A C. Adm. Zaken
Dossier compleet

compact

COMPUTER EN ACCOUNTANT

UIT DE INHOUD:

Klynveld Kraayenhof & co
ACCOUNTANTS

KMG
Klynveld Main Goerdeler
Accountants-international

NUMMER 23 8E JAARGANG LENTE 1981

COMPUTER EN ACCOUNTANT

INHOUDSOPGAVE

NUMMER 23 8E JAARGANG LENTE 1981

VAN DE REDACTIE

In dit lentenummer komen drie belangrijke stromingen aan het licht die momenteel richting geven aan het AC-werk:

a. Continuïteit en risico-analyse
b. Kleine computersystemen
c. Het gebruik van de computer in de accountantscontrole.

Ook in de hedendaagse literatuur wordt ruime aandacht besteed aan de drie onderwerpen. In de keuze die onze rubrieksredacteuren voor U hebben gemaakt, komt dit eveneens tot uitdrukking. Voor de inhoud van dit lentenummer verwijzen wij naar de binnenzijde van het schutblad.

De redactie stelt gaarne ruimte in dit blad beschikbaar voor reacties op bovengenoemde bijdragen.

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

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

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

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

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

ACCOUNTANT - CONTINUITEIT - AUTOMATISERING EN RISICO-ANALYSE

door drs. H.C. Kocks

Inleiding

Het is de bedoeling met dit artikel de aandacht te vestigen op, en een discussie op gang te brengen inzake, het aspect risico-analyse met betrekking tot de automatisering en de accountant.

De accountant gaat bij het hanteren van de waarderingsgrondslagen voor de jaarrekening in principe uit van de continuïteitsveronderstelling (going concern), tenzij hem anders blijkt.
Dit continuïteitsbeginsel is als uitgangspunt voor dit artikel genomen. Via een uiteenzetting over de in 1977 verschenen meningsuiting "De inhoud van de accountantsverklaring bij de jaarrekening van ondernemingen met continuïteitsproblemen" en een weergave van de praktijk wordt op de risico's met betrekking tot de automatisering nader ingegaan. Vervolgens zal een uiteenzetting worden gegeven van een (algemeen toepasbare) methode om inzicht te verkrijgen hoe het is gesteld met de continuïteit van geautomatiseerde gegevensverwerking en informatieverstrekking voor zover deze van evident belang is voor de continuïteit van de ondernemingsactiviteiten.

1.0 Accountant en continuïteit

In de literatuur is relatief weinig te vinden over het onderwerp accountant en continuïteit. Enige discussie inzake dit onderwerp is voorafgegaan aan de verschijning van de definitieve "Meningsuiting" van het NIvRA in 1977, die als titel draagt: "De inhoud van de accountantsverklaring bij de jaarrekening van ondernemingen met continuïteitsproblemen". Op de discussie, voorafgaand aan de verschijning van de "Meningsuiting" wordt verder in deze paragraaf niet nader ingegaan. Die discussie wordt voor de strekking van dit artikel niet relevant geacht.

De publikatie wekt in eerste instantie - ook gezien de titel - de indruk dat het primair gaat om de inhoud van de accountantsverklaring, af te geven bij de jaarrekening van een onderneming die met dreigende discontinuïteit kampt. Bij nadere bestudering echter blijkt dat in feite de gehele problematiek inzake accountant en (dis)continuïteit in de publikatie ligt opgesloten. De drie (kern)begrippen waar het in de "Meningsuiting" om draait zijn: (dis)continuiteit, waarderingsgrondslagen en de (inhoud van de) accountantsverklaring.

Deze drie componenten hebben een zodanige relatie dat ze niet los van elkaar kunnen worden gezien en waarbij de (dis)continuïteitsfactor de meest bepalende is.
De toe te passen waarderingsgrondslagen in de jaarrekening worden bepaald door de situatie waarin de accountant de onderneming op het desbetreffende moment aantreft. De inhoud van de accountantsverklaring wordt bepaald door zowel de ondernemingssituatie als de toegepaste waarderingsgrondslagen (fig. 1).

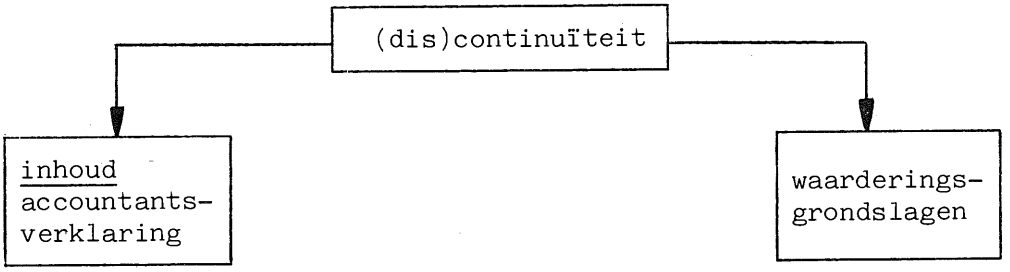


fig. 1: Relatie (dis)continuïteit, waarderingsgrondslagen en inhoud accountantsverklaring

Gezien het voorgaande blijft de vraag:
"Hoe bepaalt de accountant in welke situatie de onderneming verkeert",
met andere woorden:
wat is dreigende discontinuïteit en welke "tools" heeft de accountant om te beoordelen of zo'n situatie zich voordoet.

De "Meningsuiting" zegt hierover het volgende:
"In principe is de continuïteit van ondernemingen nooit geheel gewaarborgd. Onder normale omstandigheden echter wordt de jaarrekening van een onderneming opgesteld in de veronderstelling dat de onderneming voor onbepaalde tijd zal voortbestaan. Deze veronderstelling is voor de jaarrekening van betekenis omdat de toegepaste waarderingsgrondslagen hierop mede zijn gebaseerd. Als die continuïteitsveronderstelling niet langer gerechtvaardigd blijkt, zal naar andere grondslagen van waardering moeten worden omgezien".

"De continuïteit van een onderneming wordt bedreigd indien het gevaar bestaat dat de onderneming niet langer in staat zal zijn op eigen kracht de aangegane verplichtingen na te komen. Dit is een vraagstuk van liquiditeit, het is uiteindelijk het gebrek aan liquiditeit dat tot liquidatie dwingt. Zodra liquiditeitsproblemen opkomen moet men zich afvragen of bedoelde situatie is ingetreden. Er zijn velerlei signalen die op liquiditeitsproblemen duiden, te noemen zijn (onder vele andere):

- de onmogelijkheid te profiteren van betalingskorting;
- betaling van interest op schulden aan leveranciers;
- etc.."

Kort samengevat beantwoordt de Meningsuiting de vraag aldus:

- een situatie van dreigende discontinuïteit is ontstaan als de onderneming niet meer in staat is op eigen kracht haar financiële verplichtingen na te komen;
- om zo'n situatie vast te kunnen stellen hoeft de accountant zich alleen maar te richten op financiële informatie.

Niet ontkend kan worden dat meestal de financiële positie de graadmeter is die het reilen en zeilen van de onderneming aangeeft maar: "Mag het voor de toepassing van de waarderingsgrondslagen van de jaarrekening en voor de inhoud van de accountantsverklaring enig verschil uitmaken of de verplichtingen die de onderneming niet meer op eigen kracht kan nakomen (situatie dreigende discontinuïteit) van financiële of niet-financiële aard zijn?".

De Meningsuiting geeft hierop geen antwoord maar in principe kan en mag er geen verschil zijn. De accountant kan niet in alle gevallen de oorzaken van een dreigende discontinuïteit onderkennen door zich alleen te richten op de financiële positie van een onderneming.

Dit moge blijken uit het volgende:

- Een situatie, die gezien de financiële positie van de onderneming nog niet als een bedreiging voor de continuïteit kan worden beschouwd, kan in combinatie met niet-financiële factoren wel als een bedreiging voor de continuïteit worden aangemerkt, bijvoorbeeld: het niet meer of niet meer tijdig beschikbaar komen van betrouwbare management- en/of operationele informatie.
- Niet-financiële factoren, die tijdig onderkend dienen te worden, kunnen gevolgen voor de financiële positie van de onderneming hebben, welke niet direct hoeven te blijken uit de financiële positie van de onderneming zelf.
- Het nalaten van het nemen van maatregelen noodzakelijk om de continuïteit van het bedrijfsgebeuren onder normale omstandigheden te waarborgen.

Het zal de lezer duidelijk zijn dat met de geschetste situaties gedoeld wordt op de invalshoek "automatisering". Gezien de voortschrijdende automatisering wordt mijns inziens thans onvoldoende onderkend - ook in de accountantswereld - dat de continuïteit van het ondernemingsgebeuren steeds sterker afhankelijk wordt van de automatisering. De informatievoorziening binnen de onderneming zal in toenemende mate door de voortschrijdende automatisering geschieden. Aandacht zal derhalve moeten worden besteed aan de "continuïteit van de 'informatievoorziening' welke van vitaal belang kan zijn voor de continuïteit van de onderneming".

2.0 Accountant en automatisering

Zo weinig als er geschreven is over de accountant en continuïteit, zoveel is er gepubliceerd over de accountant en automatisering. In deze paragraaf zal niet uitgebreid worden ingegaan op hetgeen over dit onderwerp in de literatuur is verschenen. Het is voor de strekking van dit artikel minder relevant. In dit kader gaat het primair om de benadering van de automatiseringsproblematiek door de accountant in zijn functie als controleur van de jaarrekening.

Uit literatuuronderzoek en uit praktijkervaring komt de schrijver tot de conclusie dat globaal gesproken kan worden van drie benaderingswijzen.

