooi-wetgeving	Auteurs-wetgeving	Trade secrecy
Onderwerp van bescherming	• innovatie-concept • fysieke presentatie	fysieke presentatie	• innovatie-concept • fysieke presentatie
Reikwijdte bescherming	absolute bescherming bij copiëring e.d.	in hoge mate internationaal, doch onafhankelijke ontwikkelingen expliciet toegestaan	voornamelijk contractueel bepaald (buiten-contractueel via het strafrecht en onrechtmatige daad)
Vereisten voor bescherming	nieuwheid en een "produkt"	• originaliteit; al dan geen depot • het copyright-notice wordt ten zeerste aanbevolen	aanwezigheid van vertrouwelijke gegevens
Handhaving van bescherming	een toelatingsprocedure door de octrooi-rechthebbende	door de auteurs-rechthebbende	door de rechthebbende

3.5 Technische faciliteiten

Het is technisch mogelijk om programmatuur tegen copiëren te beschermen door het programma vast te leggen in een Read Only Memory (R.O.M.), welke wordt aangebracht in een cassette of insteekmodule. Hiermee krijgt het programmaprodukt een fysiek aanwijsbare manifestatievorm en gaat het als deel van de hardware meespelen in de werking van het computersysteem.
Daar de fabrikanten van microcomputers streven naar een zo hoog mogelijke uitwisselbaarheid van software wordt bij het ontwerp van de computer, onvoldoende rekening gehouden met deze technische beschermingsmogelijkheid.

Ook al zou dit laatste niet het geval zijn, blijft het nog steeds mogelijk om software uit te lenen.
Volgens Seymour Rubinstein, de president-directeur van Micropo, kan dit laatste probleem opgelost worden, door het aanbrengen van een geheime code op de R.O.M. in de insteekmodule, welke alleen bekend is bij de computer, waarmee de R.O.M. de eerste keer gewerkt heeft.
Het beschermen van programma's tegen plagiaat door middel van scrambling, is weinig effectief daar ontcijferingsprogramma's (Locksmith, Nibbles Away 2) op de markt zijn die "binnen zeer korte tijd" in staat zijn om de meeste versluierde programma's om te zetten in een uitvoerbaar programma.

3.6 Unieke programmakenmerken

Een van de problemen bij de wettelijke bescherming van software is het ontbreken van algemeen aanvaarde eigenschappen die een programma uniek identificeren.
Volgens Karl J. Dakin en David A. Higgins bezitten programma's kenmerken die een zelfde onderscheidend vermogen hebben als de vingerafdrukken van een mens.
Volgens bovengenoemde schrijvers is het mogelijk om te bewijzen, dat twee programma's die in verschillende talen voor verschillende computers geschreven zijn en de zelfde functie hebben, gelijk zijn indien het ene programma een kopie is van de ander.
Een consistente software-ontwikkelingsmethode zoals de Warnier/Orr Data Structured Systems Design Method (D.S.S.D.) is een hulpmiddel voor het uniek maken van een programma.
Uitgangspunten voor deze methode zijn:

- het ontwerp moet georiënteerd zijn op de output;
- het ontwerp dient onafhankelijk te zijn van een bepaalde computer;
- het ontwerp wordt afgeleid van de structuur van de gegevens die bewerkt worden.

De hiervoor genoemde schrijvers stellen dat een programma, welke ontwikkeld is volgens de D.S.S.D.-methode leidt tot een software-produkt met een bijna unieke combinatie van input-, verwerkings- en output-specificaties.
Het vermelde concept van gestructureerd programmeren is niet nieuw. Wel nieuw is de realisatie dat alle programma's dezelfde invoergegevens in dezelfde volgorde moeten verwerken om dezelfde output te krijgen.
Het feit dat programma's op verschillende manieren kunnen inspelen op de fysieke omgeving zorgt er voor, samen met de logische specificaties, dat een programma voor 100% uniek wordt.

4. Nationale en internationale ontwikkelingen

Op dit moment zou slechts één beslissing bekend zijn in het Nederlandse rechtsysteem over het al dan niet beschermen van computersoftware.

Het betreft een beslissing van de octrooiraad, afdeling van beroep, uitgesproken op 16 december 1970, welke handelde over een programma dat een geavanceerd(er) systeem van telefoonverbindingen mogelijk maakte.
Volgens mr. A. Boers bevat de uitspraak de volgende elementen:

- computerprogramma's kunnen op zich zeer wel op een "verdienstelijke gedachte" berusten, doch dat het gebruiken van een computer met een daarbij behorend programma nog niet behoeft te leiden tot een nieuw voortbrengsel;
- zaken welke betrekking hebben op het transport en de verwerking van informatie zijn niet octrooieerbaar;
- indien het programma niet op het gebied van de stoffelijke produktie ligt en evenmin in de natuur enige verandering brengt, bevat het geen octrooieerbare werkwijze.

Een commissie van de E.E.G. (Europees Computer Services Association) is bezig met de ontwikkeling van een Europees software-copyright. Daar de harmonisatie van de nationale wetten veel tijd vergt, verwacht men dat het lange tijd zal duren voordat een Europese wetgeving gerealiseerd zal zijn.
Veel landen beschikken niet over octrooiwetten voor programmabescherming.
In Duitsland, Frankrijk en vrijwel ook in Oostenrijk wordt patentering van software door de rechterlijke instanties expliciet uitgesloten.

In het Verenigd Koninkrijk kunnen computerprogramma's vrijwel niet gepatenteerd worden volgens de Patents Act van 1977.
Men neemt over het algemeen aan dat software als een "writing" geldt en derhalve onder het auteursrecht valt (Copyright Act van 1956).
Verscheidene internationale instanties zoals de E.P.C. (Europese Patent Conventie) en de P.C.T. (Patent Cooperation Treaty) hebben een kader geschetst waaraan de nationale wetten zouden moeten voldoen. De naleving van dit voorstel kan echter niet worden afgedwongen, zodat het gevaar aanwezig blijft dat een toegekend octrooi in een bepaald land geen geldingskracht heeft in andere landen.
Op aanraden van de Contu (National Commission on New Technological Uses of Copyrighted Works) is in Amerika het auteursrecht gewijzigd (Computer Software Copyright Act 1980), waardoor het copyright van software nu als volgt wordt voorgeschreven:

- kopieën kunnen door de, daartoe door de auteursrechthebbende, gemachtigde gebruiker slechts in samenhang met het computergebruik worden gemaakt;
- het programma mag slechts met goedkeuring van de auteur worden aangepast;
- het is de gemachtigde gebruiker verboden om het programma te bewerken of door te verkopen.

In de nieuwe Amerikaanse wet worden de innoverende ideeën niet beschermd. De wetgever was de mening toegedaan dat de ontwikkeling in de automatisering geremd zou worden indien uitvinders nieuwe toepassingen zouden kunnen monopoliseren.
Op dit moment wordt gewerkt aan de realisatie van het Ompi-voorstel van de International Association for the Protection of Industrial Property.
Dit voorstel omvat de invoering van een modelwet en een modelverdrag.
De modelwet biedt een minimum bescherming voor producenten van software, welke dient te worden geïntegreerd in de nationale wetten.
In de modelwet komen onder andere de volgende elementen voor:

- het programma moet een zekere mate van "originaliteit" bezitten om voor bescherming in aanmerking te komen;
- de programmabeschrijvingen en flow-charts vallen wel, de algoritmen niet onder de bescherming van het auteursrecht;
- de rechthebbende van het auteursrecht kan een ieder verbieden om de software openbaar te maken, het te gebruiken, op wat voor wijze dan ook, te copiëren alsmede van het programma een grotendeels gelijk van structuur en opzet zijnde programma te maken.

5. Conclusies

Op basis van het voorgaande kunnen de volgende conclusies getrokken worden:

- de wettelijke beschermingsmogelijkheden zijn op dit moment onvoldoende om de eigendomsrechten van software te beschermen;
- om verwarring bij de rechterlijke macht te voorkomen is het van belang dat algemeen aanvaarde standaarden tot stand komen, waaraan programma's getoetst kunnen worden ter vaststelling of het ene programma een kopie is van de ander;
- een sluitend systeem van wettelijke beschermingsmaatregelen vereist dat de wetgeving van de verschillende landen een gelijke geldingskracht krijgen;
- onder de software-fabrikanten wordt gedacht aan technische faciliteiten, die het copiëren van computerprogramma's volledig onmogelijk maken, echter de belangen van de computerfabrikanten zullen de realisatie van deze beschermingsmogelijkheid bemoeilijken.

Literatuuroverzicht

- Mr. P. Willemse, Enkele opmerkingen over: auteursrecht en computerprogramma's.
  Informatie mei 1982.

- Mr. A. Boers, Software valt niet onder octrooiwetten.
  De Automatisering Gids, 10 februari 1982.

- Mr. A. Boers, Computerprogramma zit vaak vol kennis.
  De Automatisering Gids, 17 februari 1982.

- Mr. A. Boers, De ontwikkelingen in het buitenland.
  De Automatisering Gids, 24 februari 1982.

- Mr. A. Boers, Programmatuur is in ons land vogelvrij.
  De Automatisering Gids, 3 maart 1982.

- Het copiëren van software.
  De Computerkrant, 1 september 1982.

- Nico Baayens, Software-diefstal en piraterij: brandend probleem zonder oplossing.
  De Computerkrant, 2 juni 1982.

- Malcolm Peltu, The practical problems of protection.
  Datamation, juni 1981.

- Karl J. Dakin en David A. Higgins, Fingerprinting a program.
  Datamation, april 1982.

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

COMPUTER RELATED RISKS, AUTEUR M.J. COMER

door drs. H.G.Th. van Gils

Inleiding

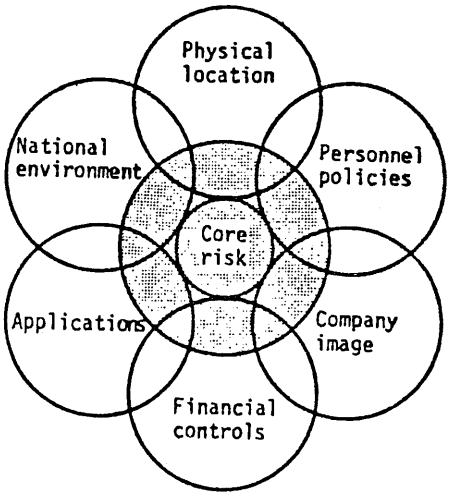
Hieronder volgt een samenvatting van twee papers van Michael J. Comer, auteur van het boek Corporate Fraud (1977).
M. Comer heeft een uitgebreide ervaring op het gebied van fraude-onderzoek en risico management.
De papers zijn getiteld "Some facts about fraud" en "Computer related risks" (ongedateerd). Zij zullen hieronder geïntegreerd worden besproken aangezien zij veel met elkaar te maken hebben en elkaar gedeeltelijk overlappen.
De beide papers en het boek zijn in de A.C.-bibliotheek opgenomen.

Risico's

Iedere onderneming met geautomatiseerde gegevensverwerking heeft te maken met een aantal risico's, waaraan een computersysteem onderhevig kan zijn.

Hoewel er in het algemeen een bepaalde kern van risico's bestaat, worden deze sterk beïnvloed door de omgeving van het computersysteem. Zo zullen de risico's rond een computersysteem dat gebruikt wordt door het KNMI voor weersvoorspellingen sterk verschillen van die rond een gelijk computersysteem dat in Italië gebruikt wordt voor verwerking van gegevens over misdadigers.
Figuur 1 geeft dit schematisch weer.
Het centrale kerndeel van computerrisico's is van veel minder invloed dan de omgevingsfactoren.

In de bedrijfsomgeving is het kerndeel van risico's toegenomen om de volgende redenen:
- concentratie van gegevens op één plaats
- afhankelijkheid van het computersysteem
- vermindering van menselijke handelingen
- vertrouwen in door de computer geproduceerde gegevens
- snelheid van verwerking
- computers zijn symbolische doelen voor bijvoorbeeld terroristen. Een staking kan al effectief zijn indien alleen het operating-personeel van het computercentrum het werk onderbreekt.



CORE RISKS

- Type of hardware
- Type of communications network
  - dial up of dedicated lines
- Controls built in into the operating system

MODIFYING FACTORS

- National environment
  - economic and social pressures
  - political factors
- Physical location
  - urban or suburban
  - greenfield site or multitenancy building
  - high-risk adjoining buildings
- Applications processed
  - Government or commercial
  - financial or scientific
  - easy conversion possibilities or of no financial significance
  - in-house programming or external consultants
  - privacy and information value
- Financial controls
  - general ledger and budgetary structure
  - cost centre accounting or global accounting
- Company image
  - abrasive or sympathetic management style
  - high or low profits
  - multinational or local
  - head-office location or remote branch
- Personnel policies

Figuur 1. Core risks and modifying factors.

