Klynveld Kraayenhof & Co.
Accountants

Automatisering en Controle-groep

COMPACT

83/3

Computer en Accountant

Uit de inhoud:

Continuïteit van de gegevensverwerking, een inleiding
door H. Roos

Back-up, Restart en Recovery (deel 1, Back-up)
door R. Bron

Onderzoek naar werking interne controle mogelijk ?
door drs. J.E. Huizenga

Data entry en interactief programmeren via de terminal: het pakket ICCF nader bekeken
door R.P. Bosman

Down to earth again, KMG potential
door R.H. Healey, Thorne Riddell
(De microcomputer in de accountantscontrole)

Nummer 32 10e jaargang Zomer 1983

Internationaal KMG Klynveld Main Goerdeler

COMPUTER EN ACCOUNTANT

INHOUDSOPGAVE

NUMMER 32 10E JAARGANG ZOMER 1983

compact

Zomer 1983

VAN DE REDACTIE

Compact in de zomer van zijn 10e levensjaar.

De basis voor ons blad wordt gevormd door drie elementen: de automatisering, de controle en beveiliging alsmede de samenhang of wisselwerking tussen de twee eerste facetten. Dit vormt het werkterrein van de EDP-audit.

In de hoofdartikelen van dit nummer kunt u de elementen herkennen:
- Continuïteit van de gegevensverwerking, een inleiding, door H. Roos
  Back-up, Restart en Recovery door R. Bron.
- Onderzoek naar werking interne controle mogelijk?
  door J.E. Huizenga.
- Data entry en interactief programmeren via de terminal:
  het pakket ICCF nader bekeken door R.P. Bosman.

Drie zeer specifieke onderwerpen gericht op de snel veranderende automatiseringswereld veroorzaakt door het brengen van de computer naar de werkplek. Dit zowel door middel van terminals als door plaatsing van micro/minicomputers. Welke opgave wacht de EDP-auditor/Accountant. J.E. Huizenga schreef hierover een artikel met visie.
Verder Nieuws op het gebied van de microcomputer en vervolg van de lezing R.H. Healey deel III hetgeen tevens het slot betekent. Ook ons commentaar op het buitengebeuren geeft blijk van bovengenoemde nieuwe problematiek.

Ons blad staat open voor uw commentaar; wij ruimen gaarne een plaats daarvoor in.

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

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

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

Zomer 1983

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

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

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

ACTUALITEITEN

Recent verschenen:

Auditing & EDP (second edition)

Schrijvers: Gordon B. Davis, CPA
Donald L. Adams, CPA
Carol A. Schaller, CPA

Het boek is een uitgave van het American Institute of Certified Public Accountants Inc. (1983) 413 pag.

De eerste editie werd uitgegeven in 1968. Deze nieuwe tweede uitgave is bijgewerkt overeenkomstig veranderingen in de computertechnologie, alsmede gewijzigde inzichten terzake van controletechnieken zoals deze door de accountant worden gehanteerd.

Het voornemen bestaat om deze nieuwe editie in een van de komende nummers van Compact te bespreken.

Zomer 1983

CONTINUITEIT VAN DE GEGEVENSVERWERKING, EEN INLEIDING

door H. Roos

Het gebruik van slechts met een computer leesbare media voor het bewaren van informatie heeft tot gevolg dat de beschikbaarheid van de informatie mede afhankelijk is van de goede werking van de computer en van de kwaliteit van de gebruikte opslagmedia.

Het artikel van R. Bron (zie pag. 8) over back-up, restart en recovery heeft betrekking op de maatregelen die kunnen worden getroffen om te voorkomen dat informatie, die op dergelijke media wordt bewaard, verloren gaat.

De aard van de te treffen maatregelen is afhankelijk van de eigenschappen van het toegepaste medium wat betreft het vasthouden van de informatie onder verschillende omstandigheden, de snelheid waarmee een willekeurige eenheid informatie op het medium kan worden aangebracht en kan worden teruggevonden, alsmede de opslagcapaciteit van het medium.

In de meeste gevallen zal de in het interne geheugen opgeslagen informatie slechts beschikbaar blijven zolang de stroomtoevoer naar de computer niet wordt onderbroken. Dit euvel kan gedeeltelijk worden ondervangen door de computerinstallatie te voorzien van een batterij die er voor kan zorgen dat, na een onderbreking van de normale stroomtoevoer via het openbare net, de computer nog enige tijd onder spanning blijft om de gelegenheid te bieden de informatie uit het interne geheugen naar een extern medium over te brengen.
Magneetbanden, magneetschijven en floppies zijn voor het behoud van de erop vastgelegde informatie niet van de handhaving van de stroomtoevoer afhankelijk en bieden daardoor een scala van mogelijkheden voor het over langere tijdsperioden vasthouden van informatie. De op die media vastgelegde informatie kan echter uitsluitend worden zichtbaar gemaakt door middel van een computerproces. Een belangrijke eigenschap van magneetbanden, floppies en magneetschijven van het verwisselbare type is de mogelijkheid om de erop vastgelegde informatie zichtbaar te maken via een andere computer dan waarmee die informatie is vastgelegd. De informatie op niet verwisselbare schijven is alleen via de computer waarmee die is vastgelegd ook weer zichtbaar te maken.
De tijdsduur waarover deze media de informatie onverminkt kunnen conserveren hangt af van onder meer de fysieke kwaliteit. De vaste schijven bieden bij de huidige stand der techniek een aanmerkelijk hogere kwaliteit dan de verwisselbare media. Voorts heeft de groei van toepassingen die de informatie zeer snel na opvragen beschikbaar maken ertoe geleid dat zowel de opslagcapaciteit van schijven als de snelheid waarmee de overdracht van informatie tussen het interne geheugen en de schijf plaatsvindt, aanzienlijk zijn toegenomen. Deze technische verbeteringen hebben evenwel in hoofdzaak betrekking op vaste schijven, omdat banden en verwisselbare schijven hiervoor te kwetsbaar zijn gebleken.

Bij de huidige stand der techniek bestaan er grote verschillen in opslagcapaciteit tussen de verschillende media en tussen de daarbij behorende overdrachtssnelheden.
Intern geheugen is zeer snel doch, ondanks de vrijwel continu dalende prijzen per eenheid opgeslagen informatie naar verhouding van beperkte capaciteit.
Vaste schijven bieden zeer grote opslagcapaciteit, tot ca. 1.000 gigabyte per schijf die niet sequentieel (random) kunnen worden gelezen en geschreven met overdrachtssnelheden in de orde van 3.000 kilo-bytes per seconde (kbps).
Banden zijn in verschillende lengtes beschikbaar. De opslagcapaciteit is sterk afhankelijk van de dichtheid waarmee de informatie wordt opgeslagen - van ca. 550 bytes per inch (bpi) tot 6.250 bpi - en van de overdrachtssnelheid, van 470 kbps tot 1.250 kbps.
Het is uiteraard wenselijk om uit dit brede scala van mogelijkheden een voor elke situatie zo optimaal mogelijke te kiezen. Bij het maken van afwegingen kunnen verschillende toepassingen op eenzelfde installatie een onderling strijdige oplossing vereisen.

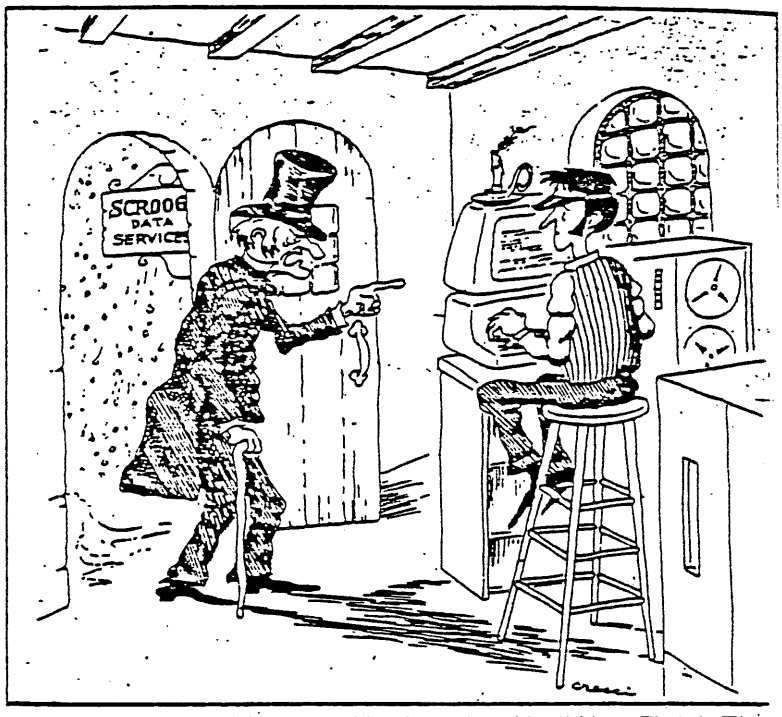
Essentieel is dat zowel tijdens een opslagoperatie, als tijdens een terugzoekoperatie, de informatie altijd tijdelijk is opgeslagen in het interne geheugen van de computer waarmee die operaties worden bestuurd. Dit betekent dat nieuwe informatie verloren kan gaan voordat die op een extern medium is opgeslagen.

Een tweede factor is de maximale tijdsduur die mag verstrijken tussen het moment waarop een bepaalde eenheid informatie wordt opgevraagd en het tijdstip van beschikbaar komen. Naarmate het bedrijfsproces waarvoor de gevraagde informatie bestemd is voor een goed functioneren sterker afhankelijk is van het snel over die informatie kunnen beschikken zullen er hogere eisen worden gesteld aan de snelheid waarmee verloren gegane informatie moet kunnen worden gereconstrueerd.

In essentie komen alle mogelijke maatregelen erop neer dat de informatie, die moet worden beschermd tegen verlies, op meer dan een medium wordt opgeslagen.
Dit roept het probleem op van de gelijkloop van de verschillende opgeslagen versies van de informatie.
De wijze waarop dit kan worden geregeld hangt tevens samen met de maatregelen die worden getroffen om te kunnen vaststellen dat opgeslagen informatie volledig en juist is en blijft. Deze integriteitscontroleprocedures moeten worden gesynchroniseerd met de back-up, recovery en restart procedures.
De vorm van deze procedures wordt voorts sterk beïnvloed door de organisatie van de processen voor het opslaan en opvragen van informatie.

Een proces waarbij slechts één aan een bepaalde bedrijfseenheid gebonden opvraag- en opslagcyclus tegelijk mogelijk is, kan met eenvoudiger procedures worden beveiligd, dan een proces dat tegelijkertijd meer dan een opslag- en opvraagcyclus toestaat. In het tweede geval zijn maatregelen nodig ter voorkoming van informatieverlies doordat vanuit twee verschillende bronnen dezelfde informatie-eenheid kan worden gewijzigd.

Hiervoor wordt normaliter gebruik gemaakt van de "concurrency-control" procedures van de speciale database management software. Dergelijke standaardprocedures gaan echter uit van bepaalde veronderstellingen die niet steeds stroken met de wijze van programmeren van toepassingen.
De zogenaamde "recoverable transactie" volgens de standaard concurrency control procedure dekt niet steeds de transactie die in het kader van een bepaalde toepassing "recoverable" moet zijn.
Een transactie is "recoverable" zolang het effect ervan op de opgeslagen en verstrekte informatie kan worden teniet gedaan.
Hieraan kan worden voldaan indien en voor zover per transactie een vastlegging wordt gemaakt van alle informatie die is uitgewisseld tussen de persoon of het proces dat de transactie gebruikt en de opgeslagen informatie.
Voor transactiesoorten die gelijktijdig meer dan één transactie toestaan, houdt dit onder meer in dat de transactievolgorde een rol speelt.



'Christmas . . . Bah! You're Not Leaving Until You Finish Tha General Ledger Program.'

In het in dit nummer en het volgende op te nemen opstel van de hand van R. Bron, wordt in extenso ingegaan op fundamentele technieken voor het voorkomen van verlies van op externe media opgeslagen informatie.

Op de implicaties van concurrency-control en van de recovery van transacties zal in een afzonderlijk opstel worden ingegaan.

Back-up, restart en recovery door R. Bron is als volgt ingedeeld:
In deze aflevering van Compact
1. Inleiding.
2. Back-up, recovery en restart: een historisch perspectief.
3. Back-up.
3.1 Techniek van back-up per categorie.
    A. Besturingssysteem en overige harde software (utilities).
    B.1 Toepassingsprogrammatuur (source-coding).
    B.2 Toepassingsprogrammatuur (object-coding).
    C. Job Control Language (de karweibesturingstaal).
    D. Gegevensbestanden:
        - batch-verwerking (generatieprincipe);
        - data entry;
        - real time on-line.
    E. Object versus medium.
3.2 Mengvorm object en medium gerichte techniek.
In het herfstnummer 1983 van Compact komen vervolgens aan de orde:
4. Recovery en restart.
4.1 Voorbeeld situatie.
4.2 Gebruik van log-bestanden.
    A. Before en after images.
    B. Alleen before images.
    C. Alleen after images.
    D. De mutaties zelf.
5. Specifieke aspecten.
    A. Besturingssysteem en overige harde software (utilities)
    B. Gegevensbestanden.
6. Controle-implicaties.
6.1 Procedures en voorschriften.
    A. Besturingssysteem en overige harde software.
    B. Toepassingsprogrammatuur (source-coding).
    C. Job Control Language.
    D. Gegevensbestanden.
6.2 Registratie van bestanden.
6.3 Bruikbaarheid van back-up kopieën.
7. Tenslotte.

Zomer 1983

BACK-UP, RESTART EN RECOVERY

door R. Bron

1. Inleiding

Bij de geautomatiseerde gegevensverwerking is het - naast de betrouwbaarheid van de systemen - van belang dat de continuïteit gewaarborgd wordt.
Om het bestaan van procedures en voorschriften gericht op de continuïteit vast te stellen, worden in voor de controle gebruikte hulpmiddelen (checklisten) veelal summiere vragen aangetroffen op het gebied van "beveiliging van informatiedragers". Daarmee wordt dan dit gebied als afgedekt beschouwd.
Bovendien worden bij het aspect "continuïteit" direct de begrippen Back-up en Restart of Restart en Recovery in één adem genoemd zonder dat stilgestaan wordt bij de problematiek, welke daarachter schuilgaat.

Doel van het artikel is de lezer inzicht te geven in die complexiteit en hem/haar de helpende hand te bieden bij het onderkennen van de problemen in verschillende praktijksituaties.
Om het artikel in enigerlei mate beperkt te houden wordt slechts ingegaan op hetgeen zich binnen een rekencentrum afspeelt.
In hoofdstuk 2 wordt een overzicht gegeven van de ontwikkeling van Back-up, Recovery en Restart gezien vanuit een historisch perspectief.
Daarna wordt in de hoofdstukken 3 en 4 ingegaan op mogelijke Back-up, Recovery en Restart-technieken.
Behandeling van specifieke aspecten vindt plaats in hoofdstuk 5; op de controle-implicaties wordt nader ingegaan in hoofdstuk 6.

2. Back-up, Recovery en Restart: een historisch perspectief

In de prehistorie van de automatisering werd de continuïteit van de gegevensverwerking gewaarborgd door organisatorische maatregelen met betrekking tot de opslag en bewaring van de bij de verwerking gebruikte ponskaarten. Een van de problemen hierbij was het volledig blijven van de kaartenbestanden. Daarnaast werd meestal vanwege de kwantitatieve verhoudingen geen kopieën van bestanden aangemaakt en elders bewaard. Bij de opkomst van magnetiseerbare media (welke voornamelijk betekenis heeft gehad op de verwerkingssnelheid) kwam eigenlijk het aspect Back-up, Recovery en Restart om de hoek kijken. Periodiek werden kopieën van gegevensbestanden gemaakt waarop in geval van meer of minder langdurige storing kon worden teruggevallen.

De continuïteit van de gegevensverwerking werd in belangrijke mate bepaald door de aanwezigheid van kopieën van mutatiebestanden. De omgeving waarin de verwerking plaatsvond (single programming, multiprogramming en/of multiprocessing) was hierop niet van invloed.

Onder single programming wordt verstaan die verwerkingsomgeving waarbij één programma de beschikking heeft over de gehele computer. Bij multiprogramming is het interne geheugen van de computer verdeeld in parten (van gelijke of ongelijke grootte), partities genaamd. Elke partitie kan één programma bevatten. Het daadwerkelijk actief zijn van het programma is afhankelijk van het aantal processoren. Een processor kan op enig moment slechts 1 proces (de uitvoering van een programma) behandelen. Bij multiprogramming is slechts 1 processor beschikbaar.
Van multiprocessing is sprake als meerdere processoren aanwezig zijn voor de gegevensverwerking.
Vanwege de steeds complexer wordende automatisering is het thans niet meer terecht Back-up, Recovery en Restart in één adem te noemen. Zowel Back-up als Recovery en Restart zijn een eigen leven gaan leiden in die zin dat voor het uitvoeren van Back-up, Recovery en Restart niet altijd kopieën van bestanden nodig zijn.
Nieuwe Recovery en Restart-technieken hebben hun intrede gedaan.
Back-up dient te worden geassocieerd met continuïteit op lange termijn; Recovery en Restart is korte termijn gericht.

3. Back-up

In hoofdstuk 2 is aangegeven dat back-up gericht is op het waarborgen van de continuïteit op langere termijn.
Dit wordt gerealiseerd door het kopiëren van bestanden met een bepaalde frequentie (generatiesysteem).
Hierbij komt de vraag op van welke bestanden kopieën nodig zijn om de continuïteit op langere termijn redelijk te kunnen waarborgen. In eerste instantie wordt daarbij meestal gedacht aan gegevensbestanden. Bij nader inzien is de continuïteit slechts te waarborgen als van de volgende categorieën de juiste kopiebestanden beschikbaar zijn:

a. het besturingssysteem en overige harde software;
b. toepassingsprogrammatuur;
c. job control language;
d. gegevensbestanden.

De registraties van bestanden zijn niet onder deze categorieën opgenomen, doch worden behandeld in hoofdstuk 6 "Controle-implicaties" paragraaf 3.