I De accountant gaat systeemgericht te werk. Hij betrekt alleen die "geautomatiseerde delen" van informatiesystemen in zijn controle, die van belang zijn voor de controle van de jaarrekening. Dit houdt in dat de accountant zich in feite alleen richt op "financiële informatiesystemen" en op die informatiesystemen, die van betekenis kunnen zijn voor het vormen van een oordeel over de cijfers die in de jaarrekening worden getoond (bijvoorbeeld: uitkomsten van een materiaalbehoefteberekening voor de waardering van voorraden).

Indien de accountant, door zich te richten op de input/output-controle alsmede op de controles in het vóór- en natraject van het informatiesysteem, van oordeel is dat de geautomatiseerde gegevensverwerking betrouwbare informatie oplevert, laat hij de automatiseringsorganisatie verder buiten beschouwing.
Bij deze benadering richt de accountant zich op de volgende aspecten:

- zijn de ingevoerde gegevens juist, tijdig, volledig en geautoriseerd;
- is alle invoer juist en volledig verwerkt;
- blijven de gegevensverzamelingen volledig en juist;
- cijferbeoordeling en toetsing uitvoer.

De indruk bestaat bij de schrijver dat deze benaderingswijze, waarbij de automatiseringsorganisatie volledig buiten beschouwing blijft, in de praktijk veel voorkomt. De accountant richt zich in deze alleen op de betrouwbaarheidsaspecten (en wel in beperkte mate) en in het geheel niet op de continuïteitsaspecten van de automatisering. Zelfs is de aandacht niet gericht op de continuïteitsaspecten van de geautomatiseerde delen van die informatiesystemen die de accountant voor zijn jaarrekeningcontrole van belang acht.

II De automatiseringsorganisatie wordt betrokken in de controle van de jaarrekening, met dien verstande echter dat de werkzaamheden van de accountant zich blijven beperken tot de "betrouwbaarheidsaspecten" van de geautomatiseerde gegevensverwerking en -verstrekking van de voor de jaarrekeningcontrole relevante informatiesystemen (financiële systemen).
Deze benaderingswijze is een uitbreiding van die uiteengezet is onder punt I.

De accountant richt zich met betrekking tot de automatiseringsorganisatie op de volgende zaken:

- organisatorische plaats van de automatiseringsafdeling binnen het bedrijf;
- functiescheiding binnen de automatiseringsafdeling;
- algemene voorschriften met betrekking tot ontwikkeling en ingebruikneming van nieuwe c.q. gewijzigde systemen en programmatuur;
- documentatie van programmatuur en systemen;
- procedures en voorschriften met betrekking tot de betrouwbaarheid van de gegevensverwerking en -verstrekking.

Evenals bij benaderingswijze I staat bij II het betrouwbaarheidsaspect in het brandpunt. Door deze benaderingswijze krijgt de accountant evenmin inzicht in het feit hoe het is gesteld met de continuïteit van de geautomatiseerde gegevensverwerking en -verstrekking van de door zijn jaarrekeningcontrole van belang zijnde informatiesystemen. De overige informatiesystemen blijven wederom totaal buiten beschouwing.

III Bij deze benaderingswijze gaat de accountant nog een stap verder dan bij II en betrekt in zijn controle naast de betrouwbaarheid tevens de beveiligings- en continuïteitsaspecten van de geautomatiseerde gegevensverwerking en -verstrekking. Echter zij ten overvloede hier vermeld dat het alleen gaat om de voor de accountantscontrole relevante informatiesystemen.

Uitgaande van hetgeen in deze paragraaf is weergegeven kan worden geconcludeerd dat de accountant in het gunstigste geval (benaderingswijze III) zich een oordeel kan vormen omtrent de beveiliging en continuïteit van de geautomatiseerde gegevensverwerking en -verstrekking. Echter - nogmaals - alleen met betrekking tot die informatiesystemen die betrokken zijn in de jaarrekeningcontrole.

Ten aanzien van de overige geautomatiseerde informatiesystemen kan ervan uit worden gegaan dat de accountant:

1. de beveiligings- en continuïteitsaspecten laat voor wat ze zijn;
2. er impliciet vanuit gaat dat de overige geautomatiseerde informatiesystemen uit gezichtspunt van beveiliging en continuïteit géén hogere eisen stellen dan die hij in zijn onderzoek heeft betrokken. In deze wordt voorbijgegaan aan het feit dat de niet-financiële informatiesystemen hogere eisen kunnen stellen met betrekking tot beveiliging en continuïteit van de informatievoorziening en dat het nalaten van het nemen van maatregelen een bedreiging kunnen vormen voor de continuïteit van de onderneming als geheel.

Schrijver is van mening dat hetgeen onder punt 1 is weergegeven het meest met de werkelijkheid overeenkomt.

3.0 De accountant en risico-analyse

3.1 Risico-analyse, onderdeel van risk management

Uit de huidige literatuur komt risico-analyse naar voren als één van een drietal acitiviteiten die te zamen als risk management worden aangeduid.
Het eerste deel, het opstellen van een beginselprogramma ten aanzien van beveiliging, is een activiteit van de leiding. Naast het uitspreken van de noodzaak om acties te ondernemen om gevaren te onderkennen en daarop te reageren dienen hierin uitgangspunten en randvoorwaarden te worden opgenomen die als richtlijnen dienen voor de hierna uit te voeren risico-analyse. Bij de risico-analyse worden risico's geïnventariseerd, waarschijnlijkheden toegekend aan de gebeurtenissen, waaraan deze risico's zijn verbonden, en getracht de gevolgen te kwantificeren. Daarna wordt aangegeven welke maatregelen (preventief, schadebeperkend en schadeherstellend) moeten c.q. kunnen worden genomen om risico's en de gevolgen daarvan tot een aanvaardbaar niveau te reduceren, alsmede met welke kosten de maatregelen gepaard gaan. Deze informatie wordt - in de vorm van een concept-beveiligingsplan - aan de leiding gepresenteerd. Deze toetst het concept-beveiligingsplan aan de gegeven richtlijnen, neemt ten aanzien van de in het concept-beveiligingsplan opgenomen alternatieven de nodige beslissingen en geeft opdracht tot de derde activiteit: het uitvoeren van de acties om het beveiligingsplan te effectueren.
Uit het voorgaande komt naar onze mening duidelijk naar voren dat een goede risico-analyse de ruggegraat vormt van het risk management maar dat een daadwerkelijke inzet en ondersteuning van de leiding hierbij van essentiële betekenis moeten worden geacht (fig. 2).

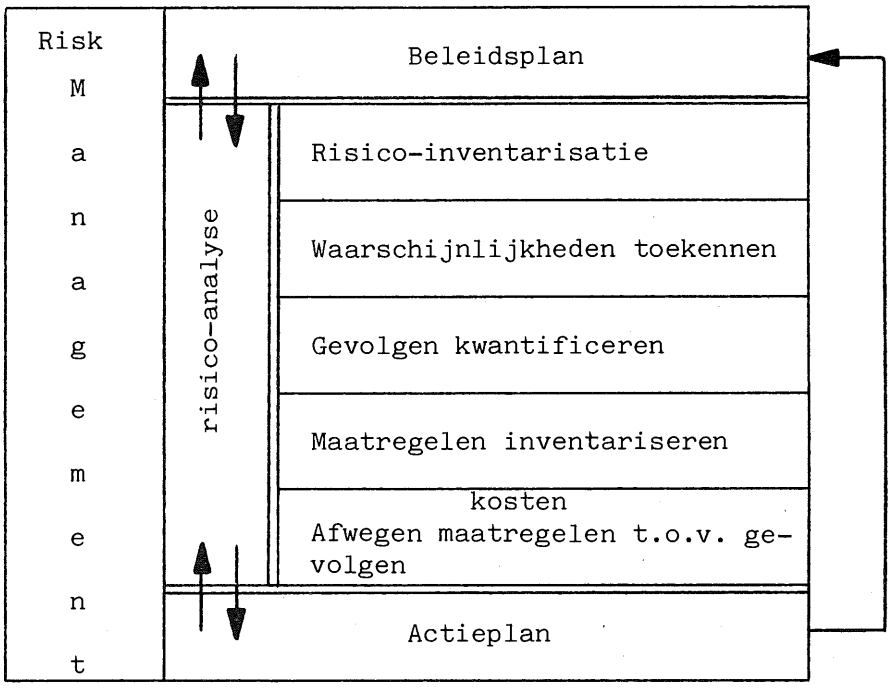


fig. 2: Risk management

Uit bovenstaande blijkt dat risico-analyse de aanduiding is van een techniek. In de volgende paragraaf wordt ingegaan op een aantal methoden die uit de literatuur blijken.

3.2 Methoden van risico-analyse

Bij de risico-analyse is de eerste stap - het inventariseren van de risico's - van grote betekenis. De wijze waarop dit gebeurt is bepalend voor de "volledigheid" van de risico's. Daarom lijkt het interessant na te gaan welke methoden hierbij gehanteerd worden. Uit de literatuur komen drie benaderingen naar voren:

1. Activabenadering (Assets approach)

   Hierbij worden de activa - zeer ruim geïnterpreteerd - geïnventariseerd, waarna per activum wordt bezien aan welke risico's het blootstaat. Het totale gebied kan worden onderverdeeld in deelgebieden ter verhoging van de eenvoud en doorzichtigheid van de werkzaamheden.