Motivatie

Een reden voor het onvoldoende onderkennen van risico's komt voort uit een houding van 'het zal mij niet overkomen' of 'x% diefstal is onvermijdelijk'.
Aan de hand van verzekeringsgegevens wordt gesteld, dat van het gemiddelde personeelsbestand (inclusief directieniveau)

. 25% onder alle omstandigheden eerlijk zal blijven
. 25% iedere kans zal aangrijpen te stelen of te frauderen
. 50% zo eerlijk of oneerlijk zal zijn als het systeem van interne controle toelaat.

Waarop deze cijfers zijn gebaseerd wordt in het artikel niet vermeld! Uit een ander onderzoek is gebleken dat als senior-management in een organisatie standaarden opstelt, deze zelf volgt en duidelijk maakt dat anderen in de organisatie hieraan zich ook dienen te houden, de kans op fraude en diefstal laag is. Waar standaarden ontbreken of management zich zelf hier niet aan houdt, zal dit gedrag ook op lagere niveaus meer voorkomen (vergelijk Equity Funding, waar op vrijwel ieder niveau fraude voorkwam, onafhankelijk van de beruchte directiefraude).

Hierna gaat Comer in op de vraag waarom mensen misdaden begaan. Hij komt hierbij tot drie bekende argumenten: Behoefte aan geld of een andere uitdaging, aanwezigheid van mogelijkheden (kennis van en toegang tot administratieve gegevens, activa e.d.) en de kans om niet ontdekt te worden. Tot slot blijkt dat erg veel fraudeurs voor zichzelf een rechtvaardiging hadden en zich ondanks een veroordeling toch eerlijk voelden.

Fraudemogelijkheden

Hoewel Comer stelt dat in beveiligingssystemen in het algemeen alleen aandacht wordt geschonken aan het ontnemen van de mogelijkheden tot frauderen en de overige elementen onterecht worden genegeerd, gaat ook hij in zijn aanbevelingen alleen op zoek naar waar zich mogelijkheden voor frauderen voordoen.
Daarbij komt hij tot de volgende opsomming, die in afnemende mate van waarschijnlijkheid is gerangschikt:

- gefalsificeerde computerinvoer (62% van de computer-fraudegevallen in de Amerikaanse overheidssystemen),
  (transactiegegevens, transactiecodes en communicatie);
- fouten, vertragingen en algemene tekortkomingen;
- manipuleren van stambestanden;
- manipuleren van wachtbestanden, tijdelijke tussenbestanden;
- manipuleren of vernietigen van uitvoer;
- aanbrengen van programmaveranderingen (in applicatie of systeemprogrammatuur);
- wijzigen Job Control Language (JCL), ten einde andere programmatuur of hardware te gebruiken.

Deze punten worden in het artikel aan de hand van beschreven fraudegevallen toegelicht.

Beveiliging

Ten slotte gaat Comer in op wat de onderneming aan computerbeveiliging zou moeten doen.

Vrijwel letterlijk overgenomen onderscheidt hij de volgende vijf stappen:

1. Senior management dient een klein beveiligingsprojectteam in te stellen.

2. Het projectteam, bestaande uit verschillende disciplines, dient een overzicht te maken van mogelijke risico's: openlijke en verborgen risicogebieden in de handmatige en geautomatiseerde gegevensverwerking, fysieke installatie en personeel.

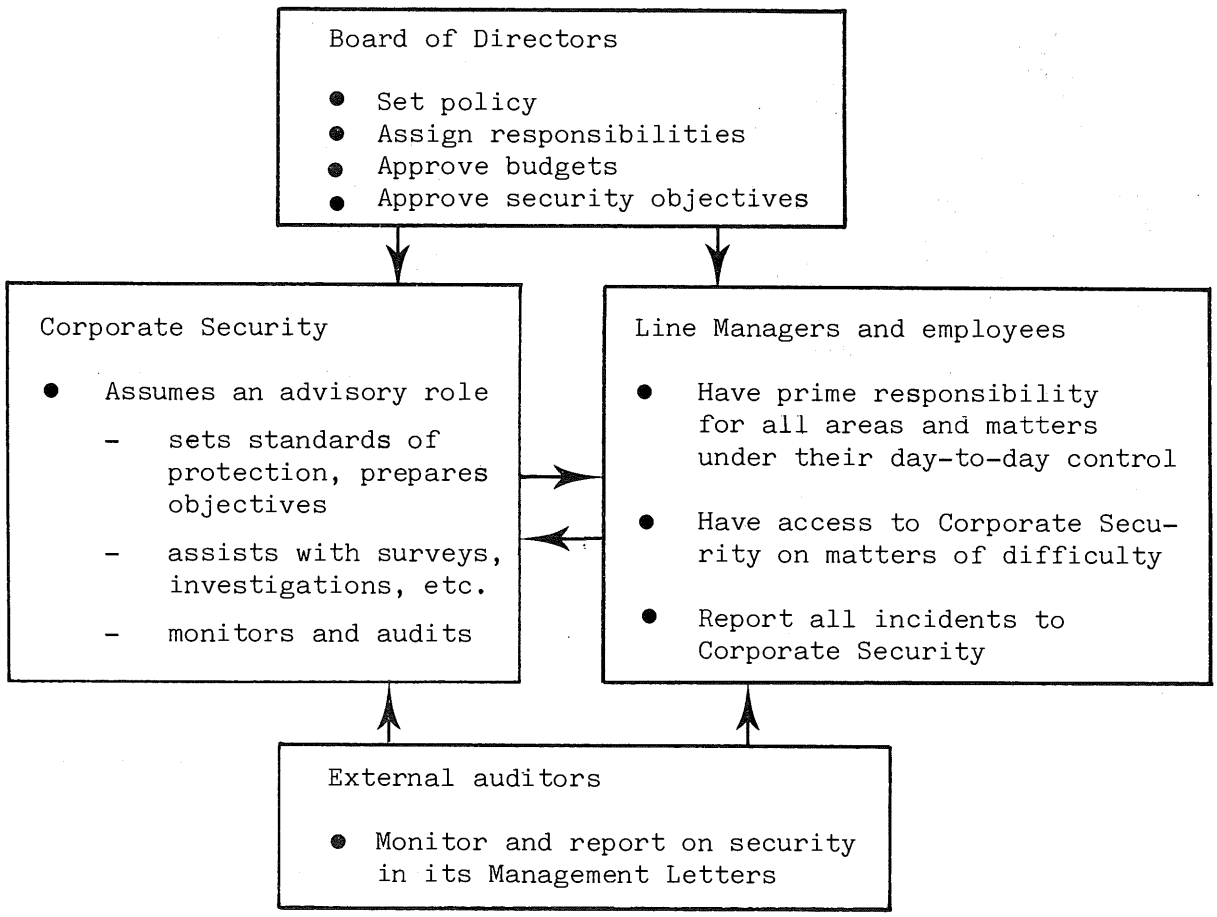
3. Geef voor deze risico's het maximaal mogelijke verlies aan.

4. Ga voor de belangrijke gebieden na of er op dit moment al sprake is van fraude en/of overige verliezen.

5. Leg de bevindingen van het projectteam aan de directie voor met de aanbeveling:
   - een "beveiligingspolitiek" op te stellen;
   - verantwoordelijkheden toe te wijzen;
   - waar mogelijk een centrale beveiligingsadviesgroep in te stellen;
   - richtlijnen voor het beveiligingsplan op te stellen;
   - een opleidingsprogramma voor het personeel op te stellen;
   - alle nieuwe personeelsleden op hun beveiligingsverantwoordelijkheden te wijzen;
   - een controlegroep in te stellen die de voortgang aan het management dient te melden.

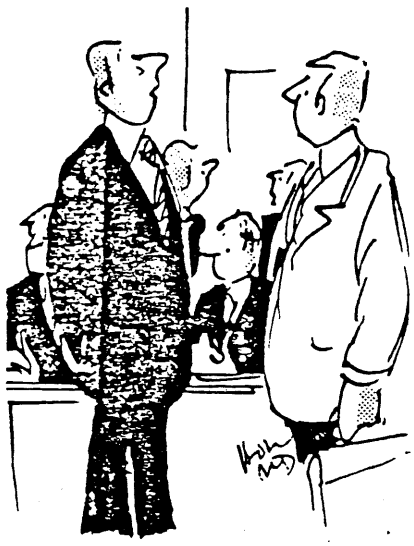
   Beveiliging is de verantwoordelijkheid van de directie. Individuele technieken zullen geen succes hebben zonder een door de hoogste leiding opgestelde beveiligingsstrategie.

In figuur 2 geeft Comer een schematisch overzicht van de taken van de directie, beveiligingsgroep, lijnfunctionarissen en de externe accountants met betrekking tot de beveiliging van de automatisering.

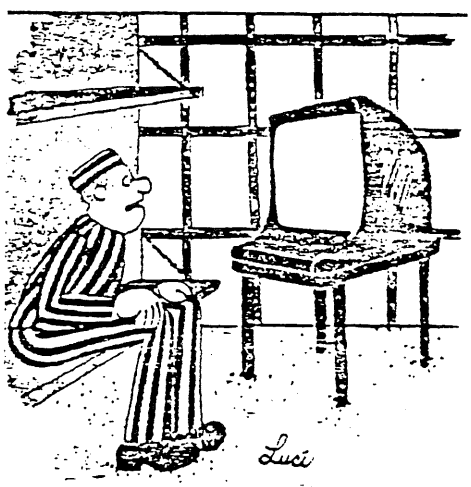


Figuur 2. Security responsibility structure.

In het kader van bovengenoemde punten wordt verwezen naar de artikelen van drs. H.C. Kocks in Compact 23 en 24 van lente en zomer 1981, waarin wordt ingegaan op risk-management en vooral op de daar deel van uitmakende risicoanalyse.



'We've eliminated all risk of computer fraud—we've gone back to using people'



'You In for Embezzling, Too?'

Name of technique
Black box method
Audit trail
Balanced methods
Integrated test facility
Test packs
Audit indicator
Systems control and audit review file (SCARF)
Tagging
Extended Records
Program Code Review
Systems management facilities and surveillance programs
Standard executable program checks

Figuur 3.

Outline of method	Effectiveness against fraud types: Input	TEC*	Master files	Patches	Exceptions and rejects
. computer treated as a black box . auditing around the computer . input/output and balance checks	High	Fair	High	Low	Fair/High
. tracing transactions through the system. possibly using random sampling techniques	Low	Low	Low	Low	Low
. review of controls in and outside computing . usually in addition to the audit trail method	Fair	Low	Fair	Low	Fair
. audit department establishes itself as a user branch of the computer being audited and monitors the result of built-in test data, whose results are predetermined	Low	Low	Low	Nil	Low
. similar to ITF only less formal use of the system is required . sample transactions (test packs) are fed through operational programs and the results checked against predetermined answers	Low	Low	Low	Nil	Low
. real input is 'tagged' and as it processes through the system interim results are produced and checked	Low	Low	Low	Low	Low
. continuous monitoring of operations at predetermined points of processing . results printed by exception	Low	Low	Low	Fair	Low
. similar to SCARF and Audit indicator	Low	Low	Low	Low	Low
. normal transaction records are extended to additional fields of data specifically for audit purposes	Low	Fair	Fair	Low	Fair
. desk top examination of source listings by an auditor or programmer	Low	Low	Low	Fair	Fair
. specially devised programs to pick out exceptions that may be symptomatic of fraud . can be designed/written by an auditor using Mark IV or similar retrieval languages	High	High	High	Fair	High
. duplicate programs kept by auditors and checked . sample transaction data run through duplicate and compared on an exception basis with normal operational runs on the same transaction data	Low	Low	Low	High	High

* Transaction Entry Code

Specifiek op fraude gericht noemt hij nog enkele bijzondere punten, waarbij hij benadrukt "think like a thief". Hij wijst met name op het snel onderzoeken van geconstateerde beveiligingsincidenten en de nodige extra aandacht voor correctiewerkzaamheden.
In figuur 3 geeft hij een overzicht van de meest gebruikte audit-technieken en de effectiviteit hiervan voor het ontdekken van fraude.

Tenslotte stelt hij

* Always thinks of computer fraud in accounting rather than technical terms. Consider how a fraud might be concealed and what impact it would have on double entry accounts, statistical records and budgets. Consider how the financial benefit of fraud, the conversion, can be obtained.