De manier waarop kopieën worden gemaakt kan vanuit twee invalshoeken worden benaderd:

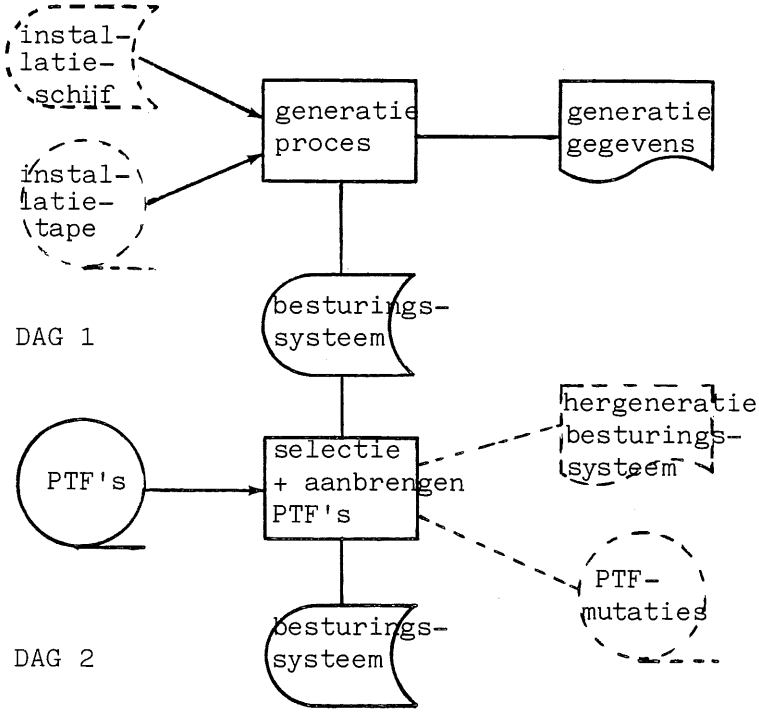
- object gericht;
- medium gericht
- combinatie.

Het frequentie-aspect dat onder andere wordt bepaald door de factoren financiële middelen, alternatieve mogelijkheden om verloren gegane delen te herstellen, blijft verder buiten beschouwing.

3.1 Techniek van back-up per categorie

A. Besturingssysteem en overige harde software (utilities)

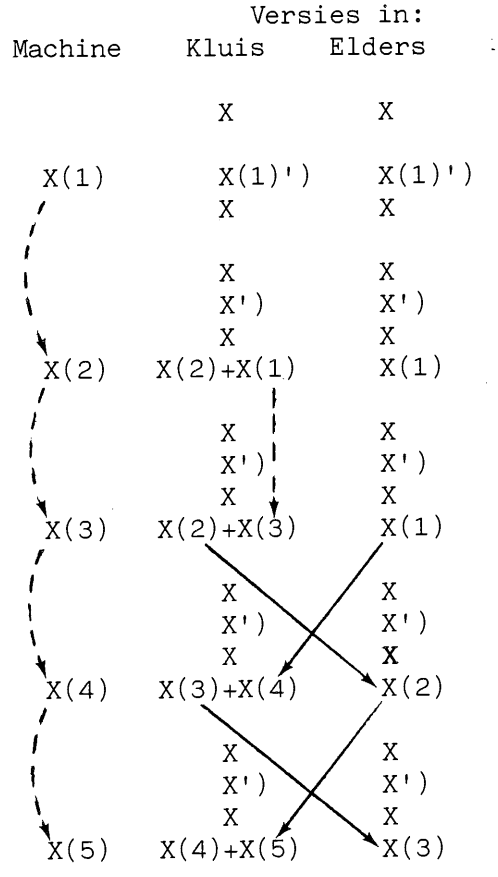
Generatie van het besturingssysteem heeft veelal plaatsgevonden op basis van de van de leverancier ontvangen installatietapes of schijf.
Wijzigingen op het besturingssysteem aangebracht door de leverancier (Program Temporary Fixes (PTF's)) worden veelal op magneetband aangeleverd.
Daarnaast kunnen eigen wijzigingen worden aangebracht.
Het voorgaande is schematisch weergegeven in figuur 1.



Figuur 1.

In figuur 2 wordt een uitwerking gegeven.
Hierin wordt de volgtijdelijke beweging aangegeven van de bestanden tussen de kluis en bewaring elders.
Een "X" in de kolommen geeft de fysieke plaats, waar de (kopie)bestanden worden aangetroffen, aan.
Tussen haakjes ( ) wordt het versienummer gegeven.
De ononderbroken lijnen geven de verplaatsing weer tussen de locaties en (mogelijk) hergebruik van het medium.
Uitgegaan wordt van de aanwezigheid van meerdere generaties (3) aangevuld met de basisgeneratie en alle in de loop van de tijd hierop aangebrachte wijzigingen (PTF (Program Temporary Fixes)-mutaties).

Ideale beveiligingssituatie besturingssysteem en overige harde software



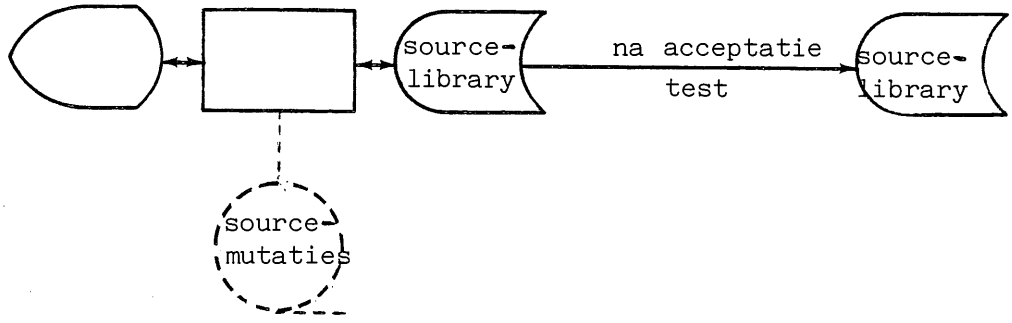
Figuur 2.

') De basisgeneratie X(1) en alle hierop in de loop van de tijd aangebrachte wijzigingen (PTF-mutaties) dienen aanwezig te zijn naast de aangegeven (her)generaties.

B.1 Toepassingsprogrammatuur (source-coding)

Bij toepassingsprogrammatuur wordt niet direct aan gegevensverzamelingen (bestanden) gedacht.
Echter ten onrechte. Het is een gegevensverzameling. Programmatuur wordt opgeslagen op magneetband, schijf, etc. en ondergebracht in bibliotheken. Hierbij kan tevens onderscheid worden gemaakt in enerzijds opslag source-coding ten behoeve van systeemontwikkeling/onderhoud en anderzijds source-coding ten behoeve van produktie.
Uit betrouwbaarheidsoogpunt dienen deze bibliotheken gescheiden te zijn (zie figuur 3).

Systeemontwikkeling/onderhoud Produktie



Figuur 3.

Voor systeemontwikkeling en onderhoud gelden twee afzonderlijke technieken.
In de praktijk wordt in de produktiesfeer meestal volstaan met het maken van twee kopieën van de gehele source-library, elke keer dat er zich iets wijzigt met gescheiden opslag van de kopieën (object gericht). Hierbij wordt geen generatiesysteem bijgehouden.
In de ontwikkelingssfeer waar mutaties real time on-line worden aangebracht, vindt kopiëren van bestanden meestal met een grote interval plaats. Dit vanwege het feit dat het geen direct verband houdt met de continuïteit van de gegevensverwerking in de produktiesfeer.
Er mag niet aan worden voorbijgegaan dat verlies van data met hoge kosten gepaard kan gaan.

In figuur 4 wordt de beweging van de back-up bestanden bij een 3-generatiesysteem (object gericht) weergegeven.

Back-up schema source-library systeemontwikkeling/onderhoud

	Machine	Kluis	Elders
Periode 1			
- Source-library	X(1)	X(1)	X(1)
- Mutaties		M(1)	M(1)
Periode 2			
- Source-library	X(2)	X(2)+X(1)	X(1)
- Mutaties		M(2)+M(1)	M(1)
Periode 3			
- Source-library	X(3)	X(3)+X(2)	X(1)
- Mutaties		M(3)+M(2)	M(1)
Periode 4			
- Source-library	X(4)	X(4)+X(3)	X(2)
- Mutaties		M(4)+M(3)	M(2)

Figuur 4.

B.2 Toepassingsprogrammatuur (object-coding)

Voor de object-coding zijn geen specifieke beveiligingsmaatregelen vereist immers bij een adequate beveiliging van de source-coding is de object-coding altijd door hercompilatie opnieuw te verkrijgen. De computertijd benodigd voor hercompilatie bepaalt in belangrijke mate het kostenniveau.
Om die reden wordt ook wel een éénmalige kopie getrokken, direct na compilatie.

C. Job Control Language (de karweibesturingstaal)

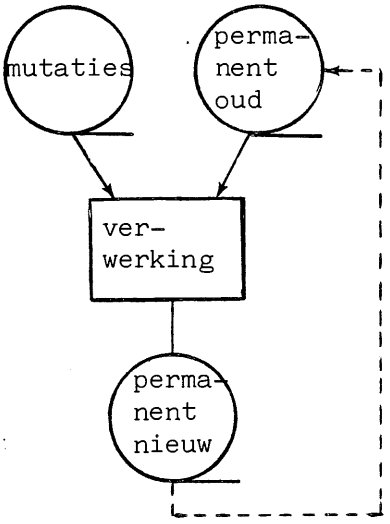
De registratie van de Job Control Language (JCL) geschiedt op magneetschijf, op ponskaart of een mengvorm van beide.
Met dit laatste wordt bedoeld dat met één (of enkele) ponskaart(en) de gehele job-definitie (de JCL-stream) wordt opgeroepen en voor uitvoering in de jobqueue (Readerqueue) wordt gezet. Een queue is een wachtkamer (vergelijkbaar met die van een tandarts).
Een mechanisme binnen de computerinstallatie selecteert hieruit de uit te voeren programma's.
Voor zover de JCL op magneetschijf staat kan deze real time on-line worden aangepast (bijvoorbeeld ten aanzien van wijziging van benodigde bestanden, e.d.).
Voor de continuïteit van de gegevensverwerking is slechts de JCL in de produktiesfeer van belang.
De back-up techniek is identiek aan het beschrevene onder "Toepassingsprogrammatuur" (source-coding) met betrekking tot systeemontwikkeling/onderhoud.
De JCL-ponskaartvorm wordt handmatig gewijzigd waardoor eveneens een nieuwe versie ontstaat.
Back-up kopieën zijn niet aanwezig. Voor het continuïteitsaspect is het van belang dat de gehele JCL-stream goed gedocumenteerd is om reconstructie mogelijk te maken. Hierbij dienen beveiligingseisen aan de documentatie te worden gesteld.

D. Gegevensbestanden

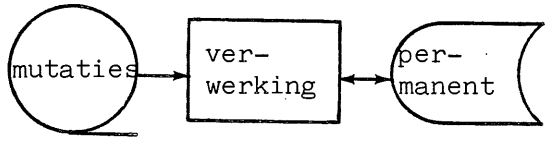
Dit zijn van oudsher de bestanden die uit continuïteitsoverwegingen de meeste aandacht hebben en hebben gekregen. De meest bekende techniek is het maken van kopieën volgens het generatieprincipe. In het magneetbandtijdperk was het maken van een kopie zowel medium- als objectgericht. Bij de introduktie van de schijf vond een verschuiving plaats naar objectgericht.
Uit efficiency-overwegingen werd later gekozen voor de mediumgerichte techniek. Hierop wordt nader ingegaan in paragraaf 3.2.
De gekozen techniek wordt mede bepaald door de verwerkingsomgeving. Ingegaan wordt op batch-verwerking (figuur 5), uitgestelde batch-verwerking (Data entry) figuur 7 en real time on-line-verwerking (figuur 8).

BATCH-VERWERKING (generatieprincipe)

a



b



Figuur 5.

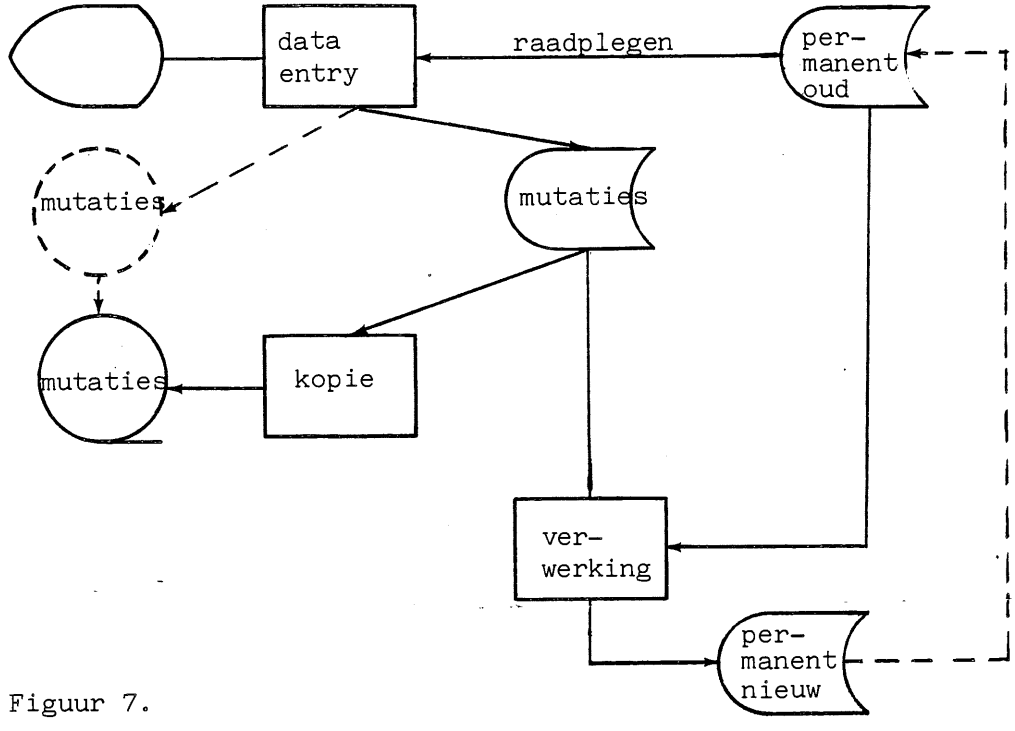
In de situatie sub a, waarbij alle bestanden op magneetband aanwezig zijn, wordt volstaan met het bewaren van permanente bestanden volgens een generatiesysteem (minimaal 3 generaties) aangevuld met mutatiebestanden (minimaal 2 generaties) (zie figuur 6).

	Machine	Kluis	Elders
Periode 1	P(0)	P(0)	
- Mutaties		M(1)	M(1)
- Permanent bestand	P(1)	P(0)+P(1)	P(0)
Periode 2			
- Mutaties		M(2)	M(1)
- Permanent bestand	P(2)	P(1)+P(2)	P(0)
Periode 3			
- Mutaties		M(3)	M(2)
- Permanent bestand	P(3)	P(2)+P(3)	P(1)
Periode 4			
- Mutaties		M(4)	M(3)
- Permanent bestand	P(4)	P(3)+P(4)	P(2)

Figuur 6.

Voor de situatie sub b, wordt verwezen naar het back-up schema source-library systeemontwikkeling/onderhoud (figuur 4).

DATA ENTRY



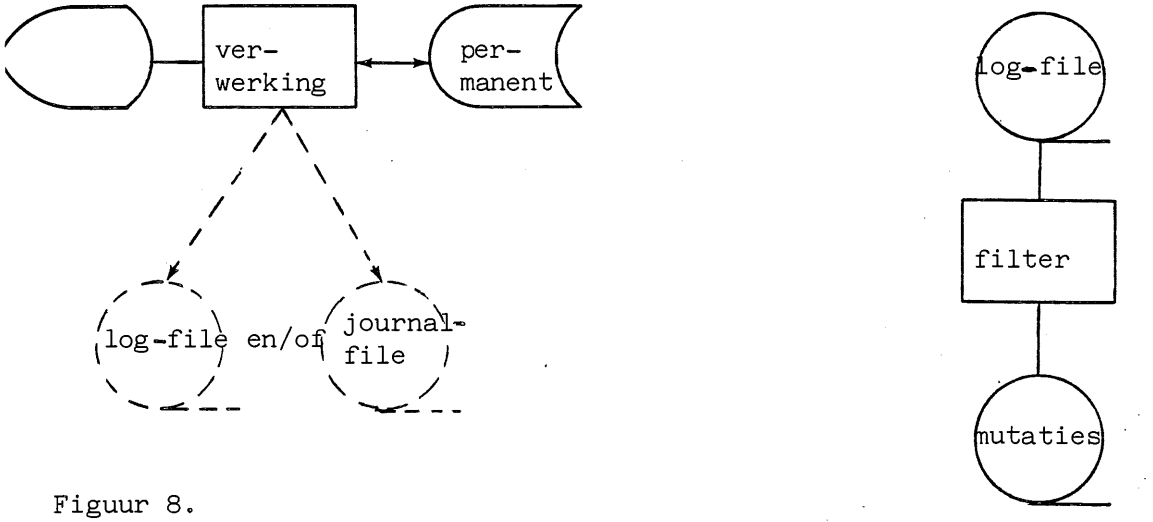
Figuur 7.

Data entry (ook wel uitgestelde batch-verwerking genoemd) kan voor wat betreft de beveiligingsproblematiek beschouwd worden als identiek aan het beschrevene onder de batch-verwerking.

De mutaties worden in de periode tussen twee verwerkingen weggeschreven naar:
- magneetschijf of magneetband;
- magneetschijf en ook naar magneetband;
- andere magnetiseerbare externe geheugenvormen.

Voor zover de mutaties alleen op magneetschijf worden weggeschreven, is het aan te bevelen een kopie te maken van het mutatiebestand op magneetband alvorens de verwerking wordt gestart.
Hierdoor wordt voorkomen dat bij het zich voordoen van een calamiteit de mutaties verloren gaan en derhalve opnieuw moeten worden ingevoerd.