2. Gevarenbenadering (Threats approach)

   Vanuit een gedefinieerd geheel (situatie/afdeling) wordt aangegeven aan welke gevaren dat gebied blootstaat. Om uiteindelijk de schade (het verlies) te kunnen bepalen worden bij elk "gevaar" die activa gezocht die aan dat gevaar blootstaan. Deze benaderingwijze lijkt op de tegenpool van de activabenadering. De activabenadering gaat via de voordeur, de gevarenbenadering via de achterdeur en schijnbaar zal het resultaat hetzelfde zijn.

3. Systeembenadering (Systems approach)

   De gevaren en de risico's worden benaderd vanuit een beperkt aantal (dus niet alle) operationele toepassingen. Belanghebbenden bepalen welke toepassingen voor hun fungeren van betekenis zijn en aan welke gevaren en risico's die toepassingen blootgesteld zijn. In de literatuur komt tot uitdrukking dat deze benaderingswijze vooral wordt gehanteerd door interne en externe accountants. Deze benaderingswijze kan door haar beperkingen als boven omschreven niet als een complete risico-analysemethode (ter voorbereiding van een beveiligingsplan) worden beschouwd.

Of het resultaat van de activa- en gevarenbenadering inderdaad hetzelfde is, zal afhangen van de mate van zekerheid die er bestaat ten aanzien van de volledigheid van het basismateriaal.
Bij de activabenadering gaat men uit van concrete, aanwezige zaken; bij de gevarenbenadering daarentegen baseert men zich op "mogelijke" gebeurtenissen.
Het vaststellen van de volledigheid van de activa is zonder meer te realiseren; voor "mogelijke" gebeurtenissen ligt dit echter veel moeilijker en de kans van het onvolledig zijn is hierbij niet denkbeeldig.

Zoals onder de systeembenadering is weergegeven, hanteert de accountant deze benaderingswijze. Begrijpelijk, vanuit de optiek van de jaarrekeningcontrole beperkt hij zijn activiteiten tot de voor zijn jaarrekeningcontrole relevante informatiesystemen. Hier kan - evenals bij par. 2 - worden gesteld dat de accountant zich beperkt tot een deelwaarneming.

3.3 Beleid in de praktijk

Risk management kan betrekking hebben op de totale onderneming of op een deel ervan, bijvoorbeeld de automatisering. In het tweede geval is het noodzakelijk dat er overeenstemming bestaat tussen het totale en het deel risk management. In de praktijk komt risk management ook alleen voor met betrekking tot delen van de onderneming. Een parallel is hierbij te trekken met het automatiserings- en het totale ondernemersbeleid.
Welk beleid ook wordt neergelegd in een beleidsplan, het zal gericht moeten zijn op de continuering van de bedrijfsactiviteiten, tenzij anders is aangegeven (bijvoorbeeld statuten: "voor onbepaalde tijd"). Dit geldt eveneens voor de automatisering.

Bij nadere beschouwing van de argumenten inzake het waarom van risico-analyse in de praktijk kan worden geconstateerd dat deze in één zin zijn samen te vatten:

"Omdat er blijkbaar risico's kunnen zijn die moeten worden afgedekt!!".

De in par. 3.2 genoemde methoden gaan dan ook uit van twee elementen: risico's en maatregelen, hetgeen op zich een goede benadering is.
In de uitwerking van die maatregelen wordt aan het continuïteitsaspect echter te weinig aandacht geschonken. Om een evenwichtig pakket van maatregelen te krijgen is het nodig dat deze maatregelen worden gelegd tegen de continuïteitsdoelstelling.

De ondernemingsleidingen zijn zich er - evenals de accountants - onvoldoende van bewust dat in een normale situatie automatisering een bedreiging kan vormen voor de continuïteit van de ondernemingsactiviteiten als geen afdoende maatregelen zijn genomen om ongestoorde gegevensverwerking en informatieverstrekking te waarborgen. Automatisering is geen doel op zich maar een middel tot. Inmiddels een zodanig krachtig middel dat in toenemende mate de continuïteit van de onderneming ervan afhankelijk kan worden.

4.0 Conclusie

In par. 3.3 is gesteld dat zowel de ondernemingsleiding als de accountant zich onvoldoende bewust zijn van de risico's verbonden aan de automatisering. Een houding van "zo'n vaart zal het wel niet lopen" of "het valt niet binnen het kader van de opdracht" valt niet goed te keuren.

De accountant loopt de volgende risico's als hij zich niet op de hoogte stelt van de mate waarin zijn cliënt voor wat betreft de continuïteit van het bedrijfsgebeuren afhankelijk is van de automatisering, c.q. zich niet ervan heeft overtuigd dat adequate beveiligingsmaatregelen zijn genomen om de continuïteit van de geautomatiseerde gegevensverwerking en informatieverstrekking te waarborgen:

1. Dreigende (dis)continuïteit, die de accountant niet heeft onderkend, evenmin als de ondernemingsleiding, kan leiden tot verkeerde waarderingsgrondslagen en een onjuiste inhoud van de accountantsverklaring. De vraag of de accountant vrij uitgaat als zo'n situatie zich voordoet is niet eenvoudig te beantwoorden. De schrijver is de mening toegedaan van niet; de accountant had het kunnen vaststellen. Een beroep op ondeskundigheid in deze is buiten kijf omdat hij het in bepaalde gevallen wel doet (zie benaderingswijze III in par. 2). Wel is het de eerste verantwoordelijkheid van het management maar dat ontslaat de accountant niet van zijn verantwoordelijkheid in deze.

2. De accountant loopt steeds meer het risico dat hij verwachtingen wekt waaraan niet wordt voldaan. De ondernemingsleiding verwacht dat de accountant iets heeft gedaan terwijl die accountant zich daarvan niet bewust is. Die verwachtingen zijn volgens de schrijver geenszins irreëel. Want wat is de situatie. Als de accountant in het kader van de jaarrekeningcontrole aandacht besteedt aan de beveiligings- en continuïteitsaspecten van de voor zijn controle belangrijke financiële informatiesystemen, brengt hij de geconstateerde leemten onder de aandacht van het management. Echter daarbij niet expliciet aangevend dat het slechts om de voor zijn jaarrekeningcontrole belangrijke financiële systemen gaat. Het management neemt hierbij aan, dat indien de door de accountant geadviseerde te nemen maatregelen worden genomen, het met de beveiliging en continuïteit van de gegevensverwerking en -verstrekking in zijn totaliteit wel goed zit. Daarbij komt nog een versterkende invloed vanuit de literatuur. Accountants (edp-auditors) houden zich nogal bezig met beveiligingsaspecten inzake de automatisering. Hiermede de indruk wekkend en de verwachtingen versterkend dat dit terrein "des accountants" is. Schrijver wil bij deze een waarschuwende vinger opsteken dat de accountantsprofessie zich van deze verwachtingen bewust blijft dan wel wordt.

De accountant zal, als hij die risico's niet wil lopen, het volgende kunnen doen:

Ten aanzien van punt 1.: Zich ook te richten op de niet-financiële factoren die de continuïteit van een onderneming kunnen bedreigen of zich er expliciet van te distantiëren.

Ten aanzien van punt 2.: In zijn rapportage uitdrukkelijk vermelden op welk deelgebied van de automatisering zijn adviezen zijn gericht en elke schijn vermijden die het tegendeel doen vermoeden.

In het volgende Compact-nummer wordt een methode uiteengezet om vast te stellen in welke mate de continuïteit van de ondernemingsactiviteiten afhankelijk is van de automatisering, en of de genomen maatregelen voldoende zijn om de continuïteit van de geautomatiseerde gegevensverwerking en informatievoorziening te waarborgen.

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

BEOORDELING OPERATIONELE SYSTEMEN

door A. Kamstra

I Inleiding

De interne controle- en beveiligingseisen die gesteld moeten worden aan operationele systemen zijn uiteraard gelijk aan die van systemen in ontwikkeling. Wel komen bij de beoordeling van operationele systemen enige additionele aspecten naar voren ten opzichte van systemen in ontwikkeling. Op een aantal van deze bijzondere aspecten, die alleen bij de beoordeling van operationele systemen van betekenis zijn, wordt hier nader ingegaan').
Deze bijzondere aspecten zijn:

a. Juistheid van de documentatie.

b. Programmatuur in gebruik; programma's zijn veelal aanwezig in drie vormen, namelijk:
   1. source-programma's (door de programmeur geschreven),
   2. object-programma's (tussenvorm),
   3. load-programma's (uitvoerbaar programma).

c. Aanwezige procedures (waaronder instructies voor gebruikers en operators, job control).

Zaken van algemene aard, zoals de organisatie van het computercentrum, documentatievoorschriften, standaardprocedures, worden zoveel mogelijk buiten het kader van dit artikel gelaten.
Ten aanzien van een specifiek operationeel systeem dienen de werkzaamheden gericht te zijn op de beantwoording van de volgende vragen:

- Komt de documentatie overeen met de inhoud van de programma's?
- Zijn en worden de juiste programma's (de laatst geautoriseerde versie) gebruikt?
- Worden de voorschriften, vooral met betrekking tot de controle op de verwerking, goed nageleefd?

Op deze drie punten zal achtereenvolgens worden ingegaan.

II Komt de documentatie overeen met de inhoud van de programma's?

Uitgaande van redelijke of goede documentatie kan de confrontatie documentatie - programma's op een aantal manieren plaatsvinden, te weten:

a. direct, door vergelijking van de documentatie met de sourcelistings van de programma's;

b. indirect, door vergelijking van de (test)in- en uitvoer van het te beoordelen systeem;

c. simulatie van de verwerking, door gebruik te maken van eigen programmatuur.

') Voor een algemene beschouwing, zie het artikel van J.H. Urbanus en J.M. Verheul "EDP-Audit, Doelmatig instrument bij het beoordelen van de automatisering" (Handboek Accountancy).