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

CULPRIT LIBRARY OF ROUTINES: EDP-AUDITOR

door: R.P. Bosman

Inleiding

Binnen de AC wordt voor het programmeren van controleprogrammatuur voornamelijk gebruik gemaakt van het retrieval pakket CULPRIT. Dit pakket aangevuld met een aantal "standaard" audit-routines wordt in zijn geheel verkocht als het pakket EDP-AUDITOR.
Van deze routines wordt, zeker ook door een stuk onbekendheid, zeer weinig gebruik gemaakt.
Het doel van dit artikel is te beschrijven welke functies deze routines in EDP-AUDITOR kunnen verrichten, zodat hiervan mogelijk een breder gebruik zal worden gemaakt.

Het werken met CULPRIT/EDP-AUDITOR

In tegenstelling tot wat men zou denken bij de term "routines", zijn de EDP-AUDITOR routines vrij flexibel in het gebruik. Het is betrekkelijk eenvoudig om instructies toe te voegen of juist stukken coding uit een routine te verwijderen.
Hierdoor kan de lay-out van een overzicht aan de specifieke behoeften worden aangepast, danwel de programmastructuur worden gemodificeerd.
Door middel van de zogenaamde argumentvelden (maximaal 9 per routine) kunnen variabelen aan een routine worden doorgegeven. Door het karakter van de programmeertaal (CULPRIT/EDP-AUDITOR is een report-generator) kunnen de standaardroutines en eigen programmadelen aan elkaar gekoppeld worden, waardoor in een job een maximum aantal van 100 verschillende overzichten geproduceerd kunnen worden.

De mogelijkheden van CULPRIT/EDP-AUDITOR

De EDP-AUDITOR routines zijn in te delen in een aantal hoofdgroepen, namelijk:

1. File footing routines.
2. Exception analysis routines.
3. Summary analysis routines.
4. Special processing routines.
5. Confirmation routines.
6. Sampling routines.
7. SMF routines.

Hieronder zal wat verder worden ingegaan op de betekenis en de mogelijkheden van de hoofdgroepen.

1. File footing routines

De routines in deze groep produceren per sleutelveld uit een bestand totalen van bedragen en recordtellingen.Deze routines worden vaak gebruikt om bedragen af te stemmen met die op reeds aanwezige lijsten om te zien of bijvoorbeeld een bestand compleet is.

2. Exception analysis routines

Deze routines signaleren of een veld een bepaalde waarde heeft overschreden of een verkeerd gegeven bevat op grond van opgegeven constanten. Deze routines worden onder andere gebruikt voor het signaleren van niet actieve rekeningen, nulfacturen en dubbele transacties.

3. Summary analysis routines

Deze routines produceren frequentieverdelingen in numerieke of grafische vorm van de waarden van een bepaald sleutelveld in een bestand. Zij worden gebruikt om een inzicht te krijgen in de samenstelling van een totaalbestand ten aanzien van een bepaald sleutelveld of specifieke gegevens. Afgedrukt kunnen worden aantallen, het aandeel in het totaalbedrag en totaalbestand en of een bepaalde waarde is overschreden. De toepassingsgebieden voor deze groep routines zijn veelerlei; enkele voorbeelden zijn:

a. het geven van een inzicht in de samenstelling van een massa;
b. het bepalen van de ouderdom van facturen en hun aandeel in het totale facturenbestand;
c. het aan de hand van de frequentieverdeling bepalen van variabelen voor een ander programma;
d. het controleren van de activiteit van b.v. grootboekrekeningen of groepen rekeningen.

4. Special processing routines

Deze routines hebben specifieke functies, zoals het trekken van de vierkantswortel, het rekenen met getallen met meer dan 15 significante cijfers (double precision arithmetic), het converteren van een datum van dagnummer naar datum en omgekeerd en het berekenen van de standaard-deviatie.

5. Confirmation routines

Confirmation routines ondersteunen de reeks van handelingen die nodig is voor controle door middel van saldobiljetten. De routines verzorgen het afdrukken van controletotalen, het drukken van adreslabels, standaardbrieven met variabele inhoud in enkel- of meervoudige vorm, controle- en foutenlijsten. In één programma kunnen de routines in elke combinatie worden gebruikt.

6. Sampling routines

In EDP-AUDITOR zijn tien soorten steekproeven beschikbaar, waaronder de interval sampling en stop-or-go sampling. Bij deze laatste methode kan de auditor een evaluatie maken over een zogenaamde subsample, een gedeelte van het totale te onderzoeken bestand. Tevens is het weer mogelijk om door middel van eigen coding bepaalde records of groepen record niet in een steekproef te laten meelopen. Bij de AC wordt alleen gebruik gemaakt van een eigen geschreven routine, de zeefmethode.

7. SMF-routines

Wanneer EDP-AUDITOR operationeel is onder het OS operating system, kan men gebruik maken van de SMF-routines. Deze routines produceren reports aan de hand van de SMF-files (system management facility), die gegevens bevatten van gebeurtenissen binnen het systeem, zoals job-initiatie, gemaakte veranderingen in libraries of datasets, verdeling van de computertijd, etc.
De analyse van door SMF-routines geproduceerde overzichten kunnen leiden tot een beeld van de integriteit, veiligheid en efficiëntie van het betreffende systeem.

Voorbeeld 1

Voor het produceren van een frequentieverdeling kunnen wij de volgende parameters gebruiken:

= MACRO AMVALRG1 (BALANCE 1000000 'NO' 'ACCOUNT BALANCE ANALYSIS')

= MEND

= COPY AMSCL1x5

De geproduceerde frequentieverdeling ziet er dan als volgt uit:

Figuur 1

Sample Report Listing

REPORT NO. 33 — VALUE RANGE ANALYSIS-EVEN INTERVALS — 04/23/80 PAGE 1

ACCOUNT BALANCE ANALYSIS

EACH RANGE BOUNDARY IN THE -TO- COLUMN HAS AN ADDITIONAL 99 CENTS UNDERSTOOD. THUS, 9.999 IS ACTUALLY $ 9.999.99.

BALANCE RANGE FROM	TO	NUMBER ON FILE	PERCENT OF FILE	FILE BALANCE WITHIN RANGE	PERCENT OF FILE	0 1 2 3 4 5 6 7 8 9 10 11 12	CUM. PCT.
NEGATIVES	9.999	1.470	84.5	2.519.686.27	13.1	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	13.1
10.000	19.999	95	5.5	1.312.562.72	6.8	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	19.9
20.000	29.999	44	2.5	1.065.797.12	5.5	XXXXXXXXXXXXXXXXXXXXXXXXXXX	25.4
30.000	39.999	31	1.8	1.102.007.72	5.7	XXXXXXXXXXXXXXXXXXXXXXXXXXXX	31.1
40.000	49.999	19	1.1	851.907.22	4.4	XXXXXXXXXXXXXXXXXXXXXX	35.5
50.000	59.999	15	.9	820.381.18	4.3	XXXXXXXXXXXXXXXXXXXXX	39.8
60.000	69.999	10	.6	640.126.52	3.3	XXXXXXXXXXXXXXXXX	43.1
70.000	79.999	10	.6	757.933.01	3.9	XXXXXXXXXXXXXXXXXXXX	47.0
80.000	89.999	5	.3	423.011.24	2.2	XXXXXXXXXXXX	49.2
90.000	99.999	5	.3	480.325.74	2.5	XXXXXXXXXXXXX	51.7
100.000	109.999	4	.2	410.066.50	2.1	XXXXXXXXXXX	53.8
110.000	119.999	6	.3	688.975.37	3.6	XXXXXXXXXXXXXXXXXX	57.4
120.000	129.999	4	.2	487.479.87	2.5	XXXXXXXXXXXXX	59.9
130.000	139.999	2	.1	274.040.44	1.4	XXXXXXXX	61.3
150.000	159.999	2	.1	310.060.17	1.6	XXXXXXXXX	62.9
160.000	169.999	2	.1	328.882.07	1.7	XXXXXXXXX	64.6
180.000	189.999	1	.1	189.058.42	1.0	XXXXXX	65.6
190.000	199.999	1	.1	198.097.12	1.0	XXXXXX	66.6
230.000	239.999	1	.1	233.037.58	1.2	XXXXXXX	67.8
250.000	259.999	1	.1	252.001.35	1.3	XXXXXXX	69.1
270.000	279.999	1	.1	274.799.01	1.4	XXXXXXXX	70.5
280.000	289.999	2	.1	573.110.03	3.0	XXXXXXXXXXXXXXXXX	73.5
290.000	299.999	1	.1	290.617.88	1.5	XXXXXXXX	75.0
430.000	439.999	1	.1	436.921.95	2.3	XXXXXXXXXXXXX	77.3
460.000	469.999	1	.1	466.657.37	2.4	XXXXXXXXXXXXXX	79.7
470.000	479.999	1	.1	479.286.30	2.5	XXXXXXXXXXXXXX	82.2
500.000	509.999	1	.1	500.000.00	2.6	XXXXXXXXXXXXXXX	84.8
570.000	579.999	1	.1	573.102.38	3.0	XXXXXXXXXXXXXXXXX	87.8
870.000	879.999	1	.1	873.570.37	4.5	XXXXXXXXXXXXXXXXXXXXXXXX	92.3
1.480.000	1.489.999	1	.1	1.485.400.03	7.7	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	100.0
	TOTALS-	1.740	100.0	19.298.902.95	100.0		

Betekenis van de parameters

= MACRO	is het statement voor het oproepen van een routine
= AMVALRG1	is de naam van de routine die de frequentieverdeling produceert
= MEND	signaleert het einde van de met argumentvelden veranderde source-module.
= COPY	kopieert een stuk programma bij de reeds opgeroepen routine.
AMSCL1x5	naam van het gekopieerde programmadeel. In deze routine verzorgt dit programmadeel de schaal van de grafiek (5x = 1%). Andere schalen zijn mogelijk.

Tussen de haken staan de z.g. argumentvelden. Door middel van deze parameters worden variabelen aan de routine doorgegeven.

BALANCE	is een numeriek invoerveld waarvan de waarde in de frequentie wordt uitgedrukt
1000000	is de grootte van het interval (in centen)
'NO'	betekent dat lege intervallen niet worden afgedrukt
'ACCOUNT BALANCE ANALYSIS'	is de titel die boven de output komt

Voorbeeld 2

Voor een controletoepassing, waarbij gebruik wordt gemaakt van saldobiljetten kan men een confirmation-routine oproepen door middel van het statement:

```
=   COPY AMCONFO4
```

Dit statement roept een programmadeel op dat een standaard saldobiljet afdrukt waarin de variabele gegevens (naam, adres, woonplaats, rekeningnummer, e.d.) kunnen worden opgenomen (zie figuur 2).

Figuur 2

N A T I O N A L S T A T E B A N K
123 street name
City, state 00000

December 15. 1982

William Wieckowski
42 Sunset Terr.
Akron OH44309

Dear customer,

From time to time, as part of our regular audit procedure, we ask our customers to confirm that their records are in agreement with ours. The information shown below is taken from our records of your ***installment loan*** account as of the audit date above.
This is not a request for payment.

Account number	2006393
Outstanding balance	6,753.16
Next payment due	11/29/83
Date charges due	.00
Remaining payments	6

Please sign and return this letter in the enclosed postage paid envelope. If your records do not agree. Additionally please write in the correct data. Your prompt reply will be greatly appreciated.

Very trouly yours.

Internal audit department

2006398 Please reply below 1

Date

Signature

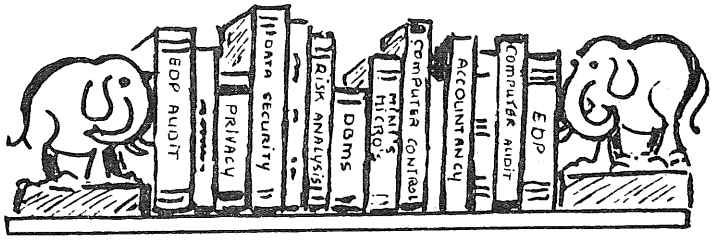
Comments

Voorbeeld van een enkelvoudig saldobiljet, geproduceerd door het programmadeel AMCONF04.

Het gebruik van EDP-AUDITOR in de praktijk

EDP-AUDITOR wordt in de praktijk nog niet zo vaak gebruikt. Dit komt onder meer omdat EDP-AUDITOR een Amerikaans produkt is en dus geënt is op de Amerikaanse markt; echter van een aantal routines, zoals file footing en exception analysis kan ook in een Nederlandse audit-omgeving meer gebruik worden gemaakt dan thans het geval is.