REAL TIME ON-LINE



Figuur 8.

Bij real time on-line systemen worden mutaties direct op het bestand aangebracht.
Registratie van mutaties is noodzakelijk om het geheel controleerbaar te houden.
Standaard software die real time on-line-verwerking mogelijk maken, bieden de mogelijkheid of dwingen af om mutaties op een apart medium vast te leggen. Dit medium is een log en/of journalfile.
Hierbij kunnen zich 3 situaties voordoen:
1. journalfile;
2. logfile;
3. gecombineerde log/journalfile.

Ad 1.

De journalfile kan de volgende informatie bevatten:
- before images: dat wil zeggen de stand van het gemuteerde record voordat de wijziging geëffectueerd wordt;
- after images: dat wil zeggen de stand van het gemuteerde record na effectuering van de wijziging;
- before en after images;
- de mutaties zelf.

Ad 2.

Worden de mutaties geregistreerd op een logfile, dan zijn zij vermengd met andere systeemboodschappen (zoals logon/logoff, foutboodschappen, e.d.) en dient speciale programmatuur gebruikt te worden om deze mutaties "eruit" te filteren.

Ad 3.

Wordt naast de logfile gebruik gemaakt van een journalfile dan bevat de logfile alleen systeemboodschappen.
De informatie op de journalfile is reeds weergegeven in ad 1.
De journalfile en de "gefilterde" log file zijn te beschouwen als mutatiebestanden.
Om deze reden kan voor de back-up techniek worden verwezen naar het back-up schema source-library systeemontwikkeling/onderhoud (figuur 4).

E. Object versus medium

In hoofdstuk 3 zijn de vier categorieën aangegeven waarop back-up technieken zich dienen te richten, namelijk:
- het besturingssysteem;
- toepassingsprogrammatuur;
- job control language;
- gegevensbestanden.

Bovendien is genoemd dat kriteria kunnen leiden tot object c.q. medium gerichte wijze van het kopiëren van bestanden.
Onder object gericht wordt verstaan dat van een specifiek bestand') - van welke categorie dan ook - een kopie wordt gemaakt.
Van medium gericht kopiëren wordt gesproken als het maken van kopieën niet gericht is op een bestand maar op de informatiedrager waarop het bestand staat.

In de hierna volgende tabel (figuur 9) is aangegeven op welke media de diverse categorieën kunnen worden aangetroffen. De keuze van de back-up techniek (object c.q. medium gericht) wordt bepaald door:
- de door gebruikers gestelde (extra) eisen (bijvoorbeeld kritische gegevensverzamelingen);
- technische en efficiency gerichte overwegingen.

In de praktijk zal het voorkomen dat één of meerdere objecten op één of meerdere informatiedragers zijn geplaatst.

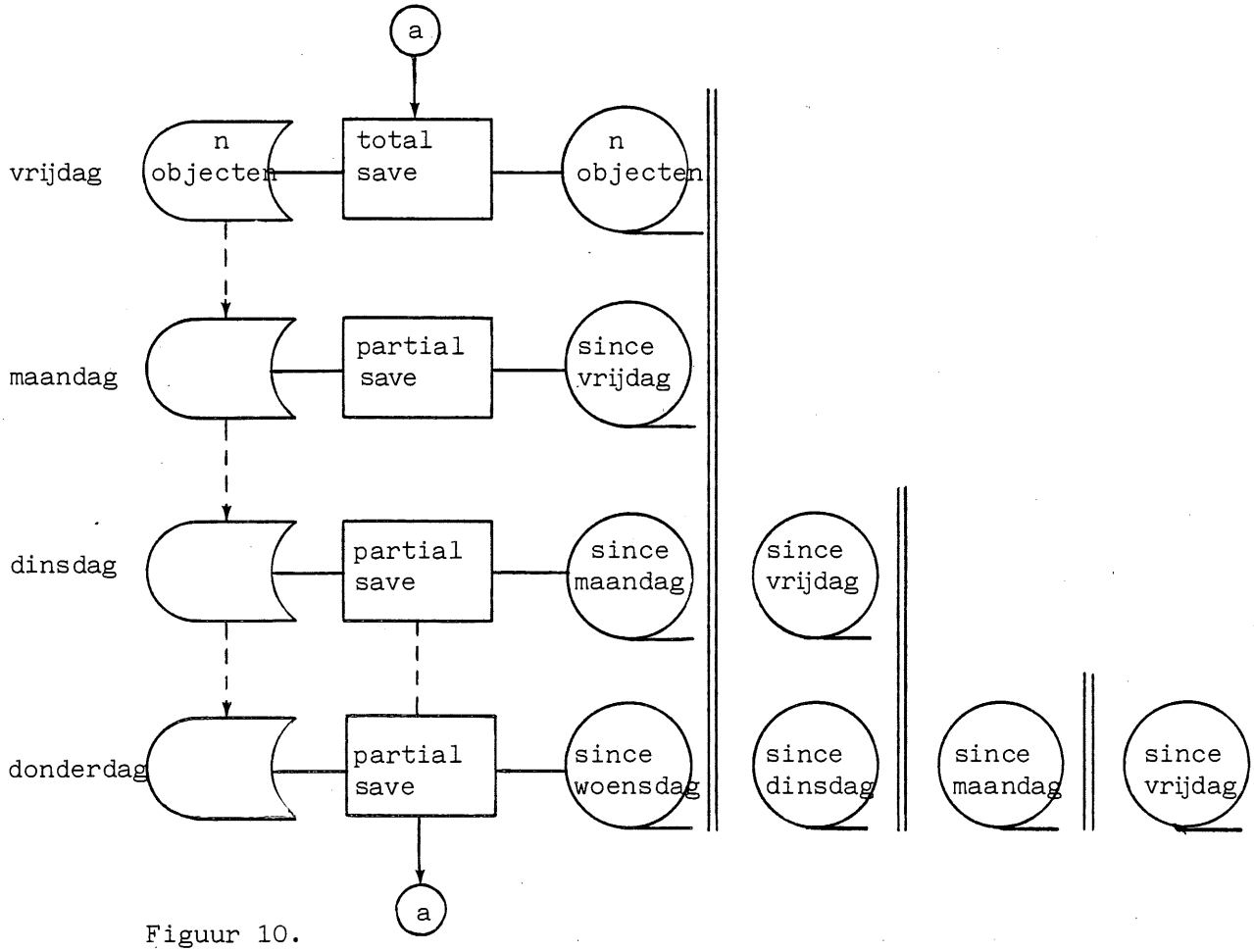
') In de zin van een "logisch" bestand. Dit bestand kan op grond van meerdere redenen (bijvoorbeeld omvang) over meerdere fysieke informatiedragers verdeeld zijn.

Object \ Medium	Magneetschijf	Magneetband en overige magnetiseerbare media	Ponskaart
A. Besturingssysteem en overige harde software (utilities)	X X	X X	
B. Toepassingsprogrammatuur			
B.1 Source-coding	X	X	X
B.2 Object-coding	X	X	
C. Job Control Language	X		X
D. Gegevensbestanden	X	X	X

Figuur 9.

3.2 Mengvorm object en medium gerichte techniek

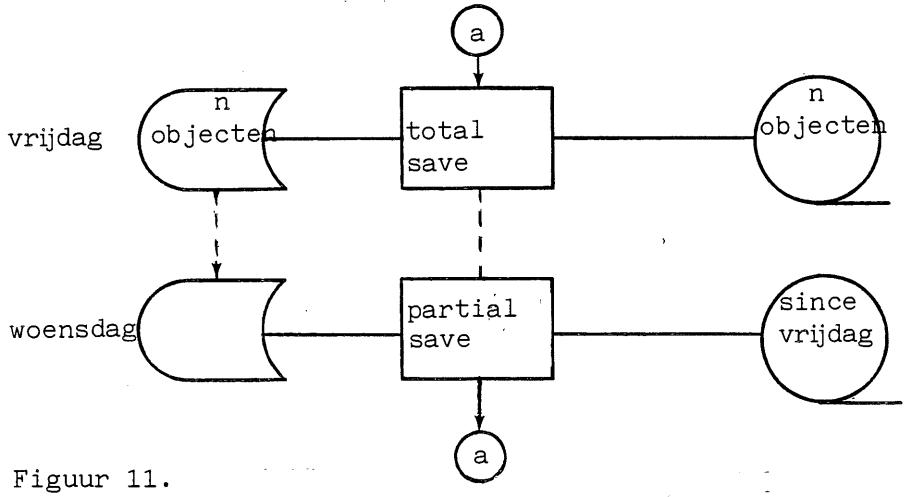
Naast de object en medium gerichte techniek komt een mengvorm voor. Deze bevat aspecten van beide technieken.
Uitgangspunt hierbij is het medium. Dit wordt meestal bepaald door technische aspecten. Bij vaste schijven is het uit beveiligingsoogpunt noodzakelijk dat een kopie van de daarop vermelde informatie elders aanwezig is. Meestal wordt gestart met het dagelijks kopiëren van de vaste schijf. Na verloop van tijd blijkt dat slechts bepaalde bestanden (objecten) frequent worden gemuteerd. Het blijkt dat het dan doelmatiger is dagelijks de gemuteerde objecten te kopiëren.
Gekopieerd worden het object en de datum van laatste wijziging. Dit laatste wordt uit de index van de informatiedrager gehaald.
Periodiek wordt de totale informatiedrager gekopieerd.
Hoewel deze mengvorm voornamelijk bij vaste schijven wordt gehanteerd komt zij ook bij verwisselbare schijven voor.



Figuur 10.

In figuur 10 is één en ander schematisch weergegeven.

Het is zeer wel mogelijk het tijdsinterval tussen het maken van back-up kopieën te vergroten. Het risico van verlies in geval van calamiteit wordt daardoor echter vergroot.
Het schema (figuur 11) wordt dan als volgt:



Figuur 11.

In voorgaande paragrafen is gesproken over object c.q. medium gerichte technieken alsmede een mengvorm.
De complexiteit van de gehele materie wordt vergroot door het feit dat deze technieken naast elkaar kunnen voorkomen binnen één en dezelfde produktie omgeven. De waarschuwing is op zijn plaats in de praktijk niet uit te gaan van "een back-up procedure". Het is verstandiger na te gaan of er meerdere zijn. Een antwoord als "Als back-up systeem wordt het generatieprincipe gehanteerd" is op zich niet veelzeggend.
Dit systeem kan binnen elke - in voorgaande - gehanteerde techniek voorkomen. Het gaat erom wat wordt gekopieerd en welk risico van gegevensverlies bestaat in geval van calamiteit. Hierbij dient niet uit het oog te worden verloren dat van alle categorieën de vereiste back-up kopieën zijn gemaakt om ingeval van calamiteit de continuïteit van de gegevensverwerking in redelijke mate te kunnen waarborgen.

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

compact

Zomer 1983

ONDERZOEK NAAR WERKING INTERNE CONTROLE MOGELIJK?

door drs. J.E. Huizenga

Inleiding

In de accountantsliteratuur heeft het begrip "interne controle" de laatste decennia een belangrijke plaats ingenomen. De discussies richten zich met name op de betekenis van de interne controle voor de werkzaamheden van de certificerende accountant.
Centraal in die discussies staat dat interne controle een middel is voor de bedrijfsleiding om in het delegatieproces toch voldoende greep op de uitvoering te houden.
Ook in de accountantscontrole wordt de interne controle gezien als een middel om de kwaliteit en de toereikendheid van de te controleren verantwoording te verhogen en aldus de controlewerkzaamheden van de accountant te beïnvloeden.
Zowel in de VS als in Nederland is een ontwikkeling gaande, waarvan het gevolg zou kunnen zijn dat de interne controle zelfstandig object van onderzoek voor accountants wordt.
In dit artikel wordt de hiervoor genoemde ontwikkeling geschetst, tevens wordt ingegaan op de gevolgen voor het accountantsonderzoek in een geautomatiseerde omgeving.

Enige ontwikkelingen in de Verenigde Staten

Het zou geen verbazing wekken als in het Amerikaanse accountantsberoep enige verwarring is ontstaan over de betekenis van de interne controle voor de accountantscontrole.

Enerzijds stelt het Amerikaanse instituut in SAS 43 (omnibus statement on auditing): "If the auditor does not plan to rely on internal accounting control, he need not document his understanding of the internal accounting control system" en "Documentation may be limited to a record of the auditor's reasons for deciding not to extend his review of the system of internal accounting control past the minimum level".
Dit betekent dat de accountant ook in gevallen van vergaand geautomatiseerde administratieve systemen vrij is in de keuze bij zijn controle het stelsel van interne controlemaatregelen te betrekken!

Anderzijds is naar aanleiding van de omkoopschandalen uit het midden van de jaren zeventig, een ontwikkeling op gang gekomen naar meer aandacht voor de interne controle.
Een van de gevolgen van de affaires (Lockheed en dergelijke) was het uitvaardigen van de Foreign Corrupt Practices Act (FCPA) in 1977. In de wet zijn onder andere voorschriften opgenomen met betrekking tot de interne controle.

Het doel van de voorschriften is het voorkomen van omkooppraktijken door bedrijven te verplichten een voor dat doel adequate interne controle op te zetten en te handhaven, zodat:
- "transactions are executed in accordance with management's general or specific authorization;
- "transactions are recorded as necessary (a) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and for (b) to maintain accountability assets;
- "access to assets is permitted only in accordance with management's general or specific authorization and;
- "the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences".

De Security Exchange Commission (SEC), welke belast is met het toezicht op de aan Amerikaanse beurzen genoteerde fondsen, vond in de FCPA aanleiding om het management (de directie) van ter beurze genoteerde bedrijven aan te bevelen:
- mede te delen dat het systeem van interne controle voldoet aan de in de FCPA gestelde eisen;
- elke belangrijke zwakke plek in de interne controle (material weakness in internal control) te publiceren, indien die zwakke plek niet gedurende het boekjaar is gecorrigeerd.

In eerste aanleg heeft de SEC bepaald dat de mededeling door het management na een proefperiode van drie jaar verplicht zou worden (te voegen bij de te deponeren jaarrekening) en vervolgens zou de externe accountant de mededeling moeten controleren en over de uitkomsten van zijn controle rapporteren.

In 1982 was de proefperiode voorbij en de druk kennelijk van de ketel, waarschijnlijk mede naar aanleiding van de vloed van (negatieve) reacties. In maart 1982 bepaalde de SEC dat de rapportage en derhalve ook de controle vooralsnog niet verplicht werden gesteld.

Hoewel de poging van de SEC om te komen tot <u>verplichte rapportage</u> over interne controle mislukt lijkt, heeft de affaire wel degelijk invloed gehad op de aandacht die in de VS besteed wordt aan internal accounting controls.

Samenvattend kan gesteld worden dat het Amerikaanse Instituut (AICPA) de accountant vrijer laat bij de beoordeling van de interne controle in het kader van de jaarrekeningencontrole. De Security Exchange Commission daarentegen dringt aan op mededelingen (al dan niet gecontroleerd en gecertificeerd) over de interne controle sec.

Nederland

Traditioneel vaardigt het Nederlands Instituut van Registeraccountants geen richtlijnen uit voor de inhoud van het accountantsonderzoek (de studie en voortgezette educatie geven voldoende waarborgen voor de vaktechnische kwaliteit, repressief is er het tuchtrecht). Een voorschrift omtrent het betrekken van de interne controle in de accountantscontrole bestaat hier dan ook niet; hetwelk niet inhoud dat in Nederland de interne controle wordt genegeerd, integendeel!
Een recente ontwikkeling welke zou kunnen duiden naar het geven van een oordeel over de interne controle heeft op het privacygebied plaatsgevonden.
In het ontwerp van "Wet op de Persoonsregistratie" is sprake van controle door de registratiekamer op de naleving van de reglementen met betrekking tot persoonsregistratie.
Het NIVRA heeft op het ontwerp van wet gereageerd met een studierapport "Privacy bescherming en Accountant", waarin wordt beargumenteerd waarom de accountant een rol kan spelen bij de controle op de naleving van privacyreglementen.
Tevens wordt in het rapport kort ingegaan op de aard van het te verrichten onderzoek en de wijze waarop de accountant de uitkomsten van zijn onderzoek zou kunnen verwoorden.

Interne controle als object van onderzoek

Zowel in de SEC-voorstellen als in het NIVRA-studierapport is er een voor accountants nieuw facet aan het onderzoek naar de werking van de interne controle. Het gaat niet meer om de werking voor zover van belang voor de totstandkoming van de jaarrekening of een andere verantwoording. In de hiervoor bedoelde situatie gaat het ook om incidentele afwijkingen in het stelsel van interne controlemaatregelen, welke afwijkingen niet hebben hoeven leiden tot materiële fouten in de verantwoording. Aan de gevolgen van deze wijziging in de doelstelling van de accountantscontrole op de uit te voeren controlewerkzaamheden, is in de literatuur weinig aandacht besteed.

Hieronder zal in het kort worden ingegaan op een aantal facetten van een onderzoek naar de continue werking van het stelsel van interne controlemaatregelen in een geautomatiseerde administratieve omgeving.

Onderzoek werking interne controle bij geautomatiseerde gegevensverwerking

De fasen in een onderzoek naar interne controle zijn in een geautomatiseerde omgeving niet anders dan bij een controle in een niet geautomatiseerde omgeving:
a. vastleggen van de administratieve organisatie;
b. vaststellen van het bestaan op enig moment (controle van de vastlegging);
c. beoordelen of de opzet mogelijkheden biedt de interne controledoelstelling te verwezenlijken;
d. vaststellen van het functioneren gedurende de verslagperiode.

In de laatste fase zit met name het onderscheid tussen controle gericht op de jaarrekening en de controle op de werking van de interne controle zoals hiervoor beschreven.
Wanneer ervan wordt uitgegaan dat in een geautomatiseerde omgeving de functiescheiding in de gebruikersorganisatie in opzet als voldoende is beoordeeld, doet zich de extra complicerende factor voor van de invloed van de automatisering op die functiescheiding.
Of met andere woorden: wordt de functiescheiding in de gebruikersorganisatie doorbroken onder invloed van de automatisering?