Ad a.

Vergelijking van documentatie met source-listings van programma's moet bepaald niet als een normaal te gebruiken controletechniek worden beschouwd. In feite is dit alleen voor zeer kleine programma's een haalbare zaak. Programma's, ook in een hogere programmeertaal geschreven, bestaan snel uit enkele honderden regels en programma's van enige duizenden regels komen regelmatig voor. Hoewel gestructureerd programmeren en een zeer goede programmadocumentatie deze controlewerkzaamheden wel kunnen verlichten, blijft het nagenoeg onmogelijk om op deze wijze te controleren of de programma's een volledige weergave zijn van het in de documentatie beschreven systeem. De enkele keren dat wij binnen de A.C.-groep via deze wijze tot een oordeel moesten komen, betrof het altijd kleine systemen, drie of vier programma's waarvan de programma's niet groter waren dan ± 200 regels (in COBOL of CA/EARL geschreven), dan wel in het kader van de accountantscontrole kritische programma's. Aanvullend werd in die gevallen ook methode ad b. gebruikt.

Ad b.

De meest gebruikte methode om tot een oordeel te komen of het in de documentatie vastgelegde systeem wel in de programma's is weergegeven, is om enkele test- of produktieruns in detail te bekijken. Bij deze wijze van beoordelen dient vooral de vraag beantwoord te worden of de invoer test- of produktiegegevens wel voldoende representatief zijn. Hoewel theoretisch het aantal mogelijke invoergevallen veelal astronomisch hoog is, kan met enig "normgevoel" door de beoordelaar wel bepaald worden of per gebruiker voldoende normale, complexe en foute gevallen zijn ingevoerd. Door middel van het doornemen en controleren van de in- en uitvoer kan niet alleen een oordeel gevormd worden over de representativiteit van de invoer, maar kan tevens de juiste werking van de programmatuur worden geconstateerd.
Dit betekent zonder meer dat alles nagerekend moet worden en dat soms afdrukken van raadpleegbestanden (bijvoorbeeld tarieven, kortingspercentages van bepaalde cliënten, enz.) gemaakt dienen te worden.
Een geheel andere vraag die de beoordelaar moet stellen is, bevat de programmatuur niet meer dan in de documentatie is weergegeven. Gedeeltelijk kan dit ontdekt worden bij de beoordeling van de werking en representativiteit, bijvoorbeeld de invoergegevens worden anders verwerkt of de resultaten zijn anders en toch juist (bijvoorbeeld rekenregels staan goed in het programma en fout in de documentatie), echter alle mogelijkheden van de programmatuur worden niet aangetoond door uitvoering van een groot aantal test- of produktieposten. Het ontdekken van meer coding in de programmatuur kan alleen op een systematische wijze aangetoond worden door of methode II a. te gebruiken of door middel van bepaalde software (onder andere COMBI en COUNT-optie')).

') Zie Compact nr. 17, voorjaar 1979, artikel A. van der Drift.

COMBI en de COUNT-optie kunnen alleen gebruikt worden voor in COBOL geschreven programma's. Beide geven ze nagenoeg gelijke informatie. De inspanningen die verricht moeten worden om niet gebruikte coding te signaleren is voor de COUNT-optie wat geringer dan voor COMBI. In beide gevallen wordt per statement (instructie) aangegeven hoeveel maal deze tijdens uitvoering van het programma actief is geweest. Indien bij een statement "nul maal" staat dan betekent dit dat dit statement niet is gebruikt. De beoordelaar staat dan voor de taak om na te gaan wat de juiste functie van dat statement is. Soms is dat zeer simpel, echter veelal is dat niet zo eenvoudig en dient het programma "droog doorlopen" te worden. Voor een programmeur die het programma geschreven heeft of voor een programmeur die met het systeem bekend is, is dit wel een uitvoerbare taak. Echter voor een derde blijft dit een tijdrovende taak, zodat hiervan in de praktijk maar in uitzonderingsgevallen gebruik wordt gemaakt.

Een geheel ander middel kan zijn om gebruik te maken van ITF (Integrated Test Facility). Bij ITF worden testgevallen te zamen met actuele gegevens aangeboden aan de operationele systemen. De testgegevens worden derhalve in een produktie-omgeving verwerkt. De uitvoer wordt gescheiden van de normale uitvoer en gaat niet naar de gebruiker doch naar de accountant. ITF is geen middel dat achteraf gebruikt kan worden; bij de opzet van het systeem dient hiermee al rekening te worden gehouden. Van ITF wordt bij grote organisaties een enkele keer gebruik gemaakt.

Ad c.

Simulatie houdt in, dat een herhaalde verwerking plaatsvindt van de gegevensverwerking zoals die door het operationele systeem geschiedt. Doel hiervan is uitkomsten te verkrijgen die met de uitkomsten van het operationele systeem vergeleken kunnen worden. Audit en retrieval packages zijn hiervoor bijzonder geschikt, vooral omdat daarmee op eenvoudige wijze allerlei bewerkingen kunnen worden uitgevoerd, zoals selecteren, sorteren en berekenen. Bijna in iedere computertoepassing in de accountantscontrole vindt een vorm van simulatie plaats.

III Zijn of worden de juiste programma's gebruikt?

Zoals in de inleiding is weergegeven, is een programma meestal in drie vormen aanwezig. (Bij bepaalde computers kent men twee vormen, terwijl een retrieval-pakket veelal alleen één vorm kent.) De uitvoerbare vorm van het programma (load-programma) is niet het in de documentatie vastgelegde programma, dat is namelijk het door de programmeur geschreven source-programma.
Een "harde" reference trail tussen source- en load-programma's ontbreekt in praktisch alle gevallen. De software biedt daar (nog) niet direct de mogelijkheden toe. De beoordelaar dient te

steunen op organisatorische maatregelen en procedures. Aanvullend kan het gebruik van bepaalde programmabibliotheekpakketten hierop een versterking betekenen, te meer daar bij enkele pakketten sprake is van een automatische versienummering. De organisatorische maatregelen en procedures dienen van algemene aard te zijn en behoeven niet ten behoeve van iedere systeembeoordeling bij een cliënt bekeken te worden. Zaken die hierbij zonder meer van belang zijn:

- functiescheiding tussen produktie en ontwikkeling (ook tot uitdrukking komende in de beveiliging van het gebruik van programma-ontwikkelingspakketten);
- gescheiden produktie-, test- en programmabibliotheken;
- goede acceptatie- en wijzigingsprocedures.

IV Worden de voorschriften goed nageleefd?

Met deze procedures wordt hier bedoeld die handmatige procedures, die alleen gelden voor het te beoordelen systeem. Vooral van belang zijn hierbij de in- en uitvoercontroles. Enerzijds dient beoordeeld te worden of de procedures voldoende zijn, anderzijds dient getoetst te worden of deze procedures worden gehandhaafd en nageleefd.
Ten aanzien van het eerste punt kunnen deze zaken bij de opzet beoordeeld worden, echter de naleving kan pas na invoering van het systeem getoetst worden.
Toetsing op de naleving van procedures is voor een deel slechts met indirecte waarneming vast te stellen, echter het incidenteel niet naleven kan in vele gevallen niet worden geconstateerd.

V Slot

Het beoordelen van systemen vindt binnen de AC-groep zowel door parttimers als kernleden plaats. Voor een deel zijn de in dit artikel genoemde werkzaamheden alleen uit te voeren door meer technisch gespecialiseerde personen binnen de kerngroep. Genoemd kunnen worden het controleren van programma's en het gebruik van COMBI of de COUNT-optie.

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

DE INVOERING VAN DE SMALL BUSINESS COMPUTER EN DE INVLOED DAARVAN OP DE ACCOUNTANTSCONTROLE

door J.F.C. van Epen

1. Algemeen

De komst van de kleinere computer als opvolger van de boekhoudmachine en soms zelfs van de doorschrijfplaat is al een aantal jaren aan de gang. Talrijke shows en beurzen overtuigen geïnteresseerden van het nut en de "geweldige mogelijkheden" van de kleine computer. Ze zijn leverbaar in nagenoeg alle afmetingen en samenstellingen. Van heel klein (niet veel groter dan een rekenmachine) tot afmetingen die je bepaald niet over het hoofd ziet.
In dit artikel wil ik mij beperken tot de laatste categorie, al zal veel van het gestelde eveneens betrekking hebben op kleinere apparaten. Deze grotere "kleine computer" voor administratieve toepassingen wordt vaak aangeduid als Small Business Computer. Dit zijn computers waaraan een aantal randapparaten (beeldschermen, toetsenborden, afdrukeenheden) kunnen worden aangesloten. Zij zijn uitgerust met een besturingssysteem dat is aangepast aan administratieve taken. Hoewel er een heel scala van dit soort computers op de markt is, zal ik mij - voor zover een voorbeeld ter toelichting gewenst is - beperken tot het IBM-systeem/34.

Het IBM-systeem/34, kortweg aangeduid als S/34, bestaat uit een centrale verwerkingseenheid met ingebouwde magneetschijven voor de opslag van gegevens en programma's. Hieraan aangesloten is tenminste één beeldscherm met toetstenbord en een regeldrukker. De centrale verwerkingseenheid kan in grootte variëren tot maximaal 256 K (1 K = 1064 tekens intern geheugen). De schijfcapaciteit kan maximaal 256 Meg bedragen (1 Meg = 1.064.000 tekens). Aan randapparatuur kunnen maximaal 64 eenheden worden aangesloten. Deze eenheden (beeldschermen of regeldrukkers) kunnen ook op afstand worden geplaatst en via een telefoonlijn met het S/34 worden verbonden.
De bediening van de machine geschiedt vanaf een daartoe aangewezen beeldscherm, het console. De gegevensverwerking met behulp van de gebruikersprogrammatuur kan ook vanaf de overige beeldschermen plaatsvinden.