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



Boeken

BOEKBESPREKING

Titel: Auditing Data Systems
Serie: EDP Audit Guide Series
Auteur: W.E. Perry
Uitgever: EDP Auditors Foundation
Jaaruitgave 1981
A.C.-bibliotheeknummer: AC 384
Aantal bladzijden: 139

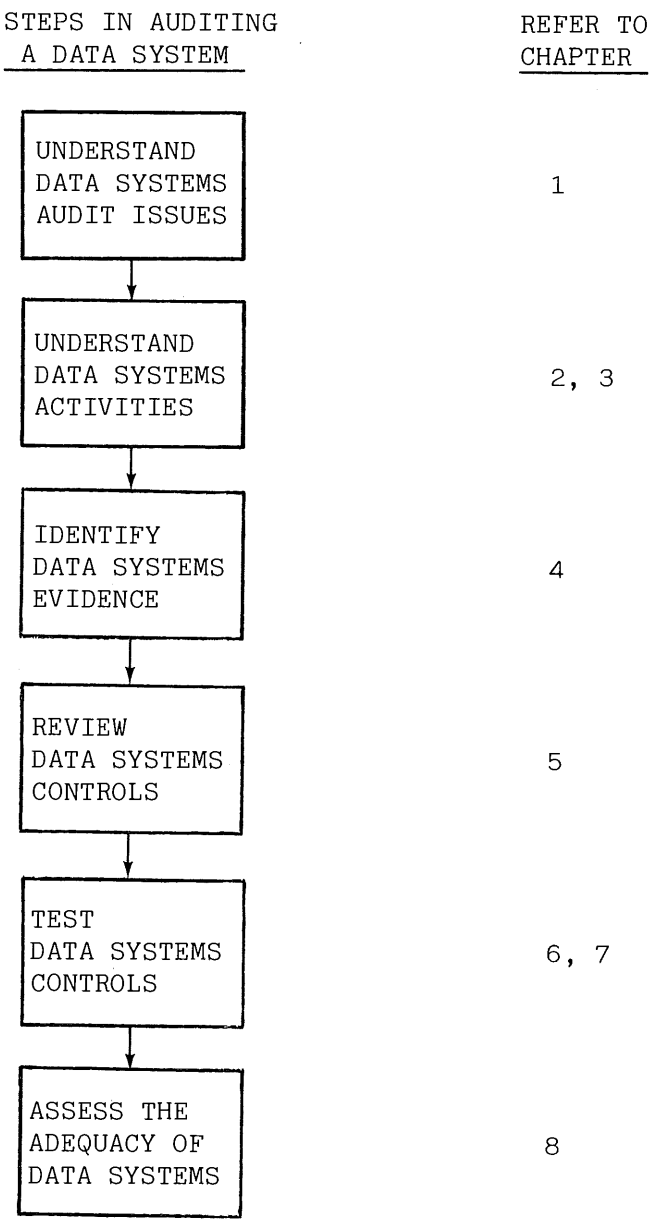
Inleiding

In het boekje wordt het onderzoek naar de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking in on-line, real time systemen beschreven op de wijze van een handleiding, geïllustreerd met vragenlijsten, overzichten van relaties van de zogenoemde audit issues en evidence met functies/activiteiten, voorbeelden van werkpapieren, e.d.

Doel van het boekje is vooral de algemene accountant inzicht te geven in specifieke "nieuwe" eigenschappen en problemen van technisch complexe toepassingen. De probleemstelling betreft dan ook de verandering die introductie van gegevenscommunicatie- en gegevensbanksystemen veroorzaakt en die tot gevolg kan hebben, dat de traditionele automatiseringsorganisatie, gebruikerscontroles en aanpak van de accountantscontrole ontoereikend zijn geworden. Een en ander kan de (verdere) inschakeling van EDP-auditors nodig maken.

Het boekje bestaat uit acht hoofdstukken, die aan het onderstaande structuurschema van een accountantsonderzoek zijn gerelateerd.

THE DATA SYSTEMS AUDIT PROCESS



Hoofdstuk 1: Data systems audit issues

In dit hoofdstuk worden dertien aandachtsgebieden opgesomd, waaronder integriteit van de gegevensbank, waarop bij on-line real time gegevensverwerking controleproblemen zijn te verwachten. Per gebied is een vijftal vragen opgenomen aan de hand waarvan bepaald kan worden:

1. waar inzet van de beschikbare onderzoekscapaciteit voldoende nut zal afwerpen;
2. of de problemen van dien aard zijn, dat als methode een evaluatie van specifieke interne controles nodig is, of dat "auditing around" mogelijk is.

Hoofdstuk 2: Data systems activities

Er worden negen functies/activiteiten opgesomd met betrekking tot on-line real time geautomatiseerde gegevensverwerking. Per functie wordt een taakbeschrijving gegeven en wordt vermeld of het hoger management, de gebruiker of automatiseringspersoneel verantwoordelijk is. In een matrix wordt per aandachtsgebied aangegeven welke functies een rol spelen. Op basis van de vragenlijst uit hoofdstuk 1 en de matrix kan worden bepaald welke functies voor verder onderzoek in aanmerking komen.

Hoofdstuk 3: Locating issues and activities in the operating environment

Het doel van dit hoofdstuk is de onderzoeker:

1. een beeld te geven van de belangrijkste kenmerken van een on-line gegevensverwerkend systeem;
2. in staat te stellen een bepaald on-line systeem te classificeren als een systeem met potentieel weinig of veel risico;
3. de werking van een on-line gegevensverwerkend systeem te verklaren. Dit gebeurt aan de hand van een systeemmodel;
4. in het beschreven model die punten te leren onderkennen waar de eerder beschreven functies worden uitgevoerd, alsmede de voornaamste middelen tot beheersing van die functies (control-points and controls).

Hoofdstuk 4: Data systems audit evidence

In dit hoofdstuk wordt de term elektronisch bewijs geïntroduceerd. Elektronisch bewijs wordt gedefinieerd als: een bewijsmiddel, dat uitsluitend op computermedia is opgeslagen. Het elektronisch bewijs ontleent de mate van kracht aan de procedures die worden gebruikt om informatie in te voeren, te verwerken en op te slaan alsmede aan de mogelijkheid tot gebruik in de accountantscontrole.

Het elektronisch bewijs, hard-copies (logs) en de procedures die de integriteit van het bewijs moeten waarborgen worden samengevat onder de naam data systems evidence. Van deze bewijzen worden 21 soorten beschreven. Tevens wordt in een matrix per soort bewijs de gebruiksmogelijkheid voor de beheersing van de eerder beschreven functies aangegeven.

Aangeraden wordt in het planningsstadium, dat wil zeggen in het voorbereidend onderzoek, een inventarisatie te maken van de "auditable evidence".

In vier hoofdstukken is, volgens de methode van opdeling van controle-objecten in hanteerbare delen en een effectieve keuze uit delen, de grondslag gelegd voor het plannen van het (eventuele) verdere onderzoek. De planning omvat mede de te volgen procedures en de te gebruiken middelen en technieken in "a realistic approach".

Hoofdstuk 5: Reviewing data systems controls

Nadat in beginsel besloten is tot "een steunen op interne controle" dienen de opzet (en nadien de werking) van interne controles ten aanzien van de voor onderzoek geselecteerde activiteiten te worden onderzocht.
Het is echter ook mogelijk dat, in een traditionele controle, "de belangstelling" beperkt is tot de hoofdlijnen en meer uitgaat naar bijvoorbeeld security.

Het beoordelen van de opzet van interne controles op achtereenvolgens te onderzoeken activiteiten in functies wordt, overeenkomstig het nieuwe en complexe karakter daarvan, in 5 stappen onderverdeeld, namelijk

1. Inventarisering van risico's (threats).
2. Bepaling van de ernst van het risico.
3. Identificatie van de beheersingstechniek (control).
4. Bepaling van de sterkte van de beheersingstechniek (control strength).
5. Beoordeling van de toereikendheid van de beheersingstechnieken.

Per functie wordt in een vragenlijst geïnformeerd naar een vijftal key-controls. De strekking van de vragen komt overeen met de beide in KKC gehanteerde vragenlijsten. Per control wordt een aanbeveling gedaan voor het geval van afwezigheid of ontoereikendheid. Enkele modellen van werkpapieren zijn toegevoegd.

Afsluitend vindt een over-all beoordeling plaats, rekening houdend met in de opzet aangetroffen compensaties van zwakheden en wordt inzicht gevormd over eigen aanvullende controlemogelijkheden.

Hoofdstuk 6: Data systems audit practices

In het kort wordt de noodzaak en beschikbaarheid beschreven van technieken (tools) ten behoeve van de beoordeling van de werking van het systeem van interne controle, gericht op de vorm van het informatieverwerkend proces: on-line, real time.

Tevens worden de vaardigheden die de onderzoeker moet bezitten opgesomd.

Per controletechniek (er worden er twaalf genoemd) zijn de volgende gegevens opgenomen:

1. Een beschrijving van de techniek.
2. De evidence die ermee wordt onderzocht.
3. De voordelen verbonden aan het gebruik van de techniek.
4. De nadelen verbonden aan het gebruik van de techniek.

Hoofdstuk 7: Designing data systems audit tests

Het beoordelen van de werking van het systeem van interne controle (compliance test) wordt beschreven in drie stappen:
1. Ontwikkelen van een testplan
2. Uitvoeren van de test
3. Evalueren van de testresultaten.

Ten behoeve van stap 1 is per functie een werkblad opgenomen waarop per maatregel van interne controle een aanbeveling is opgenomen ten aanzien van de test en de controletechniek.

Hoofdstuk 8: Evaluating data systems controls

Dit hoofdstuk bevat een aantal richtlijnen voor de eindevaluatie en voor de presentatie van de onderzoekresultaten.

Conclusie

Het boekje is systematisch van opzet en geeft de lezer in een gering aantal pagina's een beeld van de wijze waarop een onderzoek bij on-line, real time informatiesystemen kan plaatsvinden.
Ook in het kader van kleinschalige automatisering kunnen veel van de behandelde vragen en technieken worden toegepast. Jammer is, dat het boekje weinig bevat over controles die uitgevoerd kunnen worden indien de opzet en/of de werking van interne controle onvoldoende is bevonden.

Door de grote nadruk op nieuwe problemen die voortvloeien uit datacommunicatie, transactiegewijze verwerking en het gebruik van databases, verdwijnen de te behouden elementen van wat de auteur noemt de traditionele aanpak, nagenoeg uit het gezichtsveld. Het resultaat is een benadering die veel meer doet denken aan het zelfstandig onderzoek van de zogenaamde algemene of paraplumaatregelen in automatiseringsafdelingen dan aan het onderzoek van een informatiesysteem.
Niettemin vormt het boekje aanbevolen lektuur.

Tijdschriften

door D. Jansen Heytmajer, J.L.H. Kooijman en drs. B.M. de Vries

Auditor concerns with EFTS

Overdruk van een presentatie voor een CICA-symposium on computers and auditing van november 1981.
Presentatie door Gerald W. Lee, CIA.
CA-magazine februari 1982.

In het artikel wordt nader ingegaan op de middelen die aanwezig, of aanbevelenswaardig zijn ter beheersing van en controle op de werking van Electronic Funds Transfer Systemen (EFTS).
EFTS is een verzamelnaam voor een scala van geautomatiseerde systemen die één ding gemeen hebben: het verwerken van betalingsverkeer. De accountant in Nederland heeft hoofdzakelijk te maken met SWIFT als het belangrijkste middel voor afwikkeling van interbancair betalingsverkeer. In de Verenigde Staten gebeurt op dit gebied aanzienlijk meer; zij het dat dit niet altijd beter of efficiënter behoeft te zijn dan in Nederland. (Men denke bijvoorbeeld aan het gebruik van cheques, dat in de VS nog steeds in een grote behoefte blijkt te voorzien.) In de VS zijn naast money-transfer systems, zoals Swift, Bank-Wire en Fed-Wire nog een groot aantal faciliteiten, ook voor het publiek, waarvan genoemd worden:

- opname- en stortingsfaciliteiten via automated-teller-machines (wordt in Nederland hier en daar geïntroduceerd);
- kassiersfaciliteiten in warenhuizen ten behoeve van personeel en klanten (courtesy counters);
- point-of-sale terminals. Directe afrekening met klanten in winkels door verbinding van P.O.S.-terminals met bank-computers.
- telephone-banking. Biedt o.a. particulieren de mogelijkheid om met behulp van hun eigen tip-toetstelefoon rekeningsaldi naar believen over te hevelen van de ene bank naar de andere.