Thans is een normale automatiseringsomgeving als volgt te kenmerken: meerdere gebruikers maken tegelijkertijd met behulp van meerdere terminals gebruik van dezelfde computer om zowel gelijke als verschillende processen uit te voeren; tevens vindt met behulp van terminals on-line-programmering, produktiebesturing en werkvoorbereiding plaats.

In een dergelijke omgeving rijzen met betrekking tot de voortdurende handhaving voor de gewenste functiescheiding de volgende vragen:
- hoe is een effectieve scheiding gewaarborgd tussen de produktie en de ontwikkelingsomgeving?
- hoe is een effectieve scheiding gewaarborgd tussen de gebruikers onderling?

Notabene: Er wordt hier verondersteld dat de toepassingssystemen op zich, indien zij "stand-alone" zouden draaien, de gegevens juist verwerken.

Op het gebruikersniveau zijn dit vragen die betrekking hebben op de werking van de interne controle.
Op automatiseringsniveau dient wederom eerst gevraagd te worden naar de opzet en beoordeling van de opzet, alvorens (wellicht) iets kan worden gezegd over de werking.
Wat de opzet betreft zijn een aantal middelen beschikbaar:
- de organisatorische opzet dient de randvoorwaarden voor een effectieve functiescheiding te scheppen;

- procedures zijn er om inhoud te geven aan de organisatorische maatregelen;
- de techniek heeft een grote invloed op de effectiviteit van de procedures. Hierbij dient met name gedacht te worden aan:
  . de wijze waarop het besturingssysteem is geconfigureerd;
  . de manier waarop het Data Base Management Systeem, ondersteund door het Data Dictionary Systeem, wordt gebruikt;
  . de parametrisering van de Teleprocessing Monitor.

In het kader van zijn onderzoek naar de handhaving van de goede werking van het systeem van interne controle kan de accountant, bijgestaan door een deskundige EDP-auditor, zich een oordeel vormen over de opzet van de automatisering.
Met een uitgekiend stelsel van controlemiddelen en -technieken (voor een deel reeds in Compact beschreven) kan een indruk worden verkregen over de effectiviteit van de interne controlemaatregelen.

> Een oordeel over de continue werking vereist echter een nauwkeurig en volledig onbeïnvloedbaar meetinstrument, dat voortdurend actief is.

Aangezien een dergelijk instrument vooralsnog niet voorhanden is, is in het "voorbeeld voor een mededeling met goedkeurend oordeel over de werking van een verwerkingsorganisatie en alle daarin gebruikte informatiesystemen" (NIVRA-geschrift 26, blz. 35) het oordeel als volgt geformuleerd:
"Op grond van ons onderzoek delen wij u mede dat er zich in de onderzoekperiode geen systematische afwijkingen van betekenis hebben voorgedaan ten opzichte van de door ons beoordeelde stelsels van maatregelen en procedures".
De conclusie moet dan ook zijn dat met de huidige controlemiddelen de "volledige zekerheid" dat de interne controle voortdurend heeft gewerkt niet verkregen kan worden.

Echt verwonderlijk is dit niet, immers men gebruikt het systeem van interne controle om de werking van de gebruikerssystemen te beheersen en te toetsen. Dat is het normale gebruik van de interne controle als één van de controlemiddelen die de accountant ten dienste staan bij zijn jaarrekeningcontrole.
Indien de interne controle zelf object van onderzoek wordt, is het systeem van interne controle noodzakelijkerwijs niet toereikend om tot een sluitend oordeel te komen.
Hier dringt zich de parallel op met het uit de wiskunde bekende theorema van Gödel dat als volgt verwoord zou kunnen worden:
"Binnen de grenzen van een systeem is het onmogelijk te bewijzen dat dát systeem compleet en consistent is."

Samenvatting

Enkele factoren zijn geschetst waardoor accountants geconfronteerd worden met onderzoekingen naar de voortdurende goede werking van het systeem van interne controle.
Vervolgens is aangegeven welke stappen moeten worden gezet bij de uitvoering van zo'n onderzoek in een geautomatiseerde omgeving.
Er blijken vooralsnog geen instrumenten aanwezig om de voortdurende goede werking van de in de automatisering opgenomen maatregelen van interne controle op een economisch rationele wijze vast te stellen.
Dit wordt veroorzaakt doordat een meetinstrument om de goede werking van toepassingssystemen vast te stellen, de interne controle, zelf object van onderzoek wordt.
Het is derhalve niet verwonderlijk dat de rapportering over zo'n onderzoek uiteindelijk niet verplicht is gesteld (VS-SEC) dan wel een ruime marge voor niet ontdekte afwijkingen laat (Nederland).

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

compact

Zomer 1983

DATA ENTRY EN INTERACTIEF PROGRAMMEREN VIA DE TERMINAL: HET PAKKET ICCF NADER BEKEKEN

door R.P. Bosman

Inleiding

Data entry en interactief programmeren stellen de gebruiker c.q. programmeur in staat gegevens en programma's via de beeldschermterminal in te voeren, programma's ter verwerking aan het centrale computersysteem aan te bieden en uitvoer of boodschappen op het scherm te ontvangen. Onder interactief programmeren verstaat men de situatie waarbij tijdens het programmeren een voortdurende dialoog plaatsvindt tussen de programmeur en het systeem. In feite vervangen het terminal-toetsenbord en beeldscherm de kaartlezer, kaartponsmachine en in zekere zin de printer in een traditionele batchomgeving. Deze manier van invoeren en programmeren werkt snel en efficiënt, maar het goed beheersen van zaken als de opslag en beveiliging van data moet niet worden onderschat.
Voor data entry en interactief programmeren in een IBM/VSE/POWER-omgeving wordt met name het pakket ICCF veel gebruikt. Dit pakket wordt wel een 'on-line-editing-tool' genoemd en heeft als voornaamste taak het verzorgen van gegevensverkeer tussen terminal en centrale computer.
Ook bij KKC wordt voor het ontwikkelen, starten van verwerking en archiveren van auditprogrammatuur gebruik gemaakt van ICCF.
In het vervolg van dit artikel zal nader worden ingegaan op de werking en de functies van ICCF.

Het pakket ICCF (Interactive Computing and Control Facility) is een product van IBM. ICCF kan geladen worden in een VSE-partitie en bestaat uit vier componenten (logical areas), namelijk:

1. VSE/ICCF control program.
2. Foreground Command processors.
3. Background interactive partitions.
4. Terminal control program.

De foreground Command processors interpreteren de via de terminal ingevoerde commando's en voeren deze uit onder beheer van een datacommunicatiemonitor (TTF of CICS). Bij data entry worden de gegevens via het terminal control program en de foreground command processors in de ICCF-library opgenomen. De toegang tot de ICCF-library en de activiteiten in de background interactive partition worden beheerd door het VSE/ICCF control program. Bij het interactief programmeren wordt er door het VSE/ICCF control program een vrije interactieve partitie gereserveerd en een programma ter verwerking aangeboden. Na uitvoering verschijnt via het terminal control program de output op het scherm van de gebruiker. Mits de betreffende compilers op de centrale computer aanwezig zijn, bestaat de mogelijkheid tot interactief programmeren in de volgende talen: ASSEMBLER, COBOL, FORTRAN, PL/1, RPG II en BASIC.

Libraries

De VSE/ICCF system library (systeemprogrammabibliotheek) is één dataset die verdeeld kan zijn over een of meerdere diskpacks. Deze library bevat verschillende data files en een tabel met user-profiles; dit zijn gegevens over een gebruiker en zij bevatten onder andere user-identifications en passwords. Wanneer een gebruiker de verbinding tot stand heeft gebracht, heeft hij slechts de beschikking over die files die bij zijn password horen. Dit noemt men een user-library. Er zijn drie typen user-libraries, namelijk:

1. private library;
2. public library;
3. common library.

De private library is alleen toegankelijk indien user-profiles overeenkomen met ingetoetste user-identification en password. Een gebruiker kan meerdere user-libraries bezitten die hij vanuit zijn primary user-library kan aanroepen, de zogenaamde alternate user-libraries. Een public library is door iedereen te benaderen, maar moet bij gebruik worden gekoppeld aan de primary user-library door middel van het /SWITCH of /CONNECT-commando. De common library is ook door iedereen te benaderen op read-only basis en is tijdens installatie standaard gekoppeld aan de primary user-libraries en bevat bijvoorbeeld ICCF-commando's en procedures.

De sign-on procedure

Via een sign-on procedure kan een gebruiker om toegang tot het systeem verzoeken. Dit gebeurt meestal door het intoetsen van een unieke code (password), die door het systeem moet worden herkend. Nadat de verbinding tot stand is gebracht, heeft de gebruiker de beschikking over de programma's of data-files uit zijn user-library alsmede een aantal standaardfuncties van het pakket zoals het invoeren, wijzigen en verwijderen van programma's en data-files, "bladeren" in de output, het al dan niet interactief ter verwerking aanbieden van jobs en het opvragen van de machinestatus.

Bij ICCF moet de gebruiker eerst een user-identification intoetsen en daarna het password. De user-identification verschijnt wel op het scherm, het password niet. De user-identification en het password worden door het systeem vergeleken met een tabel met user-profiles, die zich voorin de VSE/ICCF library bevindt.
Indien ingetoetste gegevens overeenkomen met de gegevens uit de tabel heeft de gebruiker toegang tot zijn user-library. Indien men een fout maakt bij de sign-on procedure geeft het systeem een melding en kan men deze handeling een aantal malen herhalen. Derhalve moeten procedurele maatregelen getroffen worden om misbruik te voorkomen. De ICCF-gebruiker kan zijn eigen password veranderen door middel van het /PASSWRD commando, mits hij daartoe volgens zijn user-profile gerechtigd is.

User-profiles

De beheerder van het ICCF-pakket (ICCF-administrator), kan tijdens installatie van ICCF een aantal user- libraries creëren. Per user(-library) heeft hij de mogelijkheid beperkingen op te leggen wat betreft het gebruik van bepaalde functies van ICCF. Het toekennen van deze zogenaamde user-profiles gebeurt met het programma DTSUTIL. Dit programma kan ook draaien als ICCF reeds geladen doch niet in gebruik is. Het programma initialiseert de 'option flag bytes' (OPTA byte of OPTB/OPTC), waarvan elke bit een bepaalde functie afschermt of toekent (0 of 1). In totaal zijn 24 (3 x 8) functies af te schermen. Ter illustratie: indien de derde bit uit de OPTA-byte op één staat, betekent dit dat een gebruiker een member kan wijzigen ook al verschilt zijn user-identification van de user-ID van degene die de member heeft ingevoerd. Het zal duidelijk zijn dat wanneer bij het "aanzetten" van de bits een fout wordt gemaakt de mogelijkheid bestaat dat een gebruiker ten onrechte de beschikking krijgt over specifieke ICCF-functies. De mogelijkheid bestaat om de user-identifications met bijbehorende flag bytes af te drukken. Ter illustratie een voorbeeld van een DTSUTIL programma voor het creëren van een nieuwe user-library. De flag bytes zijn onderstreept.

```
10  // JOB    BUILD FILE
11  (ASSIGN/DLBL/EXTENT for DTSFILE)
12  // EXEC   DTSUTIL
20  FORMAT    LIB(40),USERS(30)
21  ADD  LIB,FREE(25)                  (add library no. 1)
22  ADD  LIB,MAX(200)                  (add library no. 2-common library)
23  ADD  LIB,MAX(200),FREE(25)         (add library no. 3)
30  ADD  USER ID(AAAA),LIB(1),PAS(D$ADMN),OPTA(01110111),
31  ADD  USER ID(AAAA),OPTB(11111110)
40  ADD  USER ID(UCDA),LIB(3),PASS(AWLNOV),MAXST(800),SEC(58 U 16 32 U)
41  ADD  BROADCAST
50  * MAY 22, 1983.  SYSTEM WILL SHUTDOWN AT 6 PM.
51  ADD  MEMBER (2,A$MAIL,ADMN)
52       VSE/ICCF GENERAL MAIL A NEW
53       UTILITY HAS BEEN ADDED TO THE ETC., ETC.
56  UCDA SPECIFIC MAIL FOR USER UCDA
60  UCDA BACKUP AND RESTORE THE LIBRARY FILE
71  END OF MEMBER
72  /*
73  /&
```

Toelichting

regel 10 e.v. aanmaak system library
regel 20 e.v. initialisatie van de toe te voegen libraries
regel 30 e.v. initialiseren van de option flag bytes

In bovenstaand voorbeeld is "AAAA" de user-identification van de nieuw toe te voegen user-library. "D$ADMN" is het password en LIB(1) geeft het nummer van de toe te voegen library weer. De OPTC-byte wordt in dit programma niet opgegeven en staat initieel op nul voor deze library.

regel 40 e.v. beschrijving van de gebruiker met security regels, password, gebruik library, etc. verzending bericht.
regel 50 e.v. tijdregels met andere huishoudelijke regels
regel 60 e.v. beveiliging gegevens door back-up, restore
regel 70 e.v. afsluiten job.

Modes of operation

ICCF kent verschillende basisfuncties de "modes of operation". Eenmaal aangelogd onder ICCF bevindt het beeldscherm zich altijd in de command mode, waarbij commando's kunnen worden ingetoetst. Verder zijn er nog de input, update, edit, execute en list mode.
Om in deze modes te kunnen werken onderscheidt ICCF een aantal typen statements namelijk system commands, context en editor commands, procedures en macro's (bestaan uit procedure statements). Al deze typen statements hebben hun eigen syntax en zijn aan bepaalde modes of operation gebonden.

Functies en commando's

Zoals reeds eerder genoemd heeft ICCF een aantal typen commando's met elk een eigen voorvoegsel. De commando's zijn zelfverklarende namen, maar door de veelheid van typen is een vergissing snel gemaakt. Een aantal voorbeelden van ICCF-commando's zijn:

@ED	membername	edit commando
/L	membername	list commando
$DA		voor het opvragen van machinestatus
SUBMIT	membername	ter batchverwerking aanbieden van een programma.

Deze commando's worden ingetoetst op de bovenste beeldschermregel, het "command field".
In het command field kan slechts één commando tegelijk worden ingetoetst.
Voor een summiere functiebeschrijving kan men /HELP intoetsen.

Het pakket ICCF heeft niet uitsluitend een data-entry- en programmeerfunctie. Door de mogelijkheden van documentatie, communicatie, het samenvoegen van programma's tot jobstreams, controles op autorisatie en het opnemen van standaardprogrammatuur (bijvoorbeeld planningprogramma, tapecatalogue, VTØC) vormen on-line editing tools een onmisbare schakel in een moderne produktie-omgeving.

DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE

door H. Veenman

Nieuws van het audit-micro front

De Hyperion als mogelijke Audit-Micro.

Sinds enkele weken heeft de audit-micro-groep de beschikking over een draagbare microcomputer, genaamd "HYPERION".
Deze computer weegt ca. 9,6 kg en wordt geleverd in een draagtas, waarin ze gemakkelijk vervoerd kan worden.
De Hyperion is uitgerust met een 7 inch beeldscherm, een tweetal diskettestations en een intern geheugen van 256.000 tekens. Na enkele weken van intensief gebruik is gebleken dat deze computer mag worden beschouwd als de meest geavanceerde en gebruikersvriendelijke draagbare micro tot nu toe.

De Hyperion is uiterst geschikt voor het gebruik als tekstverwerker, maar ze wordt door de micro-groep ook toegepast ten behoeve van het ontwikkelen van programmatuur.
De Hyperion is nagenoeg geheel compatible met de reeds door de micro-groep gebruikte IBM Personal Computer, hetgeen inhoudt, dat bijna alle programma's van de IBM zonder meer kunnen worden overgezet op de Hyperion; ook de programmatuur, die tot nu toe op de IBM Personal Computer is ontwikkeld, kan op deze computer worden geladen.
Naar het zich laat aanzien zal de Hyperion model staan voor de verdere ontwikkeling van de Audit Software.

Hierna volgt het derde en laatste deel van de speech van Mr. Raymond H. Healey.
Healey zal ingaan op de positie van KMG binnen de zich met enorme snelheid ontwikkelende markt van de microcomputers, zoals die worden toegepast bij kantoorautomatisering, e.d.

DOWN TO EARTH AGAIN, KMG POTENTIAL (red.)

Speech regarding microcomputers presented by
Raymond H. Healey (last part) November 1982 ')

Now that we have examined some of the factors that are going to impact the business environment, and influence the way we will do things in our profession, we should review the current status of computer related activities in KMG (see part I and II in Compact 83/1 and 83/2).
How is KMG responding? There has been a significant response to selected areas of opportunity by many national firms and some impressive progress has been made in certain areas. Time does not permit me to catalogue the individual achievements but it should be noted that there is considerable skill and expertise spread throughout the KMG organization that suitably co-ordinated will be able to obtain important and cost effective results through co-operation and synergism.
With the will to work together, we will surely prove that 1 + 1 = 3 or 5 or is it more. In very general terms, the status of computerization, the role of the computer and the computer auditor in the audit practice of the larger KMG firms falls approximately into the following pattern.

The first area is audit support. There is generally a full range of support services available to the field auditors ranging from technical support in the review of systems and controls to decisions on audit strategy and the design and execution of audit tests using CAATs. Otherwise known as computer assisted audit techniques.
There are specially designed computer programs that operate against client data files to support audit testing by performing functions such as sampling or selection (statistical or judgmental), summarization and accumulation, calculations, reperformance, and assist with other functions such as analytical procedures and confirmations.
Another aspect of audit support is the KMG Audit Manual.
It will be used by many firms to guide them in performing audits in an EDP environment or as a reference to amend their own audit procedures and internal training courses.

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

The second major area is called engagement support.
Engagement support currently takes the form of the preparation of audit working papers such as working paper lead schedules and supporting schedules, the preparation of working trial balance, the posting of adjusting entries, the preparation of accumulation schedules, the preparation of consolidation and combinations, and administrative procedures such as fee analysis, time control, scheduling of jobs and staff, time budget analysis, and the preparation of various other audit forms and schedules. Some of these functions have been automated using micro or mainframe computers.