Ten gevolge van de overgang op geautomatiseerde gegevensverwerking worden naast de administratie als gebruikersafdeling ook het management en de accountant geconfronteerd met de problematiek van de betrouwbaarheid en de continuïteit van de informatieverstrekking.
Bij het analyseren van deze problematiek openbaren zich, in tegenstelling tot de eerder genoemde "geweldige mogelijkheden", de minder gewenste mogelijkheden en de onmogelijkheden van de computer en het besturingssysteem. Daarbij komt dan nog de organisatorische situatie waarin een small business system doorgaans wordt geplaatst, namelijk bij de gebruiker "op lokatie".
Een afzonderlijke afdeling voor de geautomatiseerde gegevensverwerking, met de daarmede samenhangende mogelijkheid tot functiescheiding, ontbreekt.
De automatiseringsdeskundigheid is binnen de gebruikersafdeling óf afwezig, óf geconcentreerd bij één persoon. Deze situatie is minder gewenst en leidt in de praktijk vaak tot moeilijkheden bij het

gebruik van de computer. Het management mag niet toestaan dat één of twee mensen binnen de organisatie alles kunnen terwijl de overigen er nauwelijks iets van begrijpen. IBM adviseert dan ook om een aantal functionarissen binnen de organisatie op te leiden voor automatiseringstaken, ook al zullen zij er geen dagtaak aan hebben. Voor het S/34 wordt naast de feitelijk bediener van de machine, de console operator, die de machine opstart, reageert op (fout)-boodschappen van het besturingssysteem en dergelijke, geadviseerd een systeembeheerder aan te stellen die het gebruik dat van de computer wordt gemaakt bewaakt en een security officer die tot taak heeft de bevoegdheden te regelen: wie mag wat en wanneer.

Voor de aanschaf en het onderhoud van de toepassingsprogrammatuur is men doorgaans aangewezen op door de computerleverancier aangeboden programmapakketten (IBM levert voor S/34 een aantal standaardpakketten), of op softwarehuizen die standaardprogrammatuur dan wel speciaal voor de gebruiker vervaardigde programma's kunnen leveren. Hierbij speelt het probleem dat een gebrek aan voldoende automatiseringsdeskundhigheid tevens inhoudt een gemis aan inzicht in de in zijn algemeenheid uit het gezichtspunt van interne controle aan de applicatieprogrammatuur te stellen eisen, alsmede in de toepassingsmogelijkheden van eventuele al dan niet expliciet voor dit doel in de programmatuur opgenomen faciliteiten.

Qua werkwijze zijn aan de ene kant de batchgewijze invoer in combinatie met de batchgewijze update van bestanden en aan de andere kant de transactiegewijze invoer gecombineerd met real time update te onderscheiden (ook wel post-voor-post-verwerking genoemd). Tussen deze beide uitersten is een aantal varianten mogelijk. Zowel de batch- als de transactiegewijze invoer geschiedt veelal middels de beeldschermen met toetsenborden, waarbij de gebruiker geheel of gedeeltelijk door de programmatuur kan worden geleid (keuzemenu's*, beeldscherm-maskerindeling met vragen waarop - correct - geantwoord moet worden en dergelijke). Hiermede samenhangend kunnen vaak toegangsbeveiligingen worden gerealiseerd die noodzakelijk zijn in verband met de eenvoudige fysieke toegang tot de op lokatie geplaatste apparatuur.
Zo biedt het S/34 de mogelijkheid het gebruik van een menu te koppelen aan een password, terwijl daarnaast de mogelijkheid bestaat per gebruiker of groep van gebruikers de programma's en bestanden in een afzonderlijke, middels een password beveiligde bibliotheek onder te brengen.
In de praktijk blijkt helaas dat van deze mogelijkheden maar weinig gebruik wordt gemaakt. In feite wordt dan een doorbreking van de bestaande functiescheiding toegestaan, vaak zonder dat men zich dat bewust is. De accountant dient zich dit wel te realiseren en moet voor zich de consequenties voor zijn controle bepalen.

---

* Een menu is een op het scherm verschijnend overzicht van applicaties, programma's of transactiesoorten, waaruit de (bevoegde) gebruiker een keuze mag maken. Het menu kan telkens weer door de gebruiker worden opgeroepen, ten einde een nieuwe keuze te doen.

2. Invloed op de aanpak van de accountantscontrole

Het is een gemeenplaats te stellen dat automatisering de doelstelling van de accountantscontrole niet beïnvloedt. Uiteraard is deze inherent aan de gegeven opdracht en betreft meestal de controle van de jaarrekening. Wat wel verandert is de wijze waarop de te controleren gegevens tot stand komen. Dit zou impliceren dat ook de wijze waarop de accountant zijn doel bereikt een andere zou dienen te zijn.
In een aantal gevallen blijkt echter de komst van de computer door de accountant te worden genegeerd. Hij blijft immers in staat om zijn controle geheel om de computer heen uit te voeren. Dit betekent wel dat hij synthetisch en grotendeels integraal zal dienen te controleren. Een voorwaarde hierbij is dat de computer de voor deze controle benodigde vastleggingen oplevert, zoals historische overzichten en details van cumulatieven.

Steunt de accountant voor zijn oordeel mede op de kwaliteit van de organisatie, dan dient hij zich te realiseren dat overgaan op automatisering wijzigingen in de organisatie met zich meebrengt. Handelingen die voorheen handmatig en voor een ieder waarneembaar plaatsvonden, worden nu door een machine volgens een eens ingegeven methodiek en niet meer waarneembaar uitgevoerd. Het gaat bij automatisering dan ook voornamelijk om die methodiek van verwerken van de gegevens die niet meer geobserveerd kan worden. Wat zich eveneens aan onze waarneming onttrekt is welke functionaris het verwerkingsproces heeft laten uitvoeren. En of het niet is uitgevoerd zonder dat de geproduceerde lijsten en overzichten zijn bewaard. Een andere wijziging in geautomatiseerde systemen ten opzichte van de handsystemen is het wegvallen van de "kaartenbak" met stambestanden. In een handsysteem is van elke afzonderlijke kaart het verloop en de laatste situatie zichtbaar af te lezen. In geautomatiseerde toepassingen is meestal alleen de laatste situatie in het systeem in niet direct leesbare vorm aanwezig. Wanneer en door wie de stamgegevens zijn gewijzigd is doorgaans niet vastgelegd.

Dit zijn problemen die opgevangen dienen te worden door de organisatie waarin de computer is of wordt geplaatst. De computer kan hierbij zelf behulpzaam zijn: gebruik kan worden gemaakt van speciale programma's en faciliteiten die de computerleverancier bij het apparaat levert. Zo voorziet het S/34 in een aantal mogelijkheden. Reeds eerder is melding gemaakt van de mogelijkheid een bepaald keuzemenu te koppelen aan een password. Ieder die het password niet kent kan het keuzemenu niet op zijn beeldscherm krijgen en derhalve de daarbij behorende programma's niet uitvoeren. Nog sterker is het een bepaalde gebruikersgroep een afzonderlijke bibliotheek te geven (is niet mogelijk bij integratie van de programmatuur over de verschillende gebruikersgroepen heen). Bovendien is het S/34 in staat alle acties die door de verschillende beeldstations worden verricht, inclusief de bij de console operator verschenen (fout)meldingen, vast te leggen op de schijf en op verzoek uit te lijsten. Een volledige controle lijkt mogelijk.

Echter! Het is evengoed mogelijk deze faciliteit uit te schakelen of de activiteitenlogging te vernietigen voordat hij is uitgelijst. Bovendien kunnen passwords als waren het telefoonnummers aan een ieder bekend worden gemaakt.

Het is de plicht van de systeemontwerper/programmeur om in het toepassingsprogramma de nodige controles in te bouwen en van deze controles een verslag te laten afdrukken. Bijvoorbeeld een volledigheidscontrole door middel van een batchtotaal heeft pas waarde als op het invoerverslag batchtotaal, computertelling en het eventuele verschil worden gemeld.
Ter bewaking van de stambestanden dient een verslag te worden geprogrammeerd waaruit blijkt wanneer en door wie wijzigingen zijn aangebracht, alsmede de aard van de wijziging door vermelding van de oude inhoud en de nieuwe inhoud van de gewijzigde rubrieken.
Een dergelijk verslag ontbreekt helaas maar al te vaak.

Van niet te onderschatten belang is de wijze waarop ontwikkeling (ontwerp, programmering) en de invoering (testen, schaduwruns, opleiding personeel) door het bedrijf wordt begeleid en bewaakt. Gedurende deze ontwikkelingscyclus kan er heel wat fout gaan. En soms in zodanige mate dat de accountantscontrole erdoor in gevaar komt. Niet correct werkende programmatuur kan de verstrekte informatie zodanig verminken dat alleen ten koste van zeer grote inspanning en een aanzienlijk tijdsbeslag (correctiewerkzaamheden, herprogrammering) tot acceptabele resultaten gekomen kan worden. Het rapporteringstijdstip kan daardoor ver worden overschreden. De praktijk heeft voorbeelden genoeg gegeven, waarbij de aard en de omvang van de gebreken uiteraard verschillen.