Voorts zijn in deze circuits nog actief de zogenaamde automated clearing houses, die de distributie van betalingen en ontvangsten naar en van klantenrekeningen bij aangesloten financiële instellingen verzorgen.

Door de aanwezigheid en het gebruik van directe datacommunicatieverbindingen tussen de aangesloten instellingen is de snelheid waarmee transacties worden verwerkt, enorm toegenomen. Er is weinig of geen menselijke tussenkomst in dit proces en de hoeveelheid geld die op deze wijze wordt overgemaakt heeft gigantische afmetingen aangenomen.

Het is met name de snelheid van verwerking en het ontbreken van menselijke tussenkomst die aanleiding geven tot bezorgdheid. Wanneer een foute of frauduleuze transactie eenmaal door het terminalsysteem is geaccepteerd en doorgegeven aan het overboekingssysteem, is zij in feite niet meer te stoppen.

Het artikel draagt als ondertitel dan ook:

TOO MANY RISKS FOR COMFORT

Karakteristieken van EFT-systemen

In het artikel worden EFT-systemen uitgebreid toegelicht. Aan de orde komen de processtappen (identification, verification, authentication, funds-transfer en settlement). Met name identificatie-procedures krijgen grote nadruk (agressieve toegangsbewaking). Over settlement, het afwikkelen van saldi tussen de deelnemers in het systeem, worden een groot aantal adviezen gegeven voornamelijk betrekking hebbend op een goede aansluiting tussen alle vormen van al dan niet geautomatiseerde administraties van de partijen die bij die afwikkeling zijn betrokken.

Ten behoeve van controleerbaarheid, wordt aanwezigheid van "audit-trails" geëist, tevens bruikbaar voor recovery, terugdraaien van foutieve transacties en voor controle op inbraakactiviteiten.
Onder het hoofd "monitoring" worden procedures genoemd om de berichten, die in het netwerk rond gaan te bewaken en te volgen om te voorkomen dat berichten blijven hangen, niet worden bevestigd binnen een bepaalde tijd en om storingen voldoende tijdig op te lossen voordat deze te grote vormen aan gaan nemen.

Switched EFT-system security

Hier wordt een ander risico-gebied aangegeven, dat in verband staat met gemeenschappelijk gebruik (sharing) van EFT-systeemfuncties door verschillende aangesloten instellingen. Gesteld wordt dat:

"No single financial institution is in a position to control the security, auditability and internal controls of the total EFT-network."

In principe is het namelijk mogelijk dat een klant van Bank A de terminals, de communicatieverbindingen en computerprogramma's van Bank B gebruikt voor het uitvoeren van transacties.
Wanneer bij Bank B deze resources slecht worden beheerd, zal Bank A, die verantwoordelijk is voor de bewaring van door die klant toevertrouwde gelden, daardoor grotere risico's lopen.
De conclusie wordt getrokken, dat de betrouwbaarheid en beveiliging van het totale EFT-systeem nooit beter zal zijn dan de betrouwbaarheid en beveiliging die heerst bij de slechtst georganiseerde deelnemer aan het systeem (weakest-link theory).
Geadviseerd wordt, een minimum standaard overeen te komen met betrekking tot maatregelen van interne controle, beveiliging en reconstructie waaraan alle deelnemers zich zullen houden.

Overige aspecten voor de switched EFTS

- Message routing verification.
  Het bezorgadres van een bericht moet een geldig punt zijn in het netwerk; bevestiging van een ontvangen bericht door de ontvanger onder vermelding van identificatie van de ontvangende terminal; aanhouden van history-logs van de ontvangen en verzonden boodschappen; zorgen voor efficiënte verwerking van boodschappen om vertragingen te vermijden.

- Control over unauthorized line monitoring.
  Codewoorden verbergen in het bericht zelf, en/of het bericht verpakken tussen allerlei andere berichten (bulk message techniques) teneinde afluisteren en modificeren te bemoeilijken.
- Message delivery control.
  Procedures die er voornamelijk op gericht zijn, berichten te kunnen blijven identificeren (soort, waar vandaan, waarheen) ook en vooral wanneer problemen optreden zoals lijnstoringen en computerfouten.

Auditing the total EFT system

"Unfortunately for the auditor, a complete review of the system requires an evaluation of the entire computer system, not just the terminal servicing modules and the associated access controls and manual controls. The most difficult attribute for the auditor to evaluate is the integrity of the entire system, which is composed of terminals, a communications network, the computer itself, the data base and the switches. Determining whether or not the control system is continually in place and functions, whether it can easily be circumvented or whether undetected errors can enter the process, can be very difficult. To do this evaluation, the auditor must not only understand the logic of electronic funds transfer systems, but must also be well versed in all facets of computer and communication technology."

Als een mogelijke aanpak voor een evaluatie van EFT-systemen wordt geadviseerd het systeem onder te verdelen in de noodzakelijke eigenschappen die het moet bezitten (security, integrity and recoverability) en daarna die punten te evalueren die aangeven dat deze eigenschappen aanwezig zijn.

Terminal security and integrity

Terminal locaties onderverdelen in vriendelijke en onvriendelijke omgeving. Vriendelijk is: binnen de bank zelf, loketten in winkels etc.; onvriendelijk is bijvoorbeeld de automatic teller machines die aan de buitenmuur van banken zijn opgehangen. Belangrijkste punten:
- voorkomen van transactie-invoer buiten het identificatie-, verificatie- en authenticatieproces om;
- voorkomen dat anderen dan de bevoegde gebruiker de terminal kunnen gebruiken (automatische sign-off, zowel na gebruik als wanneer abnormale gebeurtenissen plaatsvinden; onderdrukken passwords etc.).

Data transmission security and integrity

Encryptie technieken worden hier genoemd, alsmede opname in de boodschap van terminal- en operator-identificaties, datum- en tijdgegevens, route-informatie, statusgegevens en informatie ten behoeve van tracing en audit-doeleinden.

Line and modem security and control

Bij ontwerp van het netwerk, de aanschaf van kabels, interfaces etc. moet voortdurend aandacht zijn besteed aan (overigens bekende) aspecten met betrekking tot uitval, misbruik of onbevoegd gebruik, risico van aankoppeling van onbevoegde (niet tot het systeem behorende) terminals, aftappen van lijnen of inbreken in de lijnen zelf met behulp van onbevoegde terminals. Voorts uiteraard aandacht voor alternatieve routes (line back-up) en deze alternatieve paden dan ook identificeerbaar maken voor controle- en tracingdoeleinden.

Information processing integrity, security and recoverability

- Integrity:
  De werking van het systeem conform de specificaties. In principe is het onmogelijk om bij grote EFT-systemen alle denkbare combinaties van condities te determineren en te testen. De onvoorspelbaarheid van de werking van een dergelijk systeem kan echter worden geminimaliseerd door gebruik te maken van goede programma-testprocedures.

- Security:
  Evalueren van de mogelijkheden die in de organisatie aanwezig zijn om de eigen computeractiviteiten te beheersen, te beschermen en te controleren op toegang en gebruik.
  Hierbij behoren tevens maatregelen ten aanzien van back-up en recovery.

- Recoverability:
  Betreft de mogelijkheid van de organisatie, de verwerkingscapaciteit weer te herstellen in geval van een calamiteit. Het systeem moet daarbij gecontroleerd down gaan ("must fail according to specifications") dat wil zeggen dat onafhankelijk van het type calamiteit, het altijd zeker moet zijn dat transacties niet zoekraken of tijdens recovery worden gedupliceerd.

Disaster contingency plans for EFTS

EFT-systemen geven op dit punt de grootste problemen voor contingency planners.
De systemen zijn geheel afhankelijk van het communicatie netwerk; wanneer het nodig zou zijn om de werklast over te brengen naar andere locaties (als gevolg van break-down of een calamiteit) dan moet het complete communicatienetwerk opnieuw worden gedefinieerd.
Dit is een tijdrovende, moeilijke en kostbare aangelegenheid. De accountant zal dan ook moeten vaststellen of een adequate planning ten aanzien van netwerk-herstel aanwezig is.

Audit conclusions

Nadat de accountant de evaluatie van het gehele systeem heeft voltooid en de toegangsbeveiliging en schakelproblematiek heeft beoordeeld, kan hij conclusies trekken ten aanzien van security, reliability en recovery van het Electronic Funds Transfer System.

Bovendien moet de accountant de administratieve procedures voor elk type EFT-service beoordelen.
Na deze activiteiten kan de accountant tenslotte bepalen in hoeverre hij zal "steunen" op de interne controles in het systeem zelf.
De volgende stap zal dan zijn, het bepalen van de omvang van de cijfer-controles die nodig zijn om een oordeel te verkrijgen over de jaarcijfers.

Unresolved EFT audit problems

Problemen die door de schrijver gesignaleerd worden:
- Hoe kom je aan geschoold personeel voor de controle van EFT-systemen. Nodig is namelijk een combinatie van accountant, EDP-auditor, EDP-technicus en communicatiespecialist om een complex EFT-netwerk te begrijpen en te evalueren.
- Controlekosten versus risico's. Hier de vraag hoe diep de accountant moet gaan bij zijn onderzoek en advies. Het is zeer moeilijk voor een accountant om de invloed te meten die een bepaalde zwakte van het systeem kan hebben op de financiële gegevens. Hiervan is ook weinig statistisch materiaal beschikbaar.
  Nog moeilijker wordt het in een dergelijke situatie om de leiding van de cliënt - zonder te beschikken over goede kosten/risico-gegevens - ertoe te brengen extra geld uit te geven voor aanvullende hardware en software die door de accountant wenselijk wordt geacht op grond van zijn oordeel over de aanwezige zwakke punten.

Encouraging signs not enough

Het artikel besluit met het volgende:

"Despite the problems - however - accurate, secure, high reliability EFT-systems can be and are being designed, implemented and audited, and errors and fraud in EFT-systems are not yet out of control. Although some losses are being incurred and, in many systems, the risks are too high, there are many encouraging signs that system designers and auditors are doing a better job in the EFT-system area.
Nevertheless, within the next five years, much need to be done to improve EFT-systems, or larger problems will most certainly occur."

Future applications of cryptography
Computers & Security 1 (1982)

Charles C. Wood

De beveiliging van informatie door cryptography of wel gegevensvercijfering, kan niet los gezien worden van andere beveiligingsmaatregelen, zoals fysieke toegangsbeveiliging, logische toegangsbeveiliging (bijvoorbeeld logon en applicatiesysteemcontroles), personeelsbeleid (betreffende het gebruik van computerfaciliteiten door het personeel en rechten ten aanzien van de gedurende werktijd ontwikkelde software). Naast vercijfering kunnen andere methoden van gegevensbeveiliging worden onderscheiden, zoals fysieke beveiliging van communicatielijnen (bijvoorbeeld het installeren van een ring van communicatielijnen binnen een gebouw of binnen een beschermd gebied), gebruik van glasvezelverbindingen (waardoor het aftappen van gegevens wordt bemoeilijkt), gebruik van multiplexors en concentrators, data compressietechnieken (waardoor lege tussenruimten en onnodige tekens worden geëlimineerd), foutdetectie- en correctiecodes en andere controlemiddelen, die voor een deel als alternatieven van vercijfering kunnen worden beschouwd.
Om economische redenen zal vercijfering, een relatief dure beveiligingsmaatregel, niet eerder worden geïmplementeerd dan na toepassing van qua kosten effectievere maatregelen.
Ten behoeve van de analyse van controlemaatregelen wordt voorgesteld een risico-analyse uit te voeren. Op grond van deze risico-analyse kan worden besloten tot beveiliging middels vercijfering.
Indien systemen veiliger worden door het toepassen van de hierboven genoemde elementaire beveiligingsmaatregelen, zal een toenemende behoefte ontstaan om de meer complexe beveiligingsbedreigingen te lijf te gaan.
Het feit, dat slechts 2 gevallen van gemelde lijnaftapping voorkomen in de "computer abuse files" van het Stanford Research Institute, (een bestand met meer dan 700 gevallen van inbreuk op de beveiliging) geeft aan, dat lijnaftapping een bedreiging is, die door de meer alledaagse bedreigingen, zoals manipulatie van invoergegevens, wordt overschaduwd.

Toch zal vercijfering in vele systemen worden ingevoerd niet zozeer op basis van een risico-analyse, maar omdat wettelijke voorschriften hen hiertoe aanzetten.