A third area is office management.
This covers the automated techniques to change the administrative process from one that is heavily dependent on clerks and paper to an integrated, EDP supported structure that ties together the many parts of the office management process.
The integrated electronic office or office of the future will connect together computer mainframes, personnel computers, word processors, videotext terminals, photocopiers, printers and other devices to co-ordinate such diverse applications as manpower control, budgets and fee administration, internal accounting and MIS, time control, training program schedules, word processing and electronic mail.
Special services are often requested by clients.
Many traditional client services are supported by EDP such as the building of computer models for forecasting, cash flow projections, planning and budgeting and routine or special tax returns.
Specialized accounting systems services are offered to clients in three major forms. Turnkey accounting packages will become more popular as prices fall and packages become more popular. These systems are fully tested and are turned over to client personnel ready for implementation and operation along with training and support services. Client staff are usually given extensive training in order to operate the packages with a minimum amount of technical expertise. Sometimes customized-software applications are developed to fit specific industries of business practices. In other instances, the firm assists the client to select a standard accounting package from a commercial software house. Usually these packages cut across industries and can be applied successfully in a variety of vertical or horizontal business structures. In some cases, certain firms are able to offer highly sophisticated accounting services to their clients by appearing to customize a package which is in fact a generalized package with many customized features that are industry specific - called systems integrators - which is no more than a package of computer hardware, peripherals and software programs modified for a particular type of user.

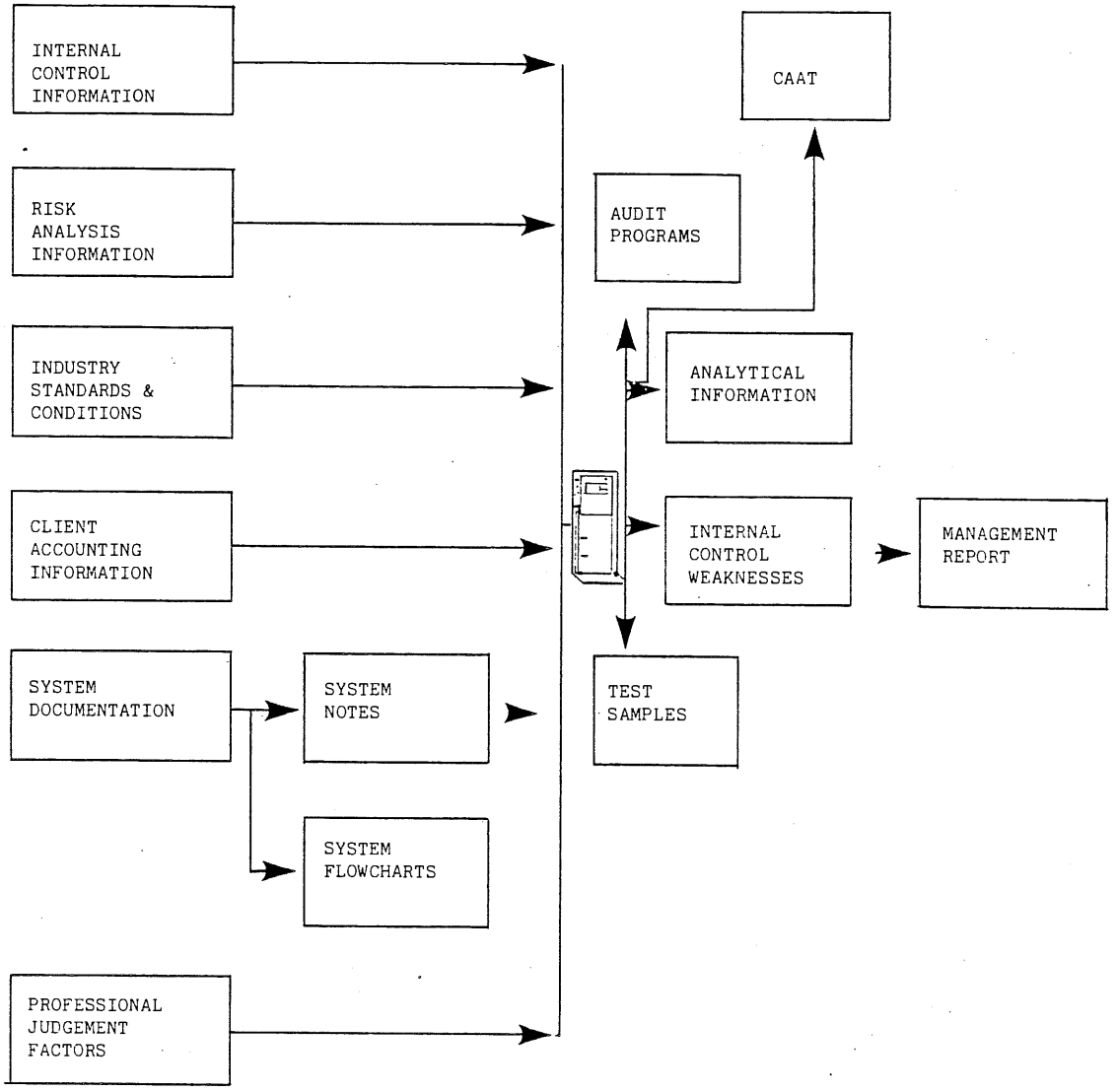
Other special services that are being provided include the training of client personnel in EDP matters (i.e., internal auditors, systems designers, managers on the use of micros), project management, systems standards development and maintenance, and EDP consultancy.

The final area that illustrates where we are today in KMG concerns data bank or information data bases.
The advancement of data processing and particularly electronic information storage techniques will provide a means for easy access to vast amounts of information which is useful to the public accounting firm. The traditional manual library is quickly giving way to the use of computerized data banks, both private or commercial, that will make vast amounts of information about every facet of the business and professional activities easily and readily available for daily reference or research purposes. The electronic file cabinet will revolutionize the procedures used in our practice to store, retrieve and transmit information in a paper intensive environment. Only moderate progress has been made by KMG in this area.
At the KMG level, co-operation between the TEC, CASC and the AAC*) has led to some impressive progress in the development and presentation of computer-related training courses. In parallel with this KMG base, firms such as TMcL and KKC have added additional training programs that are more specifically tailored to the requirements of their overall audit approach and have integrated computer audit training into the student level programs.
On a top down, or overall basis, the training courses, at least in the KMG structure tends to follow this pattern. Courses covering planning and directing the audit in an EDP environment are usually provided to partners and senior managers.
This type of course concentrates on the development of a suitable overall audit approach to computer based clients and is well represented by the famous or infamous 2-day Goliath course which is used in various forms by numerous KMG firms.
The next level down which we can refer to as the doing or performing of the audit, there is a wide variety of approaches that can be characterized throughout KMG by the 5-day course commonly referred to as Rippkoff.
Rippkoff and its various imitators has the decided advantage of requiring the participants to consider all aspects of an actual audit situation including: the review of a new system, the preparation of auditors comments to management on the system, the study and evaluation of the implemented system and completion of the internal control evaluation, the development of the audit approach and specific audit programs, the preparation of a management letter, and the conduct of the audit itself based on a combination of manual and CAAT based procedures.

---

*) TEC = Training and Education Committee
CASC = Computer Audit Subcommittee
AAC = Auditing and Accounting Committee

Throughout this comprehensive case study there are lectures to support the technical matters and the specific tasks the auditor will encounter in an EDP environment. In several firms in KMG, these various learning objectives have been dissected, supplemented and integrated throughout the training programs for students and graduate staff quite successfully.
An additional training function is the delivery of more technical courses for computer audit specialists or part time specialists. These take somewhat different form throughout KMG but core material always includes the specially developed KMG courses in the use of KMG audit software, EDP-Auditor and CARS -- which is now in place in about 14 KMG firms. Quite often these are supplemented by training in computer languages such as COBOL, RPG and more recently in response to the micro invasion, BASIC.
Other computer related training courses covering matters such as general EDP orientation and familiarization, computer selection, software or package evaluation and selection and micro computer usage are gaining in use. Equally, special technical courses for specialists are growing in frequency.
This all may seem to be a heavy duty and impressive effort, even viewed from this high level but does it really have a useful purpose.
Clearly the underlying purpose of all of these activities is to make it easier and more efficient for the KMG auditor to carry out his duties in an EDP environment. All of this looks like impressive progress but before we lapse into self-satisfied euphoria, it might be wise to look around at the competition. What are they doing?
Well, the bad news is that collectively they are doing virtually everything that KMG has done, and more. The good news is that many of the projects are not finished and some are a long way from being delivered as a practical, working approach. Rather than list what we know or have deducted that the other major firms are working on, the best approach to illustrate what the competition are trying to do may be to build up a prospective audit model -- a scenario that combines everything that we know is under development and some good guesses about many things we don't know. Perhaps this model is a reasonable forecast of what is going to happen to auditing in a few years. (zie pag. 36 red.)
The first input to the model is internal control information specific to the clients systems.



Prospective audit model.

Combined with the results of a risk analysis based on knowledge of the clients business, industry sector, management style, control consciousness and other factors specific to the client environment, industry standards and conditions, key ratios and other performance measurement data are added.
Now it might be a good idea to capture specific accounting information about the clients operation.
Systems documentation is transferred directly from the computerized text files and fed through a conversion program to produce systems notes and flowcharts. This nearly completes the process of entering the relevant data on the client profile and the industry sector.
The data is now fed into a computer which contains the templates, decision tables and other logical representations of the audit approache of the firm.
However, one very important ingredient, professional judgement is finally added to this array of factual information.
All these data are combined, analyzed, and cross-related into an automated audit model that has been built up from the prevailing professional standards and audit procedures of the firm, amended by the engagement partner to reflect his knowledge and judgement of the client situation. This logical model is used to produce an overall audit approach, based on reliance or non-reliance on internal control, completed analytical procedures, both client and industry related, audit programs including specific test sample selection and where appropriate, CAATs to assist with the testing, lists of weaknesses and draft material for the management letter.
If you think this is far-fetched you should think about some of the signals that are coming from within the profession, such as the audit computer, a portable device which is intended to directly access clients data and support many automated CAATs immediately and on site.

Quite apart from the pressure being exerted by competitors within our own profession, there is a growing list of other competitors such as the computer security consultants who are specializing in computer related matters and may present a real threat to our traditional fee base.
The software houses will grow in importance. The Financial Times Survey, dated November 5, showed growth in this industry of 31% in 1980 and 42% in 1981 - mirroring the rapid growth in software development. Digital Research in the USA is a good example. It was founded by Gary Kildall, a US citizen who produced the software program known as CP/M which is, perhaps, the most important single piece of software in the microcomputer world. It sells for only $150. Nearly everyone with a microcomputer has one. The company now has 240 employees, producing CP/M and other products at a sales level of $240M/year.

New micro based bookkeeping services are also a new area.
The F.T. Survey on professional services shows growth of 21% in 1981 for 45% of $1,500M UK market expenditures on computing services.

And finally the service bureau and computer utilities.
Typical services that are provided by this group include bookkeeping, risk analysis, computer security reviews, system evaluation and selection, contract consulting including forecasting, planning and computer consulting and training. While many of these do not pose a direct threat to the audit function, they do chip away at the broad range of services that one should expect from a major accounting firm.

Why is there so much activity in the profession?
My contention is that there is pressure for change being generated externally -- from the client base.
What are the pressure? Quite simply the clients require an expanding range of services in all areas as well as in computer related matters at the same time as they are becoming more hostile to the traditional methods of delivering those services. Much of this pressure, I believe, results from a changing client profile. The key factors in the client profile of 1987 are: 95% will be using computers; accounting applications will be even more complex and be totally integrated with business functions; there will be less reliance on people in performing routine tasks -- and more on systems; there will be greater concentration of information and control; and they will require more services than audit.

Finally, the client environment will become increasingly hostile for us to work in effectively and deliver efficient client services.
What are the reasons? There will be even more cost pressure for efficient services.
The clients and the profession will experience difficulty in keeping pace with escalating technological change.
We currently lack the proper tools to deal efficiently with sophisticated client environments.
There will be a shortage of properly trained personnel at all levels.
Controls and accounting procedures will migrate from people to computer functions.

There will be a reduction in physical audit evidence.
Clients, particularly those personnel usually involved in the audit will have limited knowledge of their EDP systems.
And finally clients expectations for more business advisory and technical support services. By way of example -- A recent survey of clients in the United States has pointed out the need to provide a more comprehensive range of services to our clients. The Conference Board Study in the U.S.A. found that the major reason (25% of the total) that companies changed auditors in the preceeding ten year period was because more services were needed than their incumbent auditor could provide.

The message behind this trend is quite simple -- if we are unable to provide the services our clients demand, our competition certainly will.
The first option is to ignore the changing opportunities and challenges. We can hope for the best and muddle through trying to retain our clients and staff - after all it might all go away - these computer predictions have been wrong before. Well, enough of that ostrich approach, the trends cannot be dismissed and we ignore the issue at our own peril.
We can choose to let others do the pioneering, take the risks and make the mistakes first, and we can follow at a safe distance. This is a better option but presents some downside risk -- clients may go elsewhere as they begin to lead us in too many areas of the emerging technology.
We could choose to lead -- to go first and be on the leading edge of change - but like the cutting edge of a sword, it sometimes gets bloody - costs can be high as well as the risk of failure from moving too soon.
I believe the best approach is to choose our opportunities. Choices would be based on factors such as the needs of our practice as the client base adjusts to the changes and the capacity of staff to absorb new approaches and procedures.

Within KMG, we have the choice of dealing with many problems individually or joining our respective strengths to develop better solutions together. There is a strength in the diversity of our individual practices and we have a unique opportunity to build on that strength to deal with a universal problem - because computers after all recognize no geographic boundaries - so that the scenario involving Mr. Gee (see part I) which for the present is a fantasy will become a reality by 1987.
However, before we reach 1987, there are a number of issues, in the form of rhetorical questions that need to be addressed in order to plan our approach to the impact of this technological change.

THE KEY QUESTION

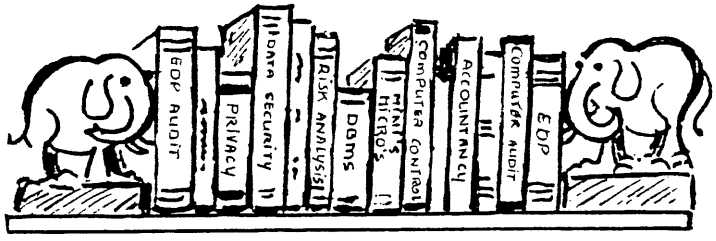
What ACTIONS will you take to deal with the coming CHANGES in YOUR PRACTICE caused by COMPUTER TECHNOLOGY?

What is the impact of computer technology on

1. The selection, training and professional status of staff.
2. The use of professional judgement in the audit engagement.
3. The level of (EDP) technical knowledge on the audit team.
4. Partner professional development (transitional training).
5. Practice profitability.
6. Job satisfaction and staff retention.
7. The range of client services that need to be provided.
8. Your competitive position.
9. Audit standards and procedures.
10. The role and responsibility of the engagement partner.

It is an exhilarating opportunity. Let's work for it and keep one step ahead so that we can face 1987 with the confidence that we are the best.

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



Boeken

Boekbespreking door H. Teeuwisse (A.C.-parttimer),
aangevuld met kritische kanttekeningen van C.J.M. Kramer
(senior Org.adviseur)

Titel: Ondernemingsraad en automatisering
Serie: OR-praktijk
Auteurs: Rien van Lent
Jan de Vries
Uitgave: Samsom uitgeverij - 1982
Aantal pagina's: 60
Bibliotheeknummer: 342-LEN-1

Doelstelling van de schrijvers met dit - eenvoudig leesbare - boekje is om aan ondernemingsraadsleden, welke veelal specifieke automatiseringskennis ontberen, duidelijk te maken op welke wijze een ondernemingsraad invloed kan uitoefenen op het automatiserings-proces in een organisatie.
Dit omdat ondernemingsraden in toenemende mate worden geconfron-teerd met automatisering en de gevolgen daarvan.

Hiertoe is het boekje onderverdeeld in de volgende 6 hoofdstukken:
1. Inleiding.
2. Automatisering - een manier van denken.
3. Hoe wordt geautomatiseerd.
4. Problemen voor de ondernemingsraad.
5. Aangrijpingspunten voor een strategie.
6. Planning van werknemersinvloed.

Door, in de hoofdstukken 2 en 3, de lezer vertrouwd te maken met principes en denkprocessen, welke aan automatisering ten grondslag liggen en te stellen dat automatiseringsbeslissingen veelal tot stand komen vanuit een financieel-economische denkwereld waarin te weinig rekening wordt gehouden met sociale facetten, wordt de noodzaak tot actieve participatie van werknemers en ondernemings-raadsleden in automatiseringsplannen duidelijk gemaakt.

Dit te meer waar automatisering (in dit boekje) wordt gezien als een in zijn uiterste consequenties doorzetten van een streven naar beheersing en regeling van de werkende mens door de machine.

Vervolgens (hoofdstuk 4) wordt opgesomd welke praktische problemen een actieve participatie belemmeren (OR-leden hebben een chronisch tekort aan beschikbare tijd, OR-leden missen specifieke automatiseringskennis, OR-leden krijgen vaak onvolledige informatie) en hoe deze te ondervangen zijn.

Met deze uitgangspunten alsmede met het uitgangspunt dat het niet de bedoeling van een ondernemingsraad mag zijn om automatisering tegen te houden maar haar bedoeling moet zijn om automatisering zo toe te passen dat verbeteringen in werk en werksituatie ontstaan, wordt een aanzet gegeven een ondernemingsraad een overlegstrategie te laten ontwikkelen met betrekking tot automatisering, met als aangrijpingspunten die welke in de wet gegeven zijn (W.O.R. art. 25 en 27; ARBO-wet).

Deze strategie is dan eerder een achteraf kritische aanpak dan een vooraf participatieve. Het management (waartoe ook de automatiseringsdeskundigen worden gerekend) doet voorstellen, de OR toetst die vooral op de sociale facetten.