Dergelijke gevallen hebben echter gemeen dat aan het softwarehuis (of aan andere systeemontwikkelaars) te veel vertrouwen wordt geschonken. Zij doen "schone" beloften en maken ze maar zelden - op tijd - waar; de goeden niet te na gesproken. Dat de accountant in dat geval mede slachtoffer is behoeft geen betoog. Met de toekomstige gebruiker zou ook hij meer alert moeten zijn op de vorderingen van het softwarehuis. En met name wanneer de planning wordt overschreden. In geen geval mag worden geaccepteerd dat concessies worden gedaan aan de testactiviteiten.

Hieruit zal het duidelijk zijn geworden dat bij de komst van een computer een deel der werkzaamheden van de accountant erdoor wordt beïnvloed. En dat hij, wil hij een zelfde kwaliteit "produkt" leveren, beter niet om de computer heen kan gaan.
Bij voorkeur op het moment waarop de ontwikkeling van een geautomatiseerd systeem van start gaat, doch in ieder geval uiterlijk bij de implementatie, dient de controlerend accountant zichzelf een aantal vragen te stellen, waarvan de voornaamste zijn:

- Is er documentatie waaruit de opzet en de werking van het informatieverwerkend systeem blijkt?
- Worden alle ingevoerde gegevens volledig en juist verwerkt?

- Kan door de gebruiker controle worden uitgeoefend op de volledige en juiste verwerking van de gegevens?
- Worden (controle)tellingen op de juiste wijze opgebouwd en door middel van verslagen zichtbaar gemaakt?
- Worden er adequate verslagen opgeleverd van de in de stamgegevens aangebrachte mutaties?
- Kan van gecumuleerde gegevens achteraf worden vastgesteld uit welke details zij zijn opgebouwd?
- Kan worden vastgesteld dat niet ongeautoriseerd is gemuteerd of posten zijn ingevoerd?
- Kan van door de computer gegenereerde (= niet direct uit de invoer af te leiden) gegevens worden vastgesteld dat zij juist en volledig zijn?
- Is de continuïteit van de informatieverstrekking voldoende gewaarborgd (beveiligingsmaatregelen voldoende, voldoende en frequente kopiëring van belangrijke bestanden)?
- Kan worden vastgesteld op welk moment een nieuwe versie van een programma in gebruik is genomen?

Op deze vragen dient een antwoord verkregen te worden voordat het geautomatiseerde systeem operationeel wordt. Daarbij komt dat de organisatie voorbereid zal moeten zijn op de invoering van de automatisering die, zoals reeds geschetst, ingrijpend kan zijn. De accountant dient dit tijdig vast te stellen. Hij zal dienen te beoordelen dat daar, waar oude functies en functiescheidingen zijn verdwenen en nieuwe verschijnen, de kwaliteit van de interne controle niet is verslechterd.
Bovendien zal hij er op dienen te letten dat er geen onaanvaardbare opeenhoping van kennis bij één persoon of op één afdeling ontstaat. En zo dit onvermijdbaar schijnt, welke aanvullende maatregelen van interne controle en beveiliging hij zal dienen te adviseren om het daaruit voortvloeiende risico te beperken.

Een en ander vereist extra inzet van de accountant (dat wil zeggen een heroverweging van het controleplan en de technische uitwerking ervan) en veroorzaakt extra kosten voor de cliënt. Het zijn echter kosten die, evenals de aanschaf van apparatuur en programmatuur en het opleiden van personeel, tot de normale initiële kosten van automatisering gerekend dienen te worden. Het is bovendien raadzaam dat de accountant op een zo vroeg mogelijk tijdstip wordt ingeschakeld. Als medegebruiker van het systeem is het wenselijk dat hij zijn eisen met betrekking tot een goede controleerbaarheid kenbaar kan maken. Overigens zij hierbij opgemerkt dat de accountant per definitie geen andere eisen dient te hebben dan het management.

De accountantscontrole kan in een aantal gevallen worden aangepast door gebruik te maken van de mogelijkheden van het systeem en de daarbij behorende bestanden. Bij het laatste kan de computer op meestal eenvoudige wijze worden benut voor het maken van selecties of het zichtbaar maken van telverbanden.

Een van de faciliteiten die het IBM-systeem/34 biedt is de Data File Utility (DFU), waarmee eenvoudige selecties (posten groter dan, kleiner dan een opgegeven waarde) met telling op één niveau kunnen worden verkregen. Slechts enkele eenvoudige opdrachten aan de computer zijn hiervoor voldoende.

Concluderend stel ik vast dat in het kader van de accountantscontrole bij gebruik van een small business computer de navolgende werkzaamheden dienen plaats te vinden:

- Bij de installatie van het systeem en vervolgens periodiek wordt een onderzoek ingesteld naar de invloed van automatisering op de organisatie, naar de maatregelen van interne controle in de programmatuur, naar de opzet van de testprocedure en naar de beveiligingsmaatregelen die de continuïteit van het gegevensverwerkingsproces moeten waarborgen.
- Periodiek zal vastgesteld dienen te worden of de getroffen maatregelen blijven functioneren, zodat het vertrouwen dat management en accountant erin stellen gerechtvaardigd is.
- Nagegaan dient te worden of bij de controle doelmatig van de mogelijkheden van het geautomatiseerde systeem gebruik kan worden gemaakt, bijvoorbeeld door raadpleging van de informatieverzamelingen op dezelfde of op een andere computer (bijvoorbeeld die van de accountant zelf).
- Periodiek zal een management letter over de opzet en werking van de automatiseringsorganisatie worden uitgebracht. Daarbij dient de accountant zich te realiseren dat in een geautomatiseerde omgeving het frauderisico is toegenomen. Het management als drager van de verantwoordelijkheid voor dit risico, dient daarop gewezen te worden.

Hulpmiddelen en literatuur inzake de controle in een minicomputeromgeving

1. Vragenlijst ten behoeve van de beoordeling van de organisatie van de geautomatiseerde gegevensverwerking (I.C.V. hoofdstuk 0). Daarvan zijn alleen de paragrafen 3 t/m 7 van toepassing (voor intern gebruik).
2. Checklist ter beoordeling van (standaard)toepassingsprogrammatuur voor de financiële administratie op small business computers (uitgave Userclub-werkgroep "Small Systems"). In de inleidende hoofdstukken is een controlenetwerk ter beheersing van de volledige en juiste verwerking van de gegevens uitgewerkt en toegelicht.
3. Auditing in a minicomputer environment, door Leslie S. Krischner. (Edpacs, July 1978)
4. Minicomputers: goed nieuws of slecht nieuws?, door drs. J.C. van Dijk, R.A. (De Accountant, december 1980).

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

lente 1981

COMPUTERTOEPASSING BIJ EEN AUTO-IMPORTEUR

door H.G.T. van Gils

Inleiding

In dit artikel wordt ingegaan op de controle van betalingen, die door een auto-importeur zijn verricht, in het kader van zijn garantieverplichtingen door de verkoop van nieuwe auto's. Het onderzoek vindt ieder halfjaar plaats en is voor het eerst verricht in 1979.
Deze toepassing is in EDP-AUDITOR geschreven, waarbij voor een belangrijk deel gebruik gemaakt is van de LIBRARY-OF-ROUTINES, een programmabibliotheek, waarin een aantal kant-en-klare programma's zijn opgenomen.
De lijst-voorbeelden die bij dit artikel zijn opgenomen bevatten gefingeerde cijfers!

Systeembeschrijving

Het garantiesysteem van deze importeur is volledig geautomatiseerd.
Het grootboek bevat voor de garantie-uitkeringen een aantal rekeningen. Per uitkering wordt slechts één rekening belast. Welke rekening belast wordt, is afhankelijk van het moment van uitkering (in of buiten de garantietermijn) en van de reden van toewijzing. Voor bepaalde garantie-uitkeringen worden van de fabrikant vergoedingen ontvangen.
De belasting van de verscheidene grootboekrekeningen vindt geïntegreerd vanuit het garantiesysteem plaats.

Voor iedere verkochte auto worden bepaalde factuurgegevens in een gegevensverzameling opgenomen. Iedere schademelding, waarvoor een garantie-uitkering wordt gevraagd, wordt in hetzelfde bestand vastgelegd. Daarna worden gegevens toegevoegd met betrekking tot de hoogte van de garantie-toewijzing, variërend van 0 tot 100%.
Ook van alle verrichte reparaties worden gegevens in het bestand vastgelegd, alsmede enkele boekhoudkundige gegevens, zoals de grootboekrekening waarop de boeking moet plaatsvinden.
Tenslotte worden door het systeem creditfacturen aangemaakt en de relevante gegevens weer in het bestand vastgelegd.

Het zal hieruit duidelijk zijn, dat het bestand omvangrijk is, met per auto een sterk wisselende hoeveelheid gegevens.
Hoewel het systeem zelf een aantal overzichten oplevert, zoals mutatieverslagen en statistische overzichten (bijvoorbeeld per dealer, per autotype, per schadetype), geven deze lijsten onvoldoende controlemogelijkheden voor de accountant.
Gezien de omvang en de mogelijkheden is hier gekozen om met behulp van de computer een aantal controletellingen te verrichten en uit de garantie-uitkeringen een gestratificeerde steekproef te nemen, ten einde aan de hand van de onderliggende documenten een oordeel te kunnen verwerven omtrent de juistheid van de boekingen.

Uitwerking

Om een gestratifceerde steekproef te verrichten, dient men eerst de volledigheid van de gegevensverzameling vast te stellen en een inzicht te hebben in de verdeling van de massa.

Voor de volledigheid moet aansluiting gezocht worden met het grootboek. Daarom is eerst een overzicht in totalen per maand en grootboekrekening vanuit het garantiebestand opgesteld. Dit overzicht is opgenomen als voorbeeld 1.