Gegevensvercijfering wordt met name toegepast om geheimhouding van gegevens uit hoofde van privacy, vertrouwelijkheid of beveiliging te bereiken. Het is zowel mogelijk tekst en gegevens als ontvangst en verzendadressen te coderen.

Gegevensvercijfering kan ook de betrouwbaarheid van de gegevens ten goede komen. Door middel van de cipher-feedback methode, die tekst omzet in cijfers, zal het wijzigen of verwijderen van zelfs één bit leiden tot voor de gebruiker onbegrijpelijke tekst.
Gegevensvercijfering kan ook gebruikt worden voor de bevoegdheidscontrole van gebruikers door voor ieder bericht een andere sleutel te gebruiken.

Om een objectief beeld te geven van de voor- en nadelen van vercijfering worden enige operationele/technische risico's ten gevolge van vercijferingssystemen genoemd:
- het verlies van vercijferingssleutels, waardoor gegevens ontoegankelijk worden;
- het niet goed functioneren van vercijferingsapparatuur, zodat coderen en decoderen verricht worden met behulp van een fout algoritme of sleutel, hetgeen kan resulteren in verloren gegane of onbegrijpelijke gegevens;
- het mislukken van de tijdige inbreng van nieuwe sleutels die wel bij andere delen van een communicatiesysteem zijn ingebracht vermindert de systeembeveiliging en kan de verwerking verstoren.

Verscheidene toepassingen van moderne gegevensvercijfering zullen in de naaste toekomst beschikbaar komen. Genoemd worden onder andere:
- personal encryption keys (ook wel genoemd digital signature): een unieke sleutel, tevens bruikbaar om te bewijzen dat aan een bericht niet geknoeid is en dat een gebruiker op een bepaald tijdstip bevoegd was;
- user or system anonymity; de anonimiteit wordt bereikt, doordat tussenpersonen de gecodeerde berichten verzenden; in vele opzichten is deze faciliteit te vergelijken met het gebruik van brievenbussen bij het traditionele postverkeer;
- public key cryptography, een nieuwe ontwikkeling die grote mogelijkheden verschaft in de dienstverlening terzake van gedigitaliseerde handtekeningen, anonimiteit of functiescheiding;
- het gebruik van verschillende sleutels voor coderen en decoderen.

Toepassingsgebieden van gegevensvercijfering zijn:
- Electronic Funds Transfer Systems, de meest geschikte hedendaagse toepassing vanwege de hoge financiële risico's.
- Electronic Mail Systems.
- Viewdata.
- Teletext.
- Timesharing servicebureaus.
- Database informatiediensten.
- Informatie in de vorm van computerprogramma's.

Een breed scala van vercijferingsapparatuur voor zowel analoge als digitale gegevens wordt aangeboden.
Transformatie van geluidssignalen van gegevens van computersystemen van gegevens in video of in grafische vorm, kan door de thans aanwezige apparatuur afgehandeld worden.

Een belangrijk probleem is de vertraging, die ontstaat ten gevolge van de codering/decodering. Tegenover dit nadeel staat echter het voordeel van een grotere beveiliging.
Verwacht wordt, dat de toekomst flexibele ("gebruikersvriendelijke") vercijferingsapparatuur zal opleveren.
Met behulp van deze apparatuur kunnen delen van berichten en/of van bestanden selectief gecodeerd worden.

Toekomstige trends:
- ontwikkelingen worden overwogen, waarbij het mogelijk is in beperkte mate direct de gecodeerde gegevens te verwerken. Het proces van decodering zou daarbij overgeslagen kunnen worden;
- de automatisering van het "key-management" dat wil zeggen de distributie en beveiliging van de geheime parameters, die in het coderings-/decoderingsproces worden gebruikt;
- meer nadruk op end-to-end vercijfering in plaats van de nu gebruikelijke link-by-link vercijfering. End-to-end vercijfering omvat de verplaatsing van een gecodeerd bericht vanaf het ene eindpunt van een verbinding naar het andere.

Verwacht wordt, dat vercijfering steeds meer zal worden toegepast. Vercijfering zal als een optie bij verschillende informatie- en communicatiesysteemapparatuur worden aangeboden. Toch voorziet Wood, dat verbeteringen (lagere kosten, gemakkelijker gebruiksmogelijkheden en bredere acceptatie van protocolstandaarden) noodzakelijk zijn, alvorens vercijfering op grote schaal geaccepteerd en gebruikt zal worden.

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

Automatisering Beveiliging Controle NIEUWS

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

Automatisering

Het onderwerp Conversie komt met enige regelmaat in de literatuur aan de orde. Onderstaand berichtje, dat wij aantroffen in De Zaanlander van 14 oktober jl., toont aan dat een conversiefout nog lang kan nawerken.

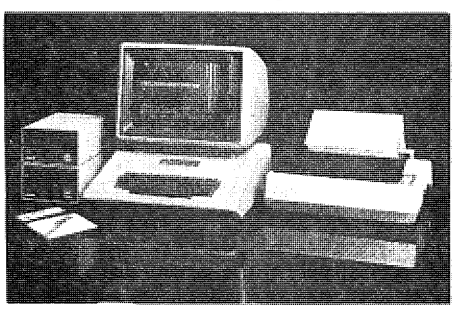
Computer-fout van negen ton

Een automatiseringsfout in de aanslaggegevens van onroerend-goed-belasting over 1981 gaat de gemeente Vlaardingen ruim 900.000 gulden kosten.
Bij een onderzoek is namelijk gebleken dat bij het invoeren van het oude ponskaartensysteem in het nieuwe computersysteem een oppervlakte van 240.000 vierkante meter te veel is opgevoerd.
Daardoor dacht men toe te kunnen met een lager tarief dan achteraf nodig bleek. Gevolg hiervan is dat de opbrengst bijna negen ton lager is dan men had verwacht. Voor 1981 wordt dit tekort uit de saldireserves betaald. Naar alle waarschijnlijkheid zal dat ook met het tekort over dit jaar gebeuren.

Jammer is dat niet aangegeven is wat de oorzaak is geweest van die fout. Dit neemt echter niet weg dat over de conversieproblematiek in het algemeen licht wordt gedacht. Door het uitlopen van de ontwikkelingstijd van een systeem wordt de planning van de conversie nogal eens vergeten. Alles moet met een zekere haast geschieden; dit kan dan leiden tot een verkeerd bestand als uitgangssituatie voor verwerking met het nieuwe systeem. De gevolgen kunnen groot zijn!!

De kop van onderstaand stukje is voor vele lezers wellicht niet nieuw. Het woord micro is reeds meer "gevleugeld" dan mini. De inhoud van het stukje is ook niet zo opzienbarend. Wel de laatste alinea. De weg in "subsidieland" schijnt moeilijk te zijn.

Micro verdringt mini



Een kwart van de computerbezitters in de sectoren industrie, groothandel, transport en zakelijke dienstverlening is voornemens op korte termijn (minder dan een jaar) zijn apparatuur te vervangen dan wel uit te breiden. Daarbij bestaat een toenemende behoefte aan externe adviezen.

Dat blijkt uit een Nipo-onderzoek dat in opdracht van Amrobank en Vereniging van Importeurs en Fabrikanten van Kantoormachines (VIFKA) is gehouden. Het huidige computerbezit bestaat voor 25% uit micro-computers, maar bij ondernemers die voor de eerste maal een computer willen hebben, is een grote verschuiving naar microcomputers beneden de ƒ 50.000 te bespeuren, waardoor het percentage van deze nieuwe aanschaffingen tot boven de 50 zal stijgen. Het aandeel van de mini-computer zal daardoor dalen van thans bijna 60% tot minder dan 30%. De helft van het computerpark is nog geen drie jaar oud. Niemand heeft echt spijt van de aanschaf en ruim één op de vijf ondervraag-den is van mening dat zij beter op een eerder tijdstip hadden kunnen kopen. Wel waren er ten aanzien van de hardware soms problemen met de geheugencapaciteit en met de verwerkingssnelheid. Bij de software liggen de voornaamste obstakels op het gebied van documentatie en uitbreidingsmogelijkheden.
Overigens blijken de bedrijven maar matig op de hoogte te zijn van bestaande subsidieregelingen voor de aanschaf van computers. Slechts een op de twaalf weet concrete regelingen te noemen, maar zo'n 20% heeft er nog nooit van gehoord.

Elseviers Magazine
13.11.1982

CODASYLRAPPORT GEREEDGEKOMEN

De Canadese regering heeft enkele weken geleden een rapport gepubli-ceerd, dat is geschreven door de eindgebruikerscommissie Codasyl. Deze commissie heeft zich beziggehouden met de databasestructuur Codasyl, en hoe deze door de eindgebruiker te benaderen moet zijn. De bevindingen van de commissie zijn neergelegd in een rapport. Hierin zijn alle eisen opgenomen, waaraan een eindgebruikersgedeelte van een Codasylsysteem moet voldoen wil ook gebruik door leken op computergebied mogelijk zijn.
Het rapport gaat nader in op de architectuur van het gewenste sys-teem, alsmede de diverse manipulatietalen, die nodig zijn om de bestanden te kunnen benaderen en wijzigen. Op het moment is men bezig, deze eisen nader bij te stellen en aan te passen. Te gelege-ner tijd zullen de nieuwe eisen worden neergelegd in een tweede rapport. Tot die tijd hoopt de commissie de nodige feed-back te krijgen van gebruikers en andere belanghebbenden.

Automatisering Gids nr. 46
17.11.1982

ANNONCERINGEN

Tape Management for VM

VM Software, Inc. has announced the release of VMTAPE, a tape management software product for IBM's VM/370, VM/SP, and CMS environments. The initial version of VMTAPE is intended for the installation with VM and either OS/VS1 or MVS which desires a single installation tape library and tape management catalog.
VMTAPE provides standard label and non-labeled tape support, password and expiration date protection, tape drive and tape volume management and full data set control within the CMS subsystem environment. Guest SCP's such as DOS and OS may also take advantage of the facilities of this system. Operator problems are eased by having the VMTAPE service virtual machine provide drive management and volume verification. A full audit data base is maintained.

CA-DRIVER Now Available for OS

Computer Associates International has announced the availability of its CA-DRIVER software package for OS/VS1 and MVS installations. CA-DRIVER is intended to avert problems in handling job streams, reduce JCL maintenance, and improve job throughput.
Programmers can catalog common JCL or tables of data in one procedure and call it from another procedure with the Nested Procedure feature. Using Variable Parameter Substitution, parameters that change frequently can be updated throughout a procedure using only one PROC statement. The Data Inclusion feature of CA-DRIVER provides a facility for job streams that process data each time the job is run or which read* date cards. With this facility it is possible to insert data at pre-determined points within a procedure.
Additionally, CA-DRIVER offers Extended Procedure Expansion, Automatic Job Submission and other features designed to reduce JCL maintenance and improve job throughput.

* Dat wil zeggen ook op van te voren vastgestelde tijdstippen kan uitvoer gevraagd worden. Hiertoe worden datumkaarten meegegeven in de job streams.

Beveiliging

In de Nederlandse Staatscourant van 17 augustus 1982 (nr. 156) is de publikatie opgenomen van het op 16 juli 1982 genomen regeringsbesluit tot het vaststellen van

AANWIJZINGEN INZAKE DE BEVEILIGING VAN PERSOONSGEGEVENS, VERWERKT EN OPGESLAGEN IN GEAUTOMATISEERDE GEGEVENSVERWERKENDE SYSTEMEN BIJ DE RIJKSOVERHEID

Aangezien elke organisatie die persoonsgegevens verwerkt als gevolg van de toekomstige privacywetgeving te maken zal krijgen met eisen van beveiliging, werd het nuttig geacht u attent te maken op deze publikatie. Gezien de omvang ervan wordt volstaan met een beknopt uittreksel.

1. Inleiding

Deze aanwijzingen strekken ertoe voor de gehele rijksoverheid beveiligingsvoorschriften te geven voor het beheer en het gebruik van geautomatiseerde systemen die persoonsgegevens verwerken en opslaan. In de eerste plaats heeft het ten doel te verzekeren dat onbevoegd kennis nemen van persoonsgegevens door derden en door eigen personeel, dat die gegevens niet behoeft te kennen, wordt voorkomen. Verder zullen deze aanwijzingen bijdragen tot een vermindering van de mogelijkheden opzettelijk of onopzettelijk schade aan gegevens en/of apparatuur toe te brengen.