Hoe men ook moge denken over de ruime uitleg van wettelijke bepalingen, in ieder geval moet worden gewaarschuwd voor vertragingen die door de voorgestelde zware overlegstructuur kunnen optreden. Met name een hernieuwd overleg voorafgaand aan invoering van een reeds voltooid systeem lijkt overbodig als het overleg over de probleemoplossing en de wijze van aanpak toereikend is geweest en geen afwijkingen van betekenis aan de OR zijn te melden. Bovendien wordt het nog meer tijdrovend als de zaken niet naar de zin van de OR zijn uitgewerkt.

Conclusie is dat dit boekje aan de categorie personen voor wie het bedoeld is de noodzaak tot actieve participatie in een vroeg stadium van de automatiseringsplannen duidelijk maakt en aangeeft welke wettelijke aangrijpingspunten er voorhanden zijn om deze participatie "af te dwingen".
Er blijven echter vragen bestaan over het niveau van automatiseringskennis dat bij de OR-leden aanwezig zal moeten zijn om deelname aan automatiseringsbeslissingen en toetsing van automatiseringsplannen aan eigen criteria zinvol te doen zijn. Schrijvers gaan niet verder dan de noodzaak tot scholing (door wie?, waarin?) aan te geven en de mogelijkheid van het aantrekken van externe deskundigen (hierbij werd de vakbond genoemd) te beklemtonen.
Over de rol die accountants hierin ten opzichte van de OR zouden kunnen spelen wordt niet gesproken, zoals evenmin op de laatst gehouden accountantsdag is gebeurd.

compact

Zomer 1983

Voor adviseurs, wier opdracht thans dikwijls ter beoordeling en goedkeuring aan de OR wordt voorgelegd, is het nuttig en wellicht leerzaam dit boekje te lezen. Al zou het alleen maar zijn om te weten hoe de OR (middels dit boekje) is voorgelicht.
Ook voor de "gewone gebruiker" bevat dit geschrift vele handvaten voor zijn mogelijke, tijdige participatie binnen een automatiseringsproces.

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

Zomer 1983

TIJDSCHRIFTEN

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

JURIDISCHE BESCHERMING SOFTWARE IN HET BUITENLAND

In aansluiting op het onderwerp "Bescherming software tegen ongeautoriseerd copiëren" dat aan de orde is geweest in nummer 29 van Compact, zijn de volgende artikelen voor u gelezen:

- Legal protection of software
  Gerard F. Dunne
  Datamation, September 1982.
- Software-copyright: Schaltwerkgeometrie schutzwürdig, Datenschutz-Berater, november 1982.
- Software-Patentverletzung in USA
  Datenschutz-Berater, November 1982.
- Legal Protection of Computer Graphics Software
  Warren G. Lavey
  IEEE, January/February 1983.
- Program purploiners doubly deterred
  Roger M. Milgrim
  Datamation, March 1983.
- Software van Basis in de fout (Kop aangepast. red.)
  Databus, mei 1983.

Zoals in het voornoemd nummer van Compact duidelijk is geworden, is de wetgeving nationaal en internationaal niet toereikend om ongeautoriseerd gebruik van software tegen te gaan.
Niettegenstaande dit feit zijn op dit moment een aantal gerechtelijke procedures bekend, waarmee wordt/is getracht dit ongeautoriseerde gebruik te bestraffen:

- Door het gerechtshof van Santa Clara (Californië) is de president van Semiconductor Systems International Inc. veroordeeld tot zes jaar gevangenisstraf wegens diefstal van banden met gegevens, die het geometrisch ontwerp van geïntegreerde schakelingen beschrijven.
- Boole & Babbage, een van de leidende software-bedrijven in de U.S.A., heeft Candle Corporation aangeklaagd bij de districtsrechtbank van Los Angeles wegens schending van eigendomsrechten van computer software (uitspraak is nog niet bekend).
- Uitspraak door een districtsrechtbank in Amerika inzake Data Cash Systems, Inc. versus JS&A Group, Inc.:
  Programma's vastgelegd in de vorm van flow-charts, source- en object listings kunnen worden beschermd door middel van het copyright-notice. Dit is echter niet het geval met de objectcode, welke is vastgelegd in een ROM (Read Only Memory).
  Een ROM wordt beschouwd als een mechanisch hulpmiddel, dat deel uitmaakt van de computer en als zodanig niet onder de bescherming kan vallen van een copyright-notice.

Deze uitspraak gaat in tegen de geest van het beleid van de Copyright Office, dat is gericht op het doen hebben van een zo groot mogelijk toepassingsgebied van bescherming middels copyright. Voorts is deze uitspraak in strijd met die van een andere districtsrechtbank inzake Tandy Corp. versus Personal Micro Computers, Inc. Volgens deze laatste uitspraak kunnen de gegevens, vastgelegd in ROM-chips, wel worden beschermd door middel van copyright.

Op dit moment bestaan in Amerika drie vormen van juridische bescherming: copyright, trade-secrecy en patentrecht. Deze drie bieden afzonderlijk onvoldoende bescherming tegen het ongeautoriseerd gebruiken van software. De drie vormen trachten alle hetzelfde doel te bereiken nl. het beschermen van een idee. In Nederlandse verhoudingen vindt dit zijn uitwerking al naar gelang de internationale regelingen in auteursrecht (copyright), licentierecht (trade secrecy) en patentrecht.
Aangezien het wachten op een nieuw stuk wetgeving, welke aansluit bij de nieuwe technologische ontwikkeling, erg lang zal gaan duren, beveelt Roger M. Milgrim aan om copyright en trade-secrecy, in combinatie met elkaar te hanteren.
De voordelen van een dergelijke combinatie zijn niet onbelangrijk.
Het gebruik laten maken van software als een trade secret door middel van licentie-overeenkomsten en daarmee verbonden technieken, biedt bescherming van de innoverende ideeën en de uiterlijke verschijningsvorm ervan (bijvoorbeeld source-listings). Daar licentie-overeenkomsten slechts bepalingen bevatten welke betrekking hebben op de contracterende partijen zijn aanvullende maatregelen nodig. Hoewel copyright niet gericht is op de bescherming van het innovatie-concept, biedt het bescherming van de software tegen ongeautoriseerd copiëren door iedereen.
De verwachting bestaat dat in Amerika het gebruik maken van copyright en trade-secrecy samen een belangrijke stap op weg is naar de bescherming van software.
Vooral ook omdat het inbreuk maken op deze beschermingsmaatregelen bestraft kan worden met hoge geldboetes.

VALIDATION, VERIFICATION, AND TESTING OF COMPUTER SOFTWARE

W. Richards Adrion,
Division of Mathematical and Computer Sciences, National Science Foundation, Washington, D.C.20550

Martha A. Brandstad,
Institute for Computer Science and Technology, National Bureau of Standards, Washington, D.C.20234

John C. Cherniavsky
Division of Mathematical and Computer Sciences, National Science Foundation, Washington, D.C.20550

Bibliotheeknummer 0557, code C 30, C 31.
Aantal pagina's 30.
Gepubliceerd in Computing Surveys, Vol. 14. nr. 2 June 1982

Zomer 1983

Software quality is achieved through the application of development techniques and the use of verification procedures throughout the development process. Careful consideration of specific quality attributes and validation requirements leads to the selection of a balanced collection of review, analysis, and testing techniques for use throughout the life cycle. This paper surveys current verification, validation, and testing approaches and discusses their strengths, weaknesses, and life-cycle usage. In conjunction with these, the paper describes automated tools used to implement validation, verification, and testing. In the discussion of new research thrusts, emphasis is given to the continued need to develop a stronger theoretical basis for testing and the need to employ combinations of tools and techniques that may vary over each application.

Tot zover citaat.

In dit artikel wordt met name een overzicht gegeven van technieken, die gehanteerd kunnen worden bij het testen van programmatuur (in ontwikkeling).

Voordat een programma operationeel is, doorloopt het de volgende fasen:
- opstellen specificaties;
- ontwerp;
- constructie.

De behandelde technieken sluiten aan op deze fasering.
Hoewel het onderscheid tussen validation, verification en testing niet duidelijk wordt doorgetrokken naar de besproken technieken kan worden gesteld dat verification en validation meer omvat dan testing. Testing betreft het testen van programmatuur door middel van test-gegevens terwijl verification en validation alle testtechnieken kunnen omvatten.
Bij dit laatste kan worden gedacht aan desk-checking, simulatie en boundary value analysis.

Teneinde vast te stellen of in elke fase van de ontwikkelingscyclus op een toereikende wijze rekening is gehouden met de gebruikerseisen inzake te programmeren controles, aard van te produceren informatie, e.d. worden testtechnieken toegepast die worden gerubriceerd onder "verification".

"Validation" beoogt hetzelfde als "verification", echter in het kader van validation is het uiteindelijke programma, zoals het wordt over-gedragen naar de produktie-afdeling, object van testen.

De boodschap is dat er een groot aantal technieken van toetsen en testen bestaat om betrouwbaarheid, effectiviteit en efficiency te waarborgen bij iedere fase van de ontwikkeling van een systeem tot en met acceptatie.

Hoewel het artikel relatief weinig nieuws bevat voor de "kenners", wordt een vrij volledig overzicht gegeven van de middelen die zowel voor ontwikkelaars als voor gebruikers van programmatuur nuttig zijn, indien men te maken heeft met het testen van programmatuur in de ruimste zin van het woord.

THE AUDITOR'S ROLE IN PRE-IMPLEMENTATION REVIEWS

door: Noreen Foh, CA-magazine mei 1983

Het artikel geeft de visie van een extern accountant op de bijdrage die een accountant kan leveren in de systeemontwikkelingsfase.
Dit aspect van de accountantscontrole wordt in het algemeen door externe accountants zeer omzichtig benaderd. Meedoen in de ontwikkeling van een te automatiseren informatiesysteem betekent immers dat de accountant medeverantwoordelijkheid gaat dragen voor het eindprodukt.
Het gevolg van deze voorzichtige benadering is, dat het enorme reservoir aan theoretische en praktische kennis van automatisering van de accountant-EDP-auditor onvoldoende of te laat ten goede komt aan de cliënt.
Noreen Foh geeft in haar artikel op bondige wijze aan waar de accountant een waardevolle, objectieve bijdrage kan leveren. Samengevat:

- Toezien op en adviseren aangaande een georganiseerde aanpak van de ontwikkelingsfase.
- Erop toezien dat met het voorgestelde systeem een toereikende beheersing van het financieel-administratief gebeuren wordt bereikt.
- Nagaan of het geautomatiseerde systeem en de gebruikende organisatie op efficiënte en effectieve wijze worden geïntegreerd.
- Review van de conversieprocedures en het conversieplan.
- Review van de "environmental or integrity controls" die van invloed zijn op de ontwikkeling en programmering van de applicatie (richtlijnen, voorschriften en procedures met betrekking tot programmeren, hanteren van controletechnieken daarbij, etc.).
- Tenslotte de rapportering aan het management, waarin helder uiteengezet wordt welke risico's aanwezig (zullen) zijn in het nieuwe systeem en hoe de organisatie daarmee moet omgaan, in de zin van compenserende maatregelen.

Als vervolg op deze pre-implementation review kan de accountant een bewakende functie vervullen bij de test- en conversieprocedures om ten behoeve van het management erop toe te zien, dat de voorgenomen maatregelen van interne controle ook werkelijk in het systeem aanwezig zijn.

Het artikel vervolgt met een praktische uitwerking van de accountantswerkzaamheden voor bovengenoemde punten.

Conclusie

Het artikel vormt een nuttige bijdrage aan de discussie over de rol van de accountant in de systeemontwikkelingsfase; de taakverdeling tussen de interne en externe accountant zal - voor de situatie in Nederland - nadere beschouwing behoeven. Hiervoor geeft het artikel voldoende aanknopingspunten.

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

Zomer 1983

Automatisering Beveiliging Controle NIEUWS

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

Automatisering

SUBSIDIE VAN ƒ 20 MLN VOOR COMPUTERDIENSTEN

Onder bovenstaande kop werd in het Financieele Dagblad van 29 juni 1983 melding gemaakt van een subsidie die door de Minister van Economische Zaken voor 1983 beschikbaar is gesteld.

De subsidieregeling komt voort uit de voorstellen van een tripartite structuurcommissie onder leiding van prof.dr.ir. A.A.Th.M. van Trier om te komen tot een Actieplan Computer Services Industrie 1983-1985 (ACSI 85).

Kosten van projecten in de computerservicebranche die zich richten op het verkennen van nieuwe markten, het zich voorbereiden op de introductie van produkten in nieuwe markten, het bijscholen van personeel en het ontwikkelen van nieuwe produkten kunnen tot 40% worden gesubsidieerd.

Als produkten/markten waarvoor de subsidie is bedoeld, worden genoemd:
- software voor technisch wetenschappelijke toepassingen;
- computer aided design en computer aided manufacturing;
- netwerk software;
- computer aided instruction;
- software voor nieuwe communicatietechnieken;
- produktiviteitsverbeterende middelen, zoals software-generatoren;
- database software;
- software voor procesautomatisering.

Bij de beoordeling van de commerciële waarde en haalbaarheid van ingediende projecten zullen deskundigen van de Rijkskantoormachinecentrale (ressorterende onder de PTT) medewerking verlenen.

HET GEAUTOMATISEERDE "NEDERLANDSE FAILLISSEMENTSREGISTER"

In Computable van 6 mei 1983 werd de nodige aandacht aan dit register besteed. Het register wordt door het bedrijf Dongelmans Business Service te Den Haag met behulp van een IBM Systeem/38 gevoerd. Op verschillende manieren kan men de in het register opgeslagen gegevens van het bedrijf afnemen.

In het register worden de personen opgenomen die de afgelopen vijf jaar direct of indirect bij een faillissement betrokken waren. Dit zijn er 90.000. (Op het ogenblik zijn er al 25.000 opgenomen.)

Als voordeel van dit nieuwe register op de bestaande registers bij de Griffies van Rechtbanken, Kamers van Koophandel, Ministerie van Justitie en andere wordt aangevoerd het compleet zijn en het op meerdere wijzen toegankelijk zijn.

Dat er behoefte bestaat aan dergelijke registers blijkt wel uit de in het artikel genoemde cijfers. Tussen 1 januari 1978 en 15 maart 1983 waren 90.000 personen betrokken bij een faillissement. Van dit aantal zijn er 15.000 meerdere keren bij een faillissement betrokken. Uit een steekproef onder de recidivisten bleek, dat bij deze faillissementen gemiddeld 1,12 miljoen gulden verloren ging, terwijl het algemeen gemiddelde op *f* 276.000,-- ligt. Kennis over de bij een bedrijf betrokken personen kan dus zijn nut hebben.

Om de privacy van de gefailleerden te beschermen zal een raad van toezicht worden ingesteld die belast zal worden met controle op de opname van gegevens conform de wettelijke regelingen alsmede terzake van de tijdsduur van de opslag van de gegevens. Hieromtrent zijn geen definitieve besluiten genomen.

REPORT GENERATOR

Fusion 4/38 is designed to allow nontechnical IBM System/38 users to extract and produce professional quality reports from any data resident in their computer systems.
The menu-driven system can also perform mathematical calculations and custom document formatting and can be interfaced to output devices including laser printers and 198-column line printers.
At the heart of the 4/38 system is the vendor's data dictionary, which controls and provides access to any piece of information defined to the system in conjunction with the System/38's own data management functions. The dictionary also stores a standard heading for each data element, as well as its decimal alignment and its standard display format.

The product supports the full complement of System/38 security functions. Sensitive elements can be secured with password protection and filtered from the view of users not authorized for those data. The 4/38 system is fully interactive and table driven, so that it does not generate the overhead of source and object libraries or require compiles to be performed. Each report is formatted and presented one page at a time to the specified display device. A preview feature allows the user to verify the output format before executing a request, so that the report would not have to be rerun.
The 4/38 system costs $5,000 in single order quantities, with multiple copy licenses available. Fusion products international, Mill Valley, California.

Datamation, May 1983

Beveiliging

Een computer in het zuur ten gevolge van zure regen. Het is zuur!

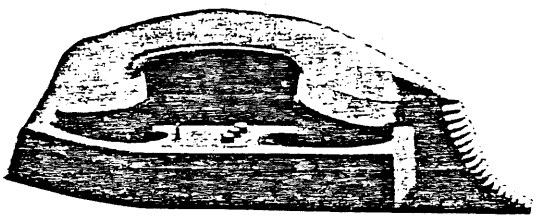
Saurer Regen: EDV kaputt

Die EDV-Anlage eines grossen Kreditinstitutes lief trotz neuer Klimaanlage, qualifizierter Stromversorgung und neuer Räume nicht störungsfrei. Immer wieder kam es zu Systemausfällen, die zu beseitigen einen hohen zeitlichen Aufwand zur Folge hatten. Diese Ausfälle führten dann so weit, dass man den Austausch der 10 Mio.-DM-Anlage ernsthaft erwog.
Um jedoch die Ursachen für die Ausfälle genau zu ermitteln, wurden Baugruppen aus der CPU, Rollenlager aus dem optischen Belegleser, Schreib-Lese-Köpfe aus dem Plattenlaufwerk, Spulmotoren aus den Bandgeräten und Hammermodule aus den Druckern ausgebaut und labormässig untersucht. Das Ergebnis: Sulfatablagerungen. Die Sulfate entstehen aus Schwefelverbindungen und verursachen in Verbindung mit Wasser oder hoher Luftfeuchtigkeit an unedlen oder halbedlen Metallteilen Korrosionen. Auf Edelmetallen, wie z. B. Gold- und Silberkontakten, wirken Sulfatablagerungen isolierend, verhindern also den gewünschten elektrischen Uebergang an den Kontakten.
Die Sulfatablagerungen konnten sich bilden, weil bei der neuen Klimaanlage ein Dimensionierungsfehler bestand. Die Gerätekühlluft führte eine Luftfeuchtigkeit von 70 bis 80% und überschritt damit die vom Hardwarehersteller zugelassenen Werte zwischen 40 und 65% bei weitem. Neben dem Dimensionierungsfehler stellten Fachleute, die die Untersuchungen führten, auch Konzeptionsfehler in der Regelung fest.
Der Schwachstromversicherer, der die Untersuchungen führte (TELA-Versicherung, München) veranlasste daraufhin dasz eine Aenderung der Regelanlage, und zwar dasz die Regelanlage der Klimatechnik auf Zuluftregelung anstelle der vorher vorhandenen Raumregelung umgerüstet wurde. Die Zuluftmenge wurde durch Umbauten an der Klimaanlage vergrossert und ein Gasabsorbtionsfilter in die Frischluftansaugung der Klimaanlage zur Ausfilterung der Schwefelverbindungen eingebaut. Denn die Untersuchung hatte ergeben, dass die Sulfatablagerungen an der Anlage durch "saure Frischluft", den berühmten sauren Regen, verursacht wurden.
Im Rahmen der Schadensregulierung hat der Versicherer für über DM 500.000,- das gesamte Objekt saniert. Da die Anlage während der Woche in Betrieb sein musste, konnten die Sanierer nur während des Wochenendes die Hardware an Ort und Stelle stückweise zerlegen, reinigen, wieder zusammenbauen und austesten. Aggregat für Aggregat wurde dies an den Wochenenden erledigt, so dass am Wochenanfang die Anlage weitergefahren werden konnte. Insgesamt dauerten die Sanierungsarbeiten mehrerer Monate.