Om tevens een inzicht te verkrijgen in het juiste gebruik van de grootboekrekening, waarop de uitkeringen binnen de garantietermijn geboekt zijn, is een ouderdomsoverzicht opgesteld, waarbij het verschil in maanden bepaald wordt tussen de factuurdatum en de uitkeringsdatum. Een gedeelte van dit overzicht is opgenomen als voorbeeld 2.

Om een inzicht te krijgen in de verdeling van de populatie is gebruik gemaakt van de LIBRARY-OF-ROUTINES uit het EDP-AUDITOR-pakket. Door middel van het aanroepen van het desbetreffende programma en het toevoegen van slechts vier kaarten, wordt een frequentieverdeling verkregen, zoals is opgenomen in voorbeeld 3. Andere klasse-indelingen zijn evenzeer mogelijk.
Met behulp van dit overzicht kan de controlerend accountant zijn selectieparameters definiëren voor de gestratificeerde steekproef, die in de volgende stap genomen zal worden. Voor deze steekproef wordt weer gebruik gemaakt van de LIBRARY-OF-ROUTINES uit het EDP-AUDITOR-pakket. Het pakket bevat een aantal verschillende steekproefroutines en men heeft de mogelijkheid zelf andere technieken toe te voegen.

In het onderhavige geval is gekozen voor een eenvoudige methode met vijf strati, waarbij per stratum een percentage is opgegeven van het aantal a-select te trekken posten.
Een voorbeeld van zo'n overzicht is opgenomen als voorbeeld 4. Alleen de hoogste stratum is hier afgebeeld, waarbij het selectiepercentage op 100 is gesteld.
Ook voor deze steekproef zijn slechts enkele programmakaarten nodig geweest.

Het steekproefoverzicht zal gebruikt worden om de desbetreffende garantiedossiers te lichten en de uitkeringen aan de hand van de documenten te toetsen op hun juistheid en autorisatie. Dit laatste hoort echter niet meer tot het geautomatiseerde gedeelte van de toepassing. Wel is overleg met de programmeur van belang. Zo bleek in de testfase, dat de garantiedossiers per tien dagen in het archief werden opgeborgen en dus niet meer op garantieverzoeknummer lagen. Ook het tijdstip van archivering bleek nog uit het bestand te achterhalen, zodat deze datum alsnog op de lijst onder controleaantekeningen kon worden opgenomen.

Voorbeeld 1

Report no. 40 * KKC - HVG * Totalen per maand en grootboekcode 08/26/80

Groot-boek-codes	Totaal eerste halfjr.	Aantal posten	januari 1980	februari 1980	maart 1980	april 1980	mei 1980	juni 1980
5900	60.000	350	23.000	4.000	8.000	8.000	10.000	7.000
5901	5.900.000	40.000	900.000	700.000	1.000.000	600.000	1.600.000	1.100.000
5902	2.800.000	7.000	400.000	300.000	600.000	400.000	800.000	300.000
5904	30.000	40	8.000	3.000	2.000	4.000	9.000	4.000
Totaal	10.000.000	50.000	1.500.000	1.200.000	1.800.000	1.200.000	2.800.000	1.500.000

Voorbeeld 2

Report no. 50 *KKC - HVG* Ouderdomsoverzicht garantie 08/26/80

Factuur-datum in maanden geleden	Totaal schade-uitkering	Aantal	januari 1980	februari 1980	maart 1980	april 1980	mei 1980	juni 1980
27	1.600	4		800	400			400
23	4.000	4	3.400			600		
14	570.000	2.500	50.000	50.000	70.000	60.000	250.000	90.000
13	540.000	3.000	70.000	50.000	90.000	80.000	140.000	110.000
12	500.000	3.000	80.000	60.000	150.000	50.000	110.000	50.000
11	420.000	2.800	80.000	70.000	90.000	50.000	100.000	30.000
10	380.000	2.500	130.000	50.000	70.000	30.000	50.000	50.000
01	130.000	1.700	20.000	10.000	20.000	10.000	40.000	30.000
00	10.000	100	1.000	1.500	1.500	4.000	1.000	1.000
01-	15.000	60	1.000	2.000	1.000	1.000	7.000	3.000
Totaal	10.000.000	50.000	1.500.000	1.200.000	1.800.000	1.200.000	2.800.000	1.500.000

Voorbeeld 3

Report no. 03 *KKC - HVG* Overzicht garantiebestand 08/26/80

Each range boundary in the -to- column has an additional 99 cents understood. Thus, 9,999 is actually $ 9,999.99.

Balance range from	to	Number on file	Percent of file	File balance within range	Percent of file	0 1 2 3 4 5 6 7 8 9 10 11 12	Cum. pct.
zero		600	1.2	0	0.0	x	.0
.01+	9	250	0.5	2,000	0.0	x	.0
10	19	850	1.7	14,000	0.1	x	.4
20	29	3,300	6.6	85,000	0.9	xxxxx	2.1
30	39	3,350	6.7	120,000	1.2	xxxxxxx	4.2
40	49	4,300	8.6	195,000	2.0	xxxxxxxxxxx	7.2
50	59	3,250	6.5	180,000	1.8	xxxxxxxxxx	9.7
60	69	2,900	5.8	190,000	1.9	xxxxxxxxxx	12.4
70	79	2,200	4.4	160,000	1.6	xxxxxxxxx	14.8
80	89	2,700	5.4	230,000	2.3	xxxxxxxxxxxx	18.1
90	99	2,700	5.4	260,000	2.6	xxxxxxxxxxxxxx	21.8
100	199	14,050	28.1	2,460,000	24.6	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	40.7
200	299	3,450	6.9	950,000	9.5	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	51.7
300	399	1,550	3.1	580,000	5.8	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	58.7
400	499	900	1.8	430,000	4.3	xxxxxxxxxxxxxxxxxxxxxxx	63.7
500	599	650	1.3	370,000	3.7	xxxxxxxxxxxxxxxxxx	67.6
600	699	500	1.0	340,000	3.4	xxxxxxxxxxxxxxxxx	71.0
700	799	500	1.0	390,000	3.9	xxxxxxxxxxxxxxxxxxx	73.9
800	899	400	0.8	350,000	3.5	xxxxxxxxxxxxxxxxx	76.2
900	999	400	0.8	390,000	3.9	xxxxxxxxxxxxxxxxxxx	78.6
1,000	1,999	1,000	2.0	1,500,000	15.0	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	92.0
2,000	2,999	100	0.2	250,000	2.5	xxxxxxxxxxxxxx	94.5
3,000	3,999	50	0.1	175,000	1.7	xxxxxxxxx	96.1
4,000	4,999	23	0.0	105,000	1.1	xxxxxx	97.3
5,000	5,999	10	0.0	55,000	0.5	xxx	98.0
6,000	6,999	1	0.0	6,500	0.1	x	98.1
7,000	7,999	3	0.0	22,500	0.2	xx	98.4
8,000	8,999	1	0.0	8,500	0.1	x	98.5
9,000	9,999	1	0.0	9,500	0.1	xx	98.7
10,000	19,999	11	0.0	172,000	1.7	xxxxxxxxx	100,1
Totals		50,000	99.9	10,000,000	100.0		

Voorbeeld 4

Report no. 10 Controle garantiekosten per 1.1.80 - 30.6.80 08/26/80

Sample selection data for stratum 5. Stratum limits: from 3,000.00 to 9,999,999,999,999.99.
Population 100. Computed sample size = 100 (100%).

Chassis-nummer	Gar.verzoek-nummer	Totaal loon	Totaal materiaal	Toeslag	Werk derden	Totaal-bedrag	Controle-aantekeningen
04MG3659	94475	675	2.500	225		3.400	31.5.79
05410541	1923	625	3.500	375		4.500	10.6.79
02018141	19778	785	2.700	315	2.000	5.800	30.6.79
Totaal		62.000	282.000	22.100	187.000	554.000	

TOP SECRET 1981

door A.W. Neisingh

Van 26 tot en met 28 januari jl. werd in Monte Carlo het eerste internationale symposium inzake computer security en privacy door Cii Honeywell Bull georganiseerd.
In totaal 20 sprekers spraken de circa 400 deelnemers toe.
De inleidingen waren geconcentreerd rondom de volgende onderwerpen:

1. Transborder data flow
2. Defenses against computer crime
3. Disaster recovery planning
4. The shape of tomorrow and computer security
5. Distributed systems and communications security.

Grensoverschrijdend gegevensverkeer (transborder data flow)

De eerste inleider G. Russell Pipe besteedde onder meer aandacht aan de belangrijkste karakteristieken van de Westeuropese wetgeving op het gebied van de privacy-bescherming, zoals één nationale wetgeving, instelling van een "Registratiekamer" (Zweden: data inspection board; West-Duitsland: Bundesbeauftragter für den Datenschutz), het toekennen van bevoegdheden aan die Registratiekamer ten aanzien van technische en administratieve controles en dergelijke.
Na een overzicht van de landen met respectievelijk zonder privacy-wetgeving werden enige "hot topics" ten aanzien van transborder data flow genoemd, te weten:

- de onmogelijkheid data protection standards buiten de eigen jurisdictie af te dwingen;
- de technologische ontwikkeling waardoor teletext, view data, electronic funds transfer systems en dergelijke nauwelijks effectief in de gaten kunnen worden gehouden.

Van belang voor de landen verenigd in de OECD is de door de Council aanvaarde "recommendation governing the protection of privacy and transborder data flows of personal data" en de door de Committee of Ministers of the Council of Europe aanvaarde "convention for the protection of individuals with regard to automatic processing of personal data".