Omdat de factor mens een zo grote rol in het geheel speelt, is het hoofdstuk betreffende het personeel (eigen personeel en dat van derden) wat gedetailleerder uitgewerkt en is ook in de andere hoofdstukken de nadruk gelegd op organisatorische maatregelen die direct het doen en laten van de betrokken personen betreffen.
Bij de uitwerking van deze aanwijzingen is ervan uitgegaan dat de bescherming van de persoonlijke levenssfeer bij het functioneren van een geautomatiseerd systeem waarin persoonsgegevens worden verwerkt ook in die zin moet zijn gewaarborgd, dat de naleving van de ter zake geldende regels is verzekerd.
Hierbij zij evenwel opgemerkt, dat zowel de aard van de opgeslagen en verwerkte gegevens als het belang dat derden bij kennisneming van die gegevens zouden kunnen hebben, in de concreet op grond van deze voorschriften te nemen maatregelen moeten worden verdisconteerd. De meeste in deze aanwijzigingen gegeven regels laten dan ook ruimte over voor verschil in uitwerking. Dit is uiteraard noodzakelijk omdat de situaties waarin de maatregelen van toepassing zijn zeer verschillend kunnen zijn.
Een volgend criterium waaraan de gegeven regels trachten te voldoen, is dat deze door alle bij de werking van een geautomatiseerd systeem betrokkenen als zinvol en redelijk moeten worden ervaren.
Juist bij beveiligingsmaatregelen is het gevaar groot dat men zich er bewust of onbewust niet (langer) aan houdt omdat de zin ervan niet wordt ingezien.

De hier gegeven aanwijzingen betreffen:
a. persoonsgegevens
b. systemen die deze persoonsgegevens geautomatiseerd verwerken en opslaan
c. de Rijksoverheid.

Vervolgens worden de punten a, b en c nader uitgewerkt.

Hoofdstuk II bevat een verklarende woordenlijst. In een aantal gevallen is hierbij gekozen voor een eigen, van het spraakgebruik afwijkende, naamgeving. De reden hiervoor is, dat deze aanwijzingen in zeer verschillende omstandigheden moeten worden toegepast. Het leek beter dat betrokkenen zich moeten realiseren hoe zij in hun geval moeten worden uitgelegd en toegepast (bijvoorbeeld wie is beveiligingsfunctionaris (BF), dan dat een algemeen begrip tot verkeerde toepassing van de aanwijzing zou leiden.

Hoofdstuk III bevat de aanwijzingen met voor zover nodig een toelichting op de afzonderlijke artikelen. In een aantal gevallen is hierbij aangegeven hoe een bepaling zou kunnen worden uitgevoerd en/of waarop men bij de uitvoering bedacht dient te zijn.

In hoofdstuk IV tenslotte is een alfabetisch trefwoordenregister gegeven.

Het belangrijkste hoofdstuk is hoofdstuk III. De indeling hiervan is:

1. Algemeen en organisatie.
   Hierin worden verantwoordelijkheden gesteld en wordt ingegaan op de taken van een beveiligingsfunctionaris (BF). Ook het controle-aspect komt aan de orde.

2. Maatregelen gericht op het personeel dat betrokken is bij de geautomatiseerde gegevensverwerking, gesplitst in 2.1 en 2.2:
   2.1 Eigen personeel.
   Wij attenderen op de punten:
   2.1.3 Geheimhoudingsplicht
   2.1.4 Functiescheiding en werkregistratie.
   Voor het personeel worden taak- en werkomschrijvingen opgesteld. Daarbij dient te worden gestreefd naar een scheiding van werkzaamheden in de navolgende functies:
   - het ontwerpen van toepassingen;
   - het programmeren van toepassingen en het onderhoud van programma's;
   - het uitvoeren van acceptatietests;
   - de bediening van G-apparatuur (zie noot);
   - het vervaardigen, onderhouden en aanpassen van bedrijfs- en steunprogrammatuur;
   - het ontvangen en afleveren van gegevens;
   - het beheren van bestanden;
   - controle.

   Van de verrichte werkzaamheden vindt zodanige registratie plaats dat te allen tijde kan worden nagegaan wie op welk moment specifieke werkzaamheden heeft uitgevoerd.

2.1.5 Maatregelen bij ontslag of overplaatsing
en
2.1.7 Inbreuk op beveiliging.

2.2 Personeel van derden.
Hierbij is van belang:
2.2.6 Geheimhoudingsverklaring
2.2.7 Maatregelen bij beëindiging der werkzaamheden
en
2.2.9 Inbreuk op beveiliging.

3. Maatregelen gericht op de toegang tot gebouwen en ruimten.

4. Maatregelen gericht op verkrijging, installatie en onderhoud van apparatuur en programmatuur.

5. Maatregelen gericht op systeemontwikkeling en programmatuur.

6. Maatregelen gericht op het beheer en de opslag van gegevens.
Hierbij wordt ook aandacht besteed aan
6.5 Beveiliging van mensleesbare gegevensdragers
en 6.10 Kopiëring van gegevens.

7. Maatregelen gericht op de toegang tot de gegevens.
Hierbij is in ruime mate aandacht besteed aan on-line beveiligingen.

8. Maatregelen gericht op de verwerking.

9. Maatregelen gericht op de verbindingen.

10. Maatregelen bij calamiteiten.
Hieronder valt tevens het zogenaamde Noodvernietigingsplan (10.3) dat bepaalt dat, indien nodig, persoonsgegevens eventueel vernietigd zouden kunnen worden.

Het zal u duidelijk zijn dat betrokkenen de "Aanwijzingen" kunnen hanteren als "aide de memoire" bij het formuleren van beveiligingseisen.

'Aanwijzingen inzake de beveiliging van persoonsgegevens, verwerkt en opgeslagen in geautomatiseerde gegevensverwerkende systemen bij de rijksoverheid' is binnenkort ook verkrijgbaar in brochurevorm. Het zal worden uitgegeven door de Staatsuitgeverij als deeltje 4 van de Algemene Aanwijzingen voor de Rijksdienst.

G-apparatuur is de verzameling apparatuur, nodig voor de geautomatiseerde gegevensverwerking in de meest ruime zin. Naast de centrale verwerkingseenheid/eenheden en de direct hiermee verbonden apparatuur valt hier dus ook onder de niet direct gekoppelde apparatuur welke bijdraagt aan de geautomatiseerde gegevensverwerking.

Op 15 november 1982 (vond) de officiële opening plaats van het Computer Uitwijk Centrum te Lelystad. De Telegraaf van 14 oktober jl. wijdde hier een voorbeschouwing aan onder de kop

PRINS BERNHARD OPENT UNIEK CENTRUM:

Bedrijf kan na ramp naar reservecomputer

Zo eenvoudig als deze "kop" suggereert is het uiteraard niet, hetgeen moge blijken uit enkele citaten uit het desbetreffende artikel.

De verzekeringsconcerns Amfas en Delta-Lloyd, FGH Hypotheekbank, KLM en de Franse staatsbank Société Générale zijn de initiatiefnemers voor dit centrum in Oostelijk Flevoland. Gezamenlijk richtten zij een aparte BV op, waarbij zij alle een minderheidsbelang in het aandelenkapitaal van ƒ 3,5 miljoen kregen.

Aanvankelijk heeft men het risico van stilstand bij storing trachten terug te dringen door het sluiten van zogenaamde reciprociteitscontracten met collegagebruikers. Gebeurde er iets bij de een, dan kon hij bij zijn collega terecht om zijn computerapparatuur te gebruiken.
Het artikel schetst verder dat dit door de wijzigende technieken steeds moeilijker wordt waardoor andere oplossingen gevonden dienen te worden.
Het beste alternatief lijkt dan ook een uitwijkcentrum, een onafhankelijk centrum, dat op elk tijdstip van de dag kan worden ingeschakeld en dat langere tijd achtereen kan worden gebruikt. Zoiets staat er nu in Lelystad.
Het CUC richt zich vooral op de middelgrote en grote IBM-gebruikers. In Lelystad staat daar nu een IBM-systeem met een geheugen van 12 megabyte, wat met de installatie van een tweede systeem volgend jaar kan stijgen tot 28 megabyte. Totale waarde van deze installaties komt dan op ƒ 15 à ƒ 20 miljoen.
Men kan zich door betaling van een bepaald bedrag aansluiten bij het CUC, een soort uitwijkverzekering dus.
Voor het overgrote deel is dat tussen de 2½ en zeven ton, een zeer klein aantal zit daaronder of -boven. In principe kunnen de klanten na een calamiteit niet langer dan twee maanden de computerruimte van CUC bezetten. Daarna kunnen zij gebruik maken van de "empty shell" van het CUC, een lege computerruimte naast de met computers gevulde zaal, waarin zij zelf nieuwe apparatuur kunnen zetten. Ook kan gebruik van de mogelijkheid een verplaatsbare computerruimte worden gemaakt, gelijkend op een soort superluxe bouwkeet met verhoogde vloeren, airconditioning e.d., waarvan meerdere gemakkelijk aan elkaar zijn te koppelen tot een grote computerzaal. Deze computerruimte kan dan zo mogelijk op het eigen terrein van de onderneming worden neergezet.

Wij merken hierbij op dat laatstgenoemde oplossing ook door (grotere) ondernemingen met meerdere rekencentra in eigen beheer kan worden gerealiseerd.
Problemen van een uitwijkcentrum op een vaste plaats zijn onder andere de afstand tot de eigen vestigingsplaats, beschikbaarheid van datalijnen, e.d. Deze problemen vervallen bij gebruik van mobiele kantoorruimten.

BEVEILIGING DD/DS

Steeds vaker wordt bij een automatiseringsafdeling een Data Dictionary/Directory System (DD/DS) aangetroffen. Deze is dan meestal om verschillende redenen aangeschaft. Eén daarvan kan zijn de "beveiliging". In het artikel "The integrated Dictionary/Directory System" van F.W. Allen, M.E.S. Loomis en M.V. Mannino troffen wij een vergelijkend overzicht aan met kenmerken van een aantal DD/DS-pakketten. Vooral het Security level aspect bevelen wij in uw aandacht aan.

SELECTED CAPABILITIES

System	Maintenance methods	On-line query
ADABAS DATA DICTIONARY	Fixed format, preformatted screens	Yes
DATA CATALOGUE 2	Keyword driven, prompted-tutorial input, preformatted screens	Yes
DATA CONTROL SYSTEM (Cincom)	Preformatted screens	Yes
DATA CONTROL SYSTEM (Haverly)	Fixed format	Yes via QLP (Sperry-Univac product)
DDS 1100	Keyword driven	Yes via QLP
DDS	Keyword driven	Yes
DATADICTIONARY	Fixed format	Yes
DATAMANAGER	Keyword driven	Yes
DB/DC DATA DICTIONARY	Keyword driven, performatted screens	Yes
DICTIONARY/204	Fixed screens	Yes
Edict	Fixed format	Yes
IDD (Cullinane)	Keyword driven, fixed and variable screens	Yes
IDD (Intel)	Keyword driven, preformatted screens	Yes
PRIDE-Logik	Keyword driven, fixed format and fixed screens	Yes
TIS DIRECTORY	Preformatted screens	Yes
UCC TEN	Fixed format, preformatted screens	Yes

Security levels	User-defined reports	Comments
Entity, attribute, attribute value, and function (read and write)	Via NATURAL	NATURAL is a program development facility
Entity type and command	Customization via macro routines; additional reports via call and file extraction capabilities	New reports require user software
Passwords for Element entity occurrences, user password profiles	Through the Socrates report writer	
None	Report options	
Command and entity occurrence	Via QLP	
Entity type, function, user, and operational status	Report options via the SELECT clause	
Entity occurrence	Through DATAREPORTER	
D/D creation, sign on, commands, user, and entity	Customization via macro routines; additional reports via Call and File extraction capabilities	New reports rely on the User
Sign on, status, and entity type	Via GIS	
Login	Via User Language	Security levels planned
Entity type and others via user-defined security routine	Via the User-Defined Language	
User view and record level	Customization through changing of parameters; new reports via CULPRIT	
Element entity and command	Via Report Writer	
Function, entity type	Via Extract facility	
Command	Via Comprehensive Retrieval Component	
Command	Report parameters	Additional security can be added via security tables

Controle

Een bekend feit is dat steeds meer gebruik wordt gemaakt van standaardtoepassingspakketten. Deze ontwikkeling is niet meer te stuiten gezien de microgeneratie. De meningen omtrent deze ontwikkeling - gezien vanuit de diverse disciplines - lopen nogal uiteen. Welke problemen de accountant kan tegenkomen zijn in het volgende artikel van Nigel Tutt beschreven. Ingegaan wordt op de activiteiten die plaatsvinden in Engeland om te komen tot normen (ook op controlegebied) voor standaardtoepassingspakketten. Zijdelings worden een aantal andere problemen aangeroerd als normen zijn vastgesteld: bijvoorbeeld het afgeven van een mededeling bij een standaardpakket (hetgeen nu reeds gebeurt). Niet ingegaan wordt op de vraag of, als eenmaal een "certificaat" door een accountant is afgegeven, een andere accountant dit zonder meer kan accepteren.

Een zaak die de nodige aandacht verdient.
Compactlezer, laat uw gedachten er eens over gaan. De redactie ziet gaarne uw bijdrage in dezen tegemoet.

Accountancy nears software standards

Nigel Tutt reports on plans in the accountancy profession to set up software standards, which would help auditors and manufacturers

The accountancy profession and computer business have never looked like suitable bedfellows, but if moves now afoot reach fruition then the bonds will be drawn closer.
Representatives from the computer industry and the Institute of Chartered Accountants (ICA) hope to persuade the Consultative Committee of Accountancy Bodies (CCAB) to publish standards for software.
The CCAB represents the six major accountancy bodies in the UK and Ireland. The bodies include chartered, certified, management and public sector accountants.
The accountancy profession has become noticeably more aware of the uses of computers in business with the issue of 'exposure drafts' (forerunners to binding standards) on auditing in the computer environment.

The history of the search for the forerunner to what could lead to the audit certification of software packages, began four years ago in Sheffield.
The Sheffield District Society of Chartered Accountants was approached by a software house which asked if its business packages were auditable.

By the end of 1981 the group had set up a working party and was beginning to reach an agreed form for a document to be issued.
A meeting last November was crucial. It was highpowered, the roll call of those present was impressive. It was chaired by Andrew Beard.

'POOR SOFTWARE IS GIVING THE INDUSTRY A BAD REPUTATION'

He introduced the meeting before speeches from British Computer Society council member Hollis and Steve Millward, the technical director of Comshare.
Millward told the meeting that despite the time spent on building in controls, a significant proportion of poor software is giving the industry a bad reputation with users and auditors. The only way to identify good software would be by compliance with standards he said.

Hollis said that the aims of an independent review body would be to reduce the time spent by auditors on reviewing identical packages and to reduce the number of unsuitable software packages on the market.
It would also ensure that software for financial accounting has adequate controls and that the control system is checkable and workable.
The meeting agreed that standards should be drawn up followed by the independent examination and certification of software complying with those standards.
John Court prepared a first draft to bring to a further meeting in February.

Ian Dunkley, pointed to one of the problems: "Where we differ from the National Computing Centre (NCC) is that the CRA is looking at the micro end of the market while the NCC goes for the bigger end. We want software controls that will cover all sizes if possible but it is more likely that there will be more than one document, one for the micro and another one for the larger machine."

The main aim, Hollis said was to get a document understood by the manufacturer, the user of the software, the software houses and the auditor.
Understanding each profession's jargon has been a problem. "The auditor and accountant have a different idea of control to the software people."
Hollis envisages the standard covering two different areas. Firstly, before a package is sold the publicity should state the capabilities of the package to a particular configuration.

Second in importance is the post-purchase position.
The standard here would cover the quality of the documentation which comes with the package, the internal and external controls, security and audit trail - and also some guidance for the auditor to enable him to audit in the best way.
Auditors have, it seems, been helpful in developing the standard for software. Parts of the new draft guidelines for auditing in the computer environment have apparently been lifted and inserted in the software document.
Hollis expects the next meeting "get close" to a final draft agreed by all the participants.

ACCOUNTANCY PROFESSION IS NOT NOTED FOR ITS SPEED

The accountancy profession is, however, not noted for speed, but Chriss Morgan admitted that a final version is "urgently needed". "A lot of the groundwork has been done and it now needs the CCAB bodies to put their weight behind it. By the end of April we will have put a CCAB committee together or will be looking for a different way forward."
The premature exposure may, he believes, have prejudiced some of the individual accountancy bodies' involvement.
The accountants have technical and legal problems if these software standardisation moves reach their eventual conclusion in audit certification.
One accounting firm is being sued in the US over the certificate it issued with a software package.
But if in such cases the accountants are loth to issue "comfort" to a software house without a stack of disclaimers, the latter is still eager to have its wares associated with a prestigious firm of accountants.
Last month Altergo, the IBM tied software and support group, announced its latest business applications for the 4300 series.
It is now negotiating a suitable form of words to "certify" the software with a large firm of accountants.
The certifying would be considerably easier if there was a set of standards to comply with.
As Hollis said: "At the moment accountants would give a lot of disclaimers but if there were standards then they could say that the software complied with laid down standards - it would also help to sell that software."

ONDERWIJS

Achtergrond van de methodiek

Interne en externe ontwikkelingen kunnen organisaties er toe brengen over te gaan tot het in kaart brengen van afspraken en regels. Groei van een organisatie betekent veelal dat op een zeker moment de behoefte ontstaat aan richtlijnen, reglementering en structurering van organisatorische regelingen ten einde het functioneren van de organisatie beter te kunnen beheersen.
In tal van organisaties vinden daarom vastleggingen plaats. Deze vastleggingen kunnen verschillende uiterlijke vormen aannemen en betrekking hebben op een groot aantal uiteenlopende onderwerpen.
Vastleggingen worden door de hele organisatie heen, van de topleiding tot de operationele werkplek, aangetroffen.

In de praktijk blijkt vaak dat pogingen die er op gericht zijn bij te dragen aan de beheersing van een organisatie middels het systematisch vastleggen van structuren en processen te vaak tijdens de uitvoering (dreigen te) mislukken. Activiteiten die met veel enthousiasme zijn gestart verzanden of er wordt van de gemaakte vastleggingen nauwelijks gebruik gemaakt. Kortom, de doelstelling om langs de gewenste weg tot een betere beheersing van de organisatie te geraken wordt niet gehaald.

Ten einde de planning, voorbereiding en uitvoering van een vastleggingsproject zo adequaat mogelijk te laten verlopen heeft de vakgroep Operationeel Management van de Organisatiegroep van Klynveld Kraayenhof & Co. een methodiek ontwikkeld waarmee een goede aanpak wordt geboden om de uitvoering van een vastleggingsproject in een organisatie te doen slagen.

Doel van de methodiek

De methodiek heeft als doel:

- het bijdragen aan het tot stand komen van vastleggingen die inzicht in de mate van efficiency en toereikendheid van structuren, taakverdelingen en processen verschaffen;

- het realiseren van effectieve vastleggingen door het duidelijk stellen van doelstellingen en het doen van keuzes met betrekking tot vastleggingsprojecten en de organisatorische en overige vereisten;

- het uitdiepen van de betekenis, het verloop van en de stappen binnen vastleggingsprojecten aan alle betrokkenen;

- het doen ontstaan van een gemeenschappelijk verwachtingenpatroon bij leiding en medewerkers ten aanzien van het nuttig effect en het gebruik van de resultaten van de vastleggingen.

Bestemd voor

De methodiek is bestemd voor al die functionarissen die in belangrijke mate betrokken zijn bij de voorbereiding op, de coördinatie tijdens en de daadwerkelijke uitvoering van het vastleggingsproject.
Hierbij wordt gedacht aan:

- het management van uitvoerende afdelingen;
- het management en de medewerkers van afdelingen zoals Administratieve Organisatie, Automatisering, Interne Controle, Organisatie en Efficiency, Systeembeheer enz.;
- organisatie-adviseurs.

Inhoud van de methodiek

De methodiek richt zich op de te doorlopen stappen van een proces dat moet leiden tot gerealiseerde vastleggingen in een organisatie, te weten:

I **Probleemanalyse en keuze van oplossingsalternatieven**

II **Voorbereiding van het vastleggingsproject**

III **Planning**

IV **Uitvoering**

V **Gebruik van de gerealiseerde vastleggingen.**

In stap II uit dit proces, de voorbereidingsfase, worden een viertal keuzegebieden behandeld die van belang zijn om tot een goede probleemdefinitie te komen waaraan de keuze van de te gebruiken vastleggingstechniek(en) kan worden gerelateerd.

De vier keuzegebieden omvatten:

- **Het onderkennen van de doelstellingen van de vastlegging**
  Hier wordt ingegaan op het "waarom" van het vastleggen, in casu de beoogde resultaten zoals het dienen als basis voor de beoordeling van de efficiency, maatregelen van interne controle, automatisering of het fungeren als (werk) instructiemiddel.
  Besproken worden de doelgroepen ("door wie" en "voor wie") en de oogmerken van het vastleggingsproject.
  Een concrete formulering van doel en doelgroepen is van belang om het project enerzijds "in lijn" te laten vallen met de groei- en ontwikkelingsfase van de organisatie en anderzijds de aanpak van het vastleggingsproject en de keuze van de hulpmiddelen hier op te kunnen afstemmen.

- **Het aangeven van de objecten van de vastlegging**
  Het betreft hier het "wat" van het vastleggen in casu de onderdelen of processen in de organisatie welke men wenst vast te leggen.
  Een drietal manieren om te kijken naar organisaties (de structuurindeling, de procesindeling en de indeling naar de doelstellingenhiërarchie) worden behandeld. Het beeld dat hierbij over een organisatie ontstaat dient als basis voor de te

kiezen vastleggingsgebieden en het opsplitsen van het vastleggingsproject in subprojecten.

- **De keuze van de vastleggingstechnieken**
  Hier komen de te gebruiken hulpmiddelen aan de orde, zoals technieken die erop gericht zijn structuren of processen vast te leggen.
  Vier verschillende groepen vastleggingstechnieken worden besproken; in casu structuur-, stroom-, autorisatie- en prestatievastleggingen.
  Gegeven de reeds vastgestelde objecten van de vastlegging en de doelstellingen worden eisen geformuleerd waaraan de concrete vastleggingstechnieken voor de betrokken organisatie moeten voldoen.

- **Het vaststellen van de randvoorwaarden voor de organisatorische beheersing van het vastleggingsproject**
  De haalbaarheid van de gewenste resultaten wordt mede bepaald door de mate waarin condities kunnen worden geschapen die de effectiviteit van het project in positieve zin kunnen beïnvloeden. Hierbij valt te denken aan het kennis- en ervaringsniveau in de organisatie ten aanzien van het omgaan met vastleggingen, de beschikbaarheid van medewerkers, de betrokkenheid van het management etc.
  Deze factoren hebben effect op de kwaliteit van het resultaat, de inzet van mensen en middelen bij de uitvoering en de gevolgde werkwijze.

Wijze van kennisoverdracht

Voor de overdracht van de cursus is een tweedaagse cursus ontwikkeld. Het zich eigen maken van de stof vereist een actief leerproces, waarbij een intensieve communicatie tussen de deelnemers onderling en tussen de inleiders en de deelnemers een belangrijke plaats inneemt.
In de cursus wordt een praktisch gerichte casus in werkgroepen uitgewerkt. Gezien de intensieve wijze van kennisoverdracht is het aantal deelnemers aan een maximum van 16 gebonden.

Op de eerste dag wordt voorbereiding en organisatie van een vastleggingsproject behandeld, op de tweede dag komt de toepassing van een viertal vastleggingstechnieken aan de orde.

De cursus kan tevens gezien worden als een inleiding op de diepgaande behandeling van één of meer specifieke vastleggingstechnieken.
Materiaal is beschikbaar om aan bijzondere onderwerpen zoals interviewtechniek, vastleggingstechniek, projectorganisatie, handboek organisatie en systeembeheer aandacht te geven. In dat geval wordt de inhoud van de tweede en eventuele volgende dagen in overleg met de cliënt ingevuld.

Vastlegging in organisaties

Cursus

De eerstvolgende cursus vindt plaats:
- op 18 en 19 januari 1983
- tegen een cursusprijs van f 550,-- p.p. excl. B.T.W.
- bij voldoende aanmeldingen (tenminste 10)
- in een nader te bepalen conferentie-oord (arrangementskosten ca. f 200,-- p.p.)
- Docenten: Drs. P.M. Ansems
  Ir. K.S. Volder
- Aanmelding te richten aan:

Klynveld Kraayenhof & Co.
Bureau Opleiding
Mevr. P. Schepel
Prinses Irenestraat 59
1077 WV Amsterdam
telefoon: 020 - 54 69 111

Klynveld Kraayenhof & Co.
Internationaal KMG Klynveld Main Goerdeler Organisatie-adviseurs