Bronvermelding: Datenschutz-Berater 8/83.

Zomer 1983

,HET WAS ZO SPANNEND EN HELEMAAL NIET MOEILIJK, ALS JE MAAR GEDULD HEBT'



Kinderen breken bij kernwapencomputer in

Van onze correspondent
JAN VAN WIERINGEN

NEW YORK — „Het was doodsimpel," zeggen de tien nieuwsgierige „computer-kinderen" uit Milwaukee die op het ogenblik door de FBI worden verhoord in verband met hun telefonische inbraak bij de computer van het supergeheime kernwapenlaboratorium Los Alamos National Laboratory in New Mexico.

„We deden het alleen omdat het zo spannend was en het is helemaal niet moeilijk. Als je maar iets van computers weet, nieuwsgierig bent en geduld hebt, kun je makkelijk tot het geheugen van computers doordringen. Je denkt er niet bij na dat je een misdaad hebt gepleegd tot de politie voor je deur staat."

Volgens de FBI is de inbraak in de computer van Los Alamos in juni ontdekt. De schoolkinderen zouden „geen permanente schade" hebben aangericht. De veiligheidscode van de betrokken computer is inmiddels veranderd — maar de publiciteit over het incident leidt in de Verenigde Staten tot een verdere discussie over een geheel nieuwe vorm van misdaad, inbraak bij computersystemen, het gemak waarmee iemand met een eenvoudige home-computer en een telefoon vanuit zijn slaapkamer bij grote computers in kan breken en de problemen om fraude of erger te voorkomen.

Volgens computerdeskundigen is het vrijwel onmogelijk om helemaal te voorkomen dat buitenstaanders doordringen tot een computer die op het telefoonnet is aangesloten. Nu de verkoop van zogenaamde „home-computers" zo'n geweldige vlucht neemt, wordt verwacht dat computer-diefstal en andere computer-fraude een steeds ernstiger probleem zal worden.

Onberekenaar

Sinds grote banken computers begonnen te gebruiken voor geld-transacties is het enkele malen voorgekomen dat aanzienlijke bedragen werden overgemaakt op rekeningen van mensen die geen geld tegoed hadden.

Inmiddels is er een geheel nieuwe en soms onberekenbare generatie computer-inbrekers opgekomen: jonge tot zeer jonge scholieren, die een verbluffend talent voor computertechniek en dus ook computer-misbruik blijken te bezitten.

Nu de Atari-computerspelletjes beginnen te vervelen brengen video-fabrikanten alsmaar nieuwe computerspelletjes op de markt (zeer veel succes heeft sinds een paar weken het voorgeprogrammeerde tekenfilmspel, waarbij ridders draken verslaan, dan wel door de draak worden opgegeten als de speler het spel niet slim speelt) — maar het is kennelijk spannender om thuis op je eigen computer te speuren naar de toegangscodes voor andermans computers. Dat blijkt erg simpel te zijn.

Benodigdheden: een computer-terminal en een „telephone hook-up" — een eenvoudig apparaat waar de hoorn van de telefoon in past, zodat instructies van de terminal thuis via de telefoonlijn naar een andere computer kunnen worden doorgegeven. De sleutel tot de meeste computersystemen bestaat uit een eenvoudig codewoord van zes letters, dat met enige fantasie vaak makkelijk te raden is en in de praktijk maar zelden wordt veranderd.

In de Verenigde Staten blijkt nu een netwerk van „computer-clubs" te bestaan met mensen die elkaar gegevens doorgeven over codewoorden van computersystemen. Met computers spelen is een rage bij jonge Amerikanen die op hun achtste of negende jaar met een Atari-spelletje beginnen en binnen opmerkelijk korte tijd beter met een computer overweg kunnen dan veel volwassenen. De leeftijd van de tien computer-inbrekers, die de FBI nu in Milwaukee onderzoekt, loopt van vijftien tot vijfentwintig jaar.

Ja en nee

„Jonge kinderen denken kennelijk nog anders dan volwassenen," zegt een computer-instructeur in New York, die probeert uit te vinden waarom jongeren soms zoveel sneller met een computer overweg kunnen dan volwassenen. „Zij denken misschien nog net als computers in ja en nee, en niet zoals volwassenen in termen als ‚misschien', die de computer niet begrijpt."

De schrijver van een bekende en veel gelezen krantenrubriek over videospelletjes, die in elf Amerikaanse dagbladen verschijnt, is een elf-jarig jongetje, Rawson Stovall. Het eerste boek over computers verschijnt het komende voorjaar bij uitgeverij Doubleday.

De griezelige gevolgen van computer-inbraak worden deze zomer uitvoerig vertoond in de actuele Hollywood-film „War Games", die onverwacht bijzonder veel succes heeft. In de film breekt een jonge video-expert eerst in op zijn school-computer om zijn rapportcijfers te verhogen, bestelt vervolgens gratis tickets voor een tocht naar Parijs via de computer van een reisbureau en stuit vervolgens al spelend op een merkwaardig computer-spel, dat onderdeel van de Pentagon-computer blijkt te zijn, die oorlogsscenario's bedenkt en „speelt".

Het is onwaarschijnlijk dat iemand er, zoals in de film, in zal slagen om door middel van een computer-inbraak bijna de Derde Wereldoorlog te ontketenen, maar nu „computer-kinderen" tot het geheugen van het zeer geheime Los Alamos kernwapenlaboratorium zijn doorgedrongen, rijst steeds meer de vraag wat geheime agenten eventueel via computers zouden kunnen bereiken.

de Volkskrant,
15 augustus 1983

compact

Zomer 1983

NOG GEEN INBRAAK PER TELEFOON IN NEDERLAND WEL FRAUDE,

„Computers worden slecht bewaakt"

Van onze verslaggever
HAN HANSEN

DEN HAAG — „In het algemeen zijn managers voor automatisering bij bedrijven en instellingen in Nederland zich onvoldoende bewust van inbraakrisico's voor hun computersystemen. Het gevolg is dat de beveiliging tegen bedreigingen van buitenaf zowel als van binnenuit niet goed is geregeld. Dat is voor een groot deel een kwestie van mentaliteit bij de bedrijfsleiding."

Deze conclusie trekken de computerexperts Neisingh en Roos, die als registeraccountant werken bij het bureau Klynveld Kraayenhof & Co en daarnaast deel uitmaken van het Nederlands Genootschap voor Informatica.

Om commentaar gevraagd op berichten uit de Verenigde Staten over de „telefonische inbraak" van een groep schoolkinderen in de computer van een supergeheim kernwapenlaboratorium, zeggen Neisingh en Roos: „Voorbeelden van dit soort trucs in Nederland zijn ons niet bekend. De risico's daarvan nemen wel razendsnel toe. Computercursussen zijn nog nooit zo populair geweest als nu en de verspreiding van huiscomputers is verbazingwekkend groot."

Telefonische inbraken van onbevoegde liefhebbers in computersystemen mogen dan nog zeldzaam zijn, misdadig misbruik van kennis doet zich wel degelijk voor. „Ons zijn gevallen bekend van ontslagen computerprogrammeurs, die dank zij hun wetenschap van de codes in de systemen van de voormalige werkgever telefonisch complete informatiebestanden lieten verdwijnen of zodanig saboteerden dat er enorme schade werd aangericht", aldus Neisingh en Roos, die deel uitmaken van een vijftigkoppige computerploeg bij het accountantskantoor.

„Er zijn ook voorbeelden van computerpersoneel dat tijdens nachtdiensten boekhoudklussen voor derden verricht. Of het incident van de expert bij een van de universiteiten, die zogeheten rekentijd van andere faculteiten in de computer benutte."

Neisingh is bestuurslid van de sectie beveiliging bij het Nederlands Genootschap voor Informatica. Hij wijst op de vaak gevaarlijke laksheid bij bedrijven en instellingen met een middelgrote computer. Die laksheid komt vooral voor bij kleinere verzekeringsmaatschappijen. De leverancier van een nieuwe installatie voorziet de klant van voorbeelden om de ingevoerde databestanden te beveiligen met codes. Het komt niet zelden voor dat eigenaars van computers de basiswachtwoorden voor toegang tot het systeem uit de instructieboekjes blijven hanteren.

Telefoonboek

Neisingh: „Het risico van inbraak wordt op die manier natuurlijk levensgroot. Zo gauw een systeemprogrammeur het bedrijf verlaat zouden de beveiligingscodes waarmee hij heeft gewerkt terstond gewijzigd moeten worden. Men kan niet voorzichtig genoeg zijn om computerfraude te voorkomen."

De twee accountants wijzen er op dat slechts een deel van het computerpark in Nederland per openbare telefoonverbinding bereikbaar is. De datacommunicatie kan in de praktijk beperkt blijven tot intern gebruik. Vaak ook wordt alleen gewerkt met vaste telefoonlijnen, die buiten de bedrijfscentrale om gaan en dus niet met een nummer in het telefoonboek staan. Dat gebeurt onder meer met het netwerk van bankinstellingen en hun bijkantoren.

In Amerika wordt door banken veel meer dan hier gebruik gemaakt van telefoon-terminals, zodat het risico van inbraak daar groter is. In Nederland zijn zulke incidenten wel eens voorgekomen, maar de bedrijven hingen dat niet aan de grote klok.

Gracht

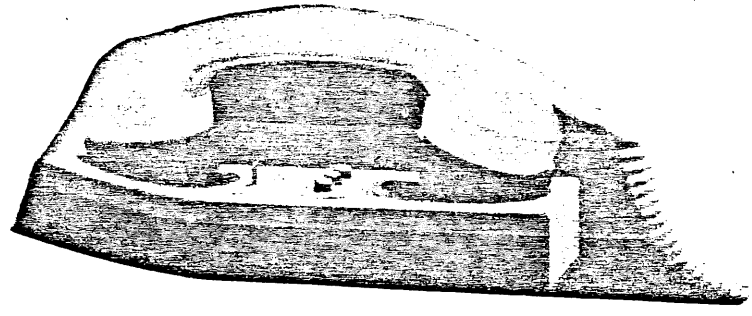
„Het simpele feit dat een accountant zijn handtekening zet onder de jaarcijfers wil nog niet zeggen dat de beveiliging van de geautomatiseerde systemen in dat bedrijf in orde zijn. En dan praten we niet eens over de fysieke bewaking, zoals de portiers en een fatsoenlijk slot op de deur of een gracht om het pand."

„Het komt voor dat een computersysteem van bereikbaarheid voor openbaar telefooncontact overschakelt op eigen verbindingen, waarbij wordt vergeten de lijnen voor vrije toegang van buiten af te koppelen. Bij grotere systemen is de techniek zover dat bij pogingen om via de telefoon een code te breken na drie of vier maal opbellen de systeembewaker automatisch een waarschuwing krijgt", leggen de deskundigen uit.

De sectie beveiliging van het genootschap voor informatica houdt zich bezig met risico-analyse bij het gebruik van computersystemen. Daar wordt in publikaties en op symposia over bericht. „Nu de computerkunde zich zo snel verdiept en verbreedt moeten de gebruikers en begeleiders zich navenant druk maken over misbruik en dus over noodzakelijke veiligheidsmaatregelen. De automatiseringstechniek leent zich nu eenmaal voor kwaadwillendheid. En dat gebeurt dan ook. Met een extra slot op de deur van het computerlokaal is men er niet. Het voorbeeld van de schoolkinderen in Amerika, die met een eenvoudige huiscomputer in grote systemen konden inbreken, bewijst hoe betrekkelijk naïef nog wordt gekeken naar mogelijke lekkages bij de beveiliging", waarschuwen Roos en Neisingh.

Kampen

De Stichting Logo, verbonden met de Universiteit van Nijmegen, heeft dit jaar voor het eerst een aantal „computerkampen" georganiseerd. Ze duurden een week en waren bestemd voor kinderen tussen tien en veertien jaar. Het spelenderwijs leren omgaan met de computer tijdens een zomerkamp was in de VS al eerder een groot succes. De berichten over de groep jonge „inbrekers" uit Milwaukee, die met de telefoon de computer van een atoomlab kraakten, vermelden niet of zij de kennis voor hun spelletjes hadden opgestoken op zo'n zomerkamp.



de Volkskrant,
16 augustus 1983

"Kinderen breken bij kernwapencomputer in" was de kop van een artikel in de Volkskrant van maandag 15 augustus jl. Dit artikel werd gevolgd door een interview met A.W. Neisingh en H. Roos, gepubliceerd in de Volkskrant van 16 augustus 1983. Hierna volgt een nabeschouwing op verzoek van de Redactie van Compact.

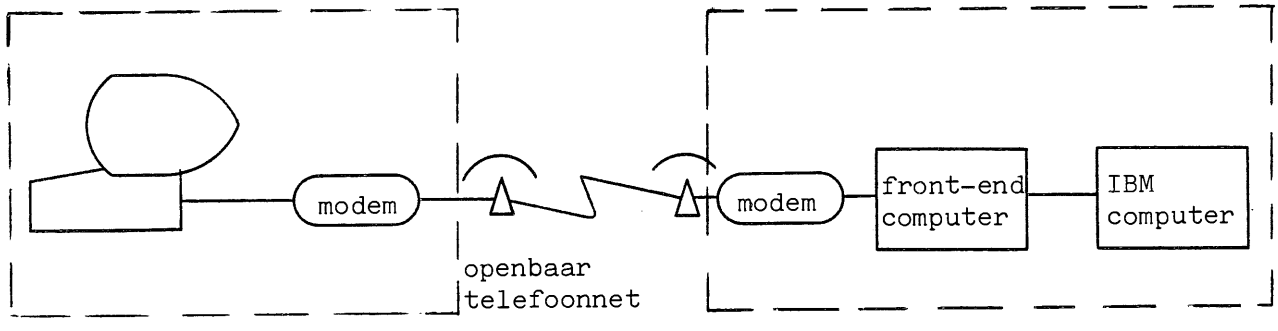
> "We deden het alleen omdat het zo spannend was en het is helemaal niet moeilijk. Als je maar iets van computers weet, nieuwsgierig bent en geduld hebt, kun je makkelijk tot het geheugen van computers doordringen.
>
> De veiligheidscode van de betrokken computer is inmiddels veranderd - maar de publiciteit over het incident leidt in de Verenigde Staten tot een verdere discussie over een geheel nieuwe vorm van misdaad, inbraak bij computersystemen, het gemak waarmee iemand met een eenvoudige home-computer en een telefoon vanuit zijn slaapkamer bij grote computers in kan breken en de problemen om fraude of erger te voorkomen."

Aan de hand van een aantal passages uit dit artikel wordt in deze rubriek een uiteenzetting gegeven over dit beveiligingsprobleem en waarom het zo eenvoudig is om in te breken in computers, afgezet tegen een VTAM-terminalnetwerk van een centrale IBM-computer.

Een eerste eis om met een centrale computer te kunnen communiceren is het beschikbaar hebben van apparatuur en programmatuur.

> "Dat blijkt erg simpel te zijn.
> Benodigdheden: een computerterminal en een "telephone hook-up" - een eenvoudig apparaat waar de hoorn van de telefoon in past, zodat instructies van de terminal thuis via de telefoonlijn naar een andere computer kunnen worden doorgegeven."

Het hierna volgende schema geeft de apparatuur weer, waarmee een verbinding tot stand kan worden gebracht.



Het identificatieproces waarmee een terminal en een terminalgebruiker zich bekend dienen te maken aan een centrale computer, is uit een aantal drempels samengesteld.

Een eerste drempel betreft het in de centrale computer actief zijn van een programma dat de lijnverbindingen onderhoudt. Bij de meeste centrale computers zijn deze programma's overdag en in de avonduren actief, zodat de centrale computer beschikbaar is voor terminals en terminalgebruikers, die het telefoonnummer weten waarmee een verbinding tot stand kan worden gebracht.

Een tweede drempel is opgenomen in het data-communicatieprotocol. In deze drempel kan worden voorzien dat de terminal zich met behulp van een hardware-identificatienummer bekend dient te maken aan de centrale computer. In tabellen van de centrale computer dient dit nummer vooraf door een systeemprogrammeur te zijn gespecificeerd. Aan de hand van dit vooraf gespecificeerde nummer en het hardware-identificatienummer waarmee een terminal, die in verbinding met de centrale computer wil komen, zich bekend dient te maken, kan een drempel voor toegangsbeveiliging worden gecreëerd.
In de praktijk blijkt dat deze elementaire drempel in veel gevallen niet wordt gehanteerd om reden van kostenbesparing. Door in de samenstelling van het netwerk gebruik te maken van goedkope apparatuur kan van deze drempel geen gebruik worden gemaakt. Home-computers maken gebruik van hetzelfde data-communicatieprotocol als de goedkope apparatuur.
Hierin bevindt zich de kern van het beveiligingsprobleem, indien voor het ontbreken van deze drempel geen compenserende maatregelen worden getroffen.