In beide stukken wordt uitgegaan van minimumstandaarden ten aanzien van privacy-bescherming in alle aangesloten landen, zoals beperkingen met betrekking tot opslag en verzamelen van persoonsgegevens, het recht op inzage en het recht van correctie.

Prof. Knut Selmer besteedde in zijn inleiding aandacht aan de problematiek van de transborder data flow en wel in die zin: "Hoe kunnen inbreuken op de privacy-wetgeving en in het bijzonder bij grensoverschrijdend gegevensverkeer worden geconstateerd?".
Immers door gebruik te maken van moderne datacommunicatietechnieken (satellieten) worden data "vluchtig".
Een wettelijke regeling als zodanig biedt op dit punt onvoldoende beperking, omdat de controle op de naleving van de wetgeving zeer moeilijk is.

Er zijn veel vormen van grensoverschrijdend gegevensverkeer, zoals die waarbij:

- gebruik wordt gemaakt van servicebureaus in het buitenland voor (delen van) de administratieve gegevensverwerking (salarisadministratie, facturering en dergelijke);
- de gegevensverwerking van dochterondernemingen bij de moedermaatschappij plaatsvindt;
- kopieën van bestanden uit beveiligingsgezichtspunt in een kluis aan de andere zijde van de grens worden bewaard;
- uitwijk in het kader van een noodvoorzieningenplan slechts in het buitenland kan plaatsvinden (bijvoorbeeld in geval van de configuratie geen tweede in hetzelfde land staat);
- enz..

Defenses against computer crime

Onder deze verzamelnaam kwamen een viertal sprekers voor het voetlicht, die de volgende onderwerpen bespraken:

1. De ontwikkelingen in computer crime in Europa
2. De invloed van computer crime
3. De noodzaak van wetgeving met betrekking tot computer crime
4. De psychologie en de motieven van fraudeurs.

In de pers is veel aandacht besteed aan de uitspraken van de heren Donn B. Parker en Stein Schjølberg.
De voorbeelden kwamen bij accountants nogal ongenuanceerd over.
De sprekers schonken geen aandacht aan de noodzaak van het bestaan en de goede werking van een adequaat stelsel van maatregelen van interne controle en beveiliging in een organisatie.
Een reeks voorbeelden gaf blijk van zodanige leemtes in de organisatie en de interne controle dat de fraudes bij wijze van spreken zelfs bij toepassing van een handdoorschrijfsysteem mogelijk waren geweest.
Ook enige gevallen van diefstal van bestanden en programmatuur en computersabotage') kwamen naar voren.
Een belangrijk probleem is op welke wijze bewijsmateriaal van computer crimes kan worden verkregen en welke betekenis hieraan kan worden toegekend.
Spreker besloot met het voorleggen van de vraag of gedragsregels voor automatiseringspersoneel een zet in de goede richting zou kunnen geven.
In Nederland beijvert het Nederlands Genootschap voor Informatica zich ten aanzien van opstellen en invoeren van bedoelde gedragsregels.

Donn B. Parker wees nadrukkelijk op de fraudemogelijkheden bij electronic funds transfer systems (zoals SWIFT). Alhoewel de ontwikkeling in EFTS niet te stoppen zal zijn, dienen gebruikers maatregelen te nemen waardoor beïnvloeding van financiële systemen kan worden voorkomen.

') Zie het artikel van H. de Jong en P.T. Laagland in Informatie, november 1980; Compact no. 22, pag. 2.

De noodzaak van een wetgeving met betrekking tot computer crime werd uiteraard onderschreven. Immers de praktijk in de V.S. was jarenlang dat computerfraudeurs slechts konden worden veroordeeld op grond van bijvoorbeeld de telegraaf- en telefoonwet in plaats van fraude of iets dergelijks.

De spreker over het onderwerp de psychologie en de motieven van fraudeurs gaf een interessante voordracht ten beste. Alhoewel hij geen Nederlands kan lezen was de gelijkenis met het boekje van W.G. Brugge: "Het fraudeprobleem" opvallend.

Tot slot zij opgemerkt dat het naar mijn mening voorkeur verdient voorals nog over computer assisted/related crime te praten dan over computer crime.

Disaster recovery planning

Een interessante voordracht werd verzorgd door Dr. Kenneth Wong. Hij sprak over "back-up for a distributed system". In dit kader werd een time-table voor disaster recovery besproken.
De problematiek van het noodvoorzieningenplan bij een distributed system (dit is een online-systeem met gebruikers op afstand) versus die bij een batch-systeem werd aan de hand van de volgende trefwoorden toegelicht:

- Data entry and access (data preparation bureau, alternate user sites, off-line data capture, manual back-up).
- Data communication (back-up modem, back-up dial-up lines, communication network, segregate communication equipment from mainframe).
- Mainframe back-up (redundancy, multiple sites).
- Back-up computer centre (take over night shift, clash of TP networks, P/W control and terminal identities, file directory registration).

Benadrukt werd dat een risico-analyse dient vooraf te gaan aan de bepaling en uitwerking van een noodvoorzieningenplan.
Tot slot werd opgemerkt dat ingeval een plan gemaakt is een en ander uitgetest dient te worden.

De spreker inzake fysieke beveiliging schetste de getroffen beveiligingsmaatregelen ten behoeve van het centrum van een bank. Een aantal opmerkelijke uitspraken waren:

- Controleer de inhoud van door operating-personeel op de zaal meegenomen tassen.
- Accepteer nooit gesloten pakken en dozen op de computerzaal. Buiten de zaal openen!
- Breng een scheiding aan tussen de volgende soorten apparatuur:
  - printers: buiten de computerzaal;
  - apparatuur die geen bediening behoeft: CPU, MSS, modems;
  - overige apparatuur waarvoor bediening vereist is, console, magneetbandeenheden, verwisselbare schijven.

Jerome Lobel besteedde aandacht aan risico-analyse. Lobel onderkent een viertal stappen, te weten:

- survey: identify risks (risk events are: people, information and facilities);
- estimates and calculations (event frequency, event cost and manual cost);
- evaluation (risks → preventive measures → cost of prevention → return on investment);
- risk reduction plan.

The shape of tomorrow and computer security

De inleiding van Dr. Willis H. Ware was een appèl aan het management. Onder de titel "security, privacy and new technology" hield hij managers voor dat het implementeren van adequate beveiligings- en privacy-beschermingsmaatregelen geen vrijblijvende aangelegenheid is. Hij gaf ernstig in overweging bestanden met "gevoelige" informatie te versluieren (ook van betekenis bij oorlogsdreiging!).

De bespreking van electronic funds transfer systems was slechts van algemene aard.

Onder de titel "emerging corporate-wide information security strategy" besteedde Donald Coppotelli aandacht aan de wijze waarop een beveiligingsstrategie van de grond werd getild.
Een aantal stappen worden onderkend:

1. Assess status
2. Develop security program
3. Publish corporate policy
4. Set standards and guidelines
5. Produce risk assessment methodology
6. Recommend corporate disaster plan
7. Establish information classification
8. Implement education program.

Verschillende studies werden uiteraard uitgevoerd.

Charles T. Clingen lichtte het beveiligingsconcept in MULTICS toe. Zoals uit de literatuur bekend is, zijn zoveel mogelijk beveiligingsmaatregelen in de hardware opgenomen.
Uitgegaan wordt van een ring-protectiemechanisme, een zogenaamd access control list en een access isolation mechanism. Deze functies zijn gelijktijdig in gebruik.

Distributed systems and communications security

De titel "secure network concepts" was een dekmantel voor een bespreking van TRANSPAC, een packet switching netwerk in Frankrijk.

Allereerst werd ingegaan op de beveiligingsaspecten, te weten:

1. qualité de transmission (echo check, parity check, redundancy, etc.);
2. performances du réseau;
3. disponsibilité du service (dubbele uitvoering van lijnen en dergelijke);
4. dispositifs de secours (access multiligne, raccordement à 2 commutateurs, secours par le réseau téléphonique).

Vervolgens aandacht voor de privacy-bescherming van via TRANSPAC verzonden gegevens, zoals het gebruik van passwords en cryptography.

Het symposium werd besloten met het onderwerp "advances in access control and network protection systems".
De Franse spreker was zó rap van tong dat zelfs de simultaanvertaalsters het moede hoofd snel in de Monagaske zonneschijn legden.

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

Record Computer Fraude

Monaco, februari 1981. Cii Honeywell Bull heeft een select gezelschap computer-experts in Monte Carlo uitgenodigd voor het symposium "Top-Secret-'81". Op het programma staat "Computerfraude" als hoofdonderwerp. Tot de internationaal bekende sprekers behoren Donald Parker van het Stanford Research Institute, en Russell Pipe, consultant bij de OECD en hoofdredakteur van het blad Transnational Data Report.

Eén van Pipe's stellingen is dat computerfraude door het management nog te zeer wordt onderschat en dat er een flinke catastrofe op computerfraude gebied moet gebeuren, wil men de ernst van de bedreiging inzien.

Pipe wist niet dat een catastrofe al in de maak was. Terwijl de heren computer experts zich tegoed deden aan de geneugden van het kleine vorstendom, sloegen "computer-zwendelaars" hun slag. De buit bedroeg maar liefst $ 21 miljoen, een record computerdiefstal.

Accountants in Beverley Hills

De vermoedelijke dader is L. Ben Lewis, operations officer van de Wells Fargo Bank, bijkantoor Beverly Hills. Op 23 januari jongstleden moest Ben Lewis 's morgens wat vragen beantwoorden van de op bezoek zijnde interne accountants omtrent een