Een derde - en in veel gevallen de laatste drempel .... - in het identificatieproces betreft het bekend maken van de sessie of dienst die men met de centrale computer wil gaan uitvoeren. Hierbij dient in de meeste gevallen een codewoord te worden meegegeven.

> "De sleutel tot de meeste computersystemen bestaat uit een eenvoudig codewoord van zes letters, dat met enige fantasie vaak makkelijk te raden is en in de praktijk maar zelden wordt veranderd.
> In de Verenigde Staten blijkt nu een netwerk van "computerclubs" te bestaan met mensen die elkaar gegevens doorgeven over codewoorden van computersystemen."

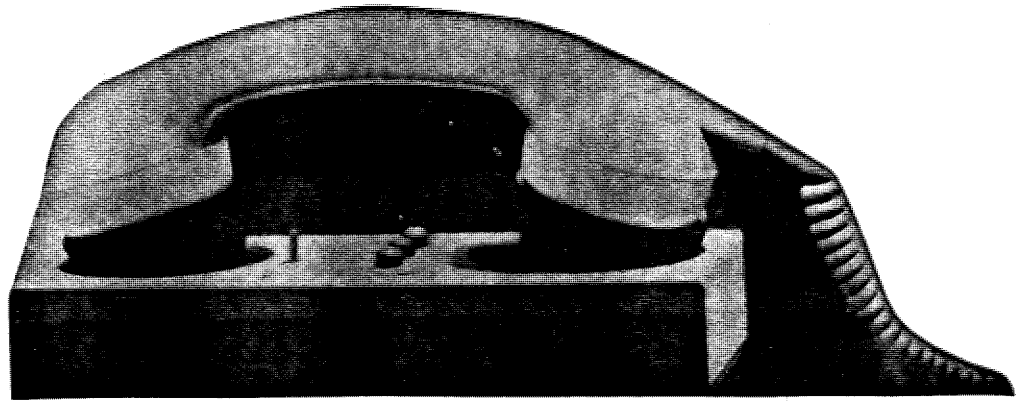
In de meeste computercentra worden codewoorden en (geheime) telefoonnummers veel te weinig gewisseld. Tevens zijn geen maatregelen getroffen gericht op het ontdekken van onregelmatigheden. Hierdoor bestaat geen inzicht of er één keer of tienduizend keer op een dag wordt getracht in te breken. Overigens wordt in Nederland voor data-communicatie geen omvangrijk gebruik gemaakt van gekozen verbindingen.

Samenvattend kan worden gesteld dat de hiervoor beschreven drempels niet of niet effectief worden gebruikt, waardoor het inderdaad kinderlijk eenvoudig wordt om tot centrale computers met behulp van home-computers door te dringen.

> "Nu de verkoop van zogenaamde "home-computers" zo'n geweldige vlucht neemt, wordt verwacht dat computerdiefstal en andere computerfraude een steeds ernstiger probleem zal worden."

In een aantal gevallen kan worden overwogen om tot vercijfering van het gegevenstransport over de lijnverbindingen en/of opgeslagen informatie over te gaan.

Omdat zelfs zeer goede apparatuur en programmatuur geen blijvende waterdichte barrière vormen voor een knappe en geduldige aspirant-indringer dient een bewuste afweging te worden uitgevoerd van kosten voor te treffen organisatorische en andere beveiligingsmaatregelen versus risico's. Daarna plan van actie.



Controle

In het Amerikaanse tijdschrift EDP JOURNAL (Uitg. E.D.P. Auditors Foundation), Summer 1983, troffen wij een artikel aan over een onderwerp waarover weinig wordt gepubliceerd. Reden voor ons om dit in verkorte vorm in onze rubriek op te nemen.

Ter verzekering van de continuïteit van de computerverwerking in een noodsituatie (volledig uitvallen van de eigen computerinstallatie) is het gebruikelijk op een andere locatie recente versies van de gegevens, de applicatieprogramma's inclusief de daarbij behorende JCL en de standaardprogrammatuur op te slaan. Tevens dient daar een registratie van de aanwezige bestanden, programma's, e.d. aanwezig te zijn. Teneinde zekerheid te hebben dat de kopieer- en externe opslagprocedures worden gehandhaafd en de kopieën geschikt zijn voor de off-site back-up dient hiernaar periodiek een onderzoek te worden ingesteld. Over de opzet, fasering en uitvoering van een volledige audit gaat dit artikel waarvan de titel is:

EDP AUDITING AND OFF-SITE STORAGE

Introduction

Most companies have some form of off-site storage facility for computer media and other vital records. Almost all companies conduct audits of their off-site storage facilities, which in most cases consist of physically counting and matching items expected to be in storage. Is this enough? There may be significant audit findings by delving a little deeper during your off-site storage reviews. Storing information off-site has been an accepted practice since the early days of data processing. A growing interest in contingency planning has inspired additional thought and discussion on the purpose of off-site storage. One of the steps in developing a disaster recovery plan is to identify critical applications and then review off-site backup. Consideration should then be given to running these systems in a contingency situation. This can lead to some interesting findings which will be highlighted later.

Phases of the off-site audit

The review of an off-site storage facility can be divided into four major areas:

a. test of compliance by conducting an inventory of the off-site facility;
b. test of efficiency by searching for unnecessary tapes;
c. test for physical security;
d. test of adequacy by application of a disaster scenario.

The first three are relatively straightforward and combine tests performed during most current audits of off-site facilities. The fourth involves an analysis of the critical systems within the organization, at least, and requires more time and expertise to complete. All tests are important for a complete audit, but each could be done separately to satisfy time or cost constraints.

Compliance

This is the standard inventory reconciliation process. In most cases a log will be kept at the main computer center listing the tapes stored off-site. This log is then matched to a physical count of the off-site storage contents. Frequently, if there is no discrepancy the audit is concluded.

Efficiency

Many off-site storage locations grow in "leaps and bounds". Specific retention rules should be established for all off-site media. With a little effort here, the audit could pay for itself. The old rule was "when in doubt, keep the data forever". Government and company retention standards should be re-examined and recommendations made to retrieve outdated tapes from off-site locations.
Data center configurations constantly change, and an attempt should be made to ensure off-site computer media remain compatible with current hardware and software requirements. File lay-outs may have changed substantially over the years and current programs may not be able to read old masterfiles. Why retain tape versions of outdated operating systems?
These and similar questions will surface as the contents of older tapes are examined.

Physical security

Your off-site location was chosen for various reasons (geographical location, transportation, cost, etc.). This part of the review reconfirms the selection criteria to be still valid, and evaluates the physical security of the off-site files. How is access restricted at the off-site facility? What security measures restrict unauthorized access to the facility? What types of security and fire alarm systems are in use, and are they tested? These are only a few of the important questions that should be asked and evaluated when looking at physical security.

Adequacy

This part of the audit asks, "Are the off-site backup files and data adequate to provide recovery in a contingency situation?" A disaster scenario can be developed to test the adequacy of the backup. The scenario should detail the magnitude of the damage, the date and time of destruction. This scenario might be a partial disaster, rendering only certain resources unavailable, but it would cover all possibilities if a total disaster scenario is designed. In order to restrict your review and findings to off-site storage contents, assume in your disaster scenario that computing power and space are readily available at an alternate site.
Using the disaster scenario as a guideline, assign critical systems to specific individuals involved in the audit.
Identify critical files within each assigned system, and determine whether these files are available at the off-site facility. Under the situation outlined in the disaster scenario, decide if you could go to off-site storage and run that particular application.
The next and most difficult step is to test (using your own installation or a contingency site if available) each application to see if operations could rerun a system from a specific point in time using only off-site data. More deficiencies may show up during this exercise.
The temptation when problems occur is to information readily available at the main computer center. These problems should be closely monitored and checked back to confirm existence at the off-site location.

Other considerations

Cycling procedures

It is important to examine delivery procedures to off-site storage when evaluating the disaster scenario for availability of files. If the disaster occurred on a Sunday, all the latest backups may still be at the main computer site if delivery to the off-site location isn't scheduled until Monday. The off-site files are not a generation of "minus-one" as would be expected, but at least "minus-two".
Problems can increase when year-to-date files accumulating statistic files are backed up and stored off-site only at month-end or year-end. Examine the reentry or rerun problems associated with losing these files with no recourse but the off-site files. With today's on-line networks and an implied need for immediate recovery, it would be impossible to perform all the necessary reruns to make the files current.

Recalled items

Procedures should be in place to ensure replacement of items prematurely recalled from off-site storage. It is not unusual to recall a specific file for additional processing requirements or current problem situations. Care should be taken to ensure this file is replaced, as it now represents the only version available with no recourse if it becomes accidentally damaged.

Additional off-site items

When reviewing the contents of off-site storage give some thought to additional items (beside tape volumes) that warrant backup. Operations documentation, policy and procedure manuals, forms and supplies, off-site premise inventory list, and program documentation may be essential when considering the disaster scenario outlined above. Development documentation and libraries should be backed up for contingency purposes.

Further storage and access considerations

If your off-site location is not a solely owned facility, several additional concerns arise. Where companies share a facility, it is advisable to have a secured room or individual vault for each firm.

Conclusion

A formal audit of an off-site storage facility can produce significant findings about an area of data processing usually taken for granted. Whether doing an audit on a scheduled basis or on demand, there are several areas requiring further analysis and investigation.
Usually the audit will be performed by data processing or internal audit personnel. Sometimes the function is performed jointly by data processing and internal audit, or internal audit and external audit personnel.
The final report should be forwarded to senior management for their consideration, regardless of who does the audit. Their understanding of the off-site function and its significance in today's environment is most important to ensure any deficiencies receive immediate corrective action.

CICA revising computer control and audit guidelines

A CICA study group is nearing the completion of the first phase of a complete revision of Computer Control Guidelines and Computer Audit Guidelines, the institute's all-time best-selling publications. (Since their publication in 1970 and 1975 they have sold over 120,000 copies worldwide in five language editions.) Although the basic advice given in those publications still stands, the context in which it was given

has changed considerably. "In the early '70s batch processing was predominant," says study group chairman Ruben J. Rosen, CA (who was also chairman of the study group that produced the earlier studies). "Since then the technology, the information systems environment and even auditing methods themselves have changed so much that the control and audit techniques described in the guidelines and the way they are applied are very different."

Not only will the revision take all the changes in technology, environment and control and audit into account, the focus of the studies will also shift somewhat.

"We're looking at all aspects of control and audit in today's information systems environment," says Rosen. "In the previous studies we concentrated on EDP control and audit in a computer environment. The current studies will be much more comprehensive."

All the changes mean a major rewrite of the two previous studies. The studies will again be published in two parts. The first, which is expected to be published later this year, will focus on the control aspects. "Much of the auditing material is still being developed" says Rosen, "so it is difficult to estimate a publication date for it." He notes, however, that the studies "are worth waiting for because the members of the study group - "a very impressive group" - have pooled their extensive knowledge and expertise to "provide the most up-to-date and comprehensive information available for auditors auditing in today's highly complex and sophisticated information environment."

Until the new studies are released, both Computer Control Guidelines and Computer Audit Guidelines continue to offer practical advice to auditors auditing in EDP environments. They are available from the CICA Order Department for $20 and $25 respectively, or for $40 for the set.

ONDERWIJS

Nieuwe ontwikkeling: Cursus Aanpak Systeembeoordeling

Inleiding

In Compact nummer 30 werd een artikel gepubliceerd met als titel "Beoordeling betrouwbaarheid van een geautomatiseerd systeem: een aanpak". Op basis van de in dat artikel beschreven methode wordt ten behoeve van het cursuspakket van Bureau Opleidingen thans door een team uit de A.C.-groep een uitgebreide cursus ontwikkeld, waarin de cursus Batchverwerking (blok II van de automatiseringscursus) zal worden geïntegreerd. De cursus zal sterk het karakter van een workshop krijgen en in totaal 8 dagen duren.
De cursus zal openstaan voor degenen die blok I van de automatiseringscursus, Computer Controls, hebben gevolgd.

De reden

Verwacht wordt, dat in de nabije toekomst door toenemende automatisering een verschuiving van systeembeoordelingswerkzaamheden naar buiten de A.C.-groep zal plaatsvinden. Hierdoor ontstaat de behoefte aan een daarop gerichte opleiding als vervolg op de basisvorming van de accountant. Van de zijde van de NIVRA-opleiding wordt in de komende jaren geen aanvulling op dit punt verwacht.

De filosofie

In de praktijk zijn de laatste jaren ideeën ontstaan ten aanzien van een methodische aanpak voor het in kaart brengen van het geautomatiseerde deel van een informatiesysteem. Hierbij is sprake van een functionele benadering.

In het kort (zie het vermelde artikel voor een uitgebreide behandeling) betreft de functionele benadering bij de beoordeling van een systeem: het redenerend vanuit gegevensaanleverende bedrijfsfuncties in logische bouwstenen in kaart brengen van het bedrijfsinformatiesysteem, daarmee aangevend welke bedrijfsfuncties verantwoordelijk zijn voor welke reken- en beslissingsregels alsmede master-gegevensverzamelingen.
Redenerend vanuit de bedrijfsfuncties wordt onderscheid gemaakt tussen relevante, minder relevante en (relatief) irrelevante functies in dit systeem en wordt bepaald naar welke functies met name moet worden gekeken. Voorts dient te worden bepaald in hoeverre specifieke managementinformatie in het onderzoek wordt betrokken.

Afdalend naar een informatiesysteem kunnen ook op dat niveau in de automatisering uit te oefenen systeemfuncties worden gedefinieerd. De geautomatiseerde werkelijkheid zal hierbij moeten aansluiten. Invalshoek bij het onderkennen van (geautomatiseerde) functies dient de beheersbaarheid en controleerbaarheid van bedrijfsfuncties te zijn. Voortbouwend op de functionele benadering worden geautomatiseerde functies onderkend op basis van in master-gegevensverzamelingen aanwezige gegevenssoorten en daarop betrekking hebbende gegevensstromen.

Duidelijk zichtbaar worden de "kritische momenten" aan de in- en uitgang van de systeemfuncties, die bepalend zijn voor de beheersbaarheid van het systeem. Deze kunnen gericht, met behulp van de APS-techniek (Administratieve Procedure Schema's), verder in kaart worden gebracht en in hun geheel worden beoordeeld uit de gezichtspunten van interne controle, beveiliging en continuïteit.

Deze benadering sluit goed aan op de Interne Controle Vragenlijsten, die eveneens een functionele opbouw kennen.

Uitgangspunten en doelstellingen

De cursisten worden in een zo reëel mogelijke praktijksituatie geplaatst om vervolgens het hele proces van beoordeling van met name een geautomatiseerd systeem door te maken (workshop). Deze praktijksituatie wordt gesimuleerd door middel van een grote casus.

De voornaamste moeilijkheid voor de beoordelaar is om op snelle en doeltreffende wijze het systeem hanteerbaar in kaart te brengen. De functionele benadering bij inventarisatie en vastlegging zal hierbij haar diensten bewijzen. Het belang van de toepassing van interview-techniek zal in de workshop tot uiting komen (rollen: de docenten treden afwisselend op als materiedeskundige gebruiker, systeemontwikkelaar, coach vanuit A.C.-kern).

Dit onderdeel van de cursus, dat bedoelt een oplossing te bieden voor het grootste in de praktijk gesignaleerde probleem, namelijk "understanding the system", zal een zwaar accent krijgen. Daarnaast zal ruime aandacht worden gegeven aan de wijze waarop vastlegging van het voor- en natraject (APS) worden betrokken in een overall-evaluatie van interne controle en beveiliging.
Het leerproces zal bij alle cursusonderdelen zoveel mogelijk plaatsvinden door middel van zelfwerkzaamheid.

Uiteindelijk dient de cursist:
- zich een oordeel te vormen over opzet en (aan de hand van output) het bestaan van maatregelen van interne controle en beveiliging in het casussysteem;
- eventuele leemtes aan te geven;
- gericht in de A.O. (voor- en natraject) te zoeken naar:
  - compenserende maatregelen (alsmede oordeel daarover);
  - handmatige/visuele follow-up van door het geautomatiseerde systeem geboden controlemogelijkheden;
- de invloed op controle-aanpak te formuleren;
- mogelijkheden te formuleren ten aanzien van controleprogrammatuur; ')
- de grenzen van zijn deskundigheid te kunnen herkennen.

') De opname van deze onderdelen in de cursus geschiedt door de integratie van de huidige cursus Batchverwerking.

Cursusschema

Het nieuwe blok II, de Cursus Aanpak Systeembeoordeling, wordt als volgt opgebouwd:

- Blok II.A: "Understanding the system" (3 dagen).
  Eindresultaat: een door de cursisten opgestelde globale, maar doelgerichte beschrijving van het geautomatiseerde systeem, waarin de te beheersen functies duidelijk tot uiting komen.

- Blok II.B: Evaluatie (2 dagen).
  Eindresultaat: oordeel over de betrouwbaarheid op basis van een confrontatie van het aangetroffen stelsel van maatregelen van interne controle met de per functie te stellen Interne Controle-eisen; de invloed van "algemene maatregelen" (in de automatiseringsorganisatie) wordt hierbij betrokken. Een organisatiebrief wordt opgesteld.

- Blok II.C: Werkprogramma (3 dagen).
  In dit onderdeel (dag 2 t/m 4 uit de huidige cursus Batchverwerking) wordt op basis van de bevindingen uit blok II.B een werkprogramma opgesteld en uitgevoerd. Het geheel wordt afgesloten met een praktijkdag over het gebruik van de computer in de accountantscontrole.

Beschikbaarheid

Na een try-out in november 1983 in het kader van de opleiding van A.C.-part-timers, zal de cursus in december voor de eerste keer worden gegeven voor de controlesector. Het is de bedoeling om vanaf 1984 de cursus op te nemen als blok II van de automatiseringsopleiding, vooralsnog alleen intern.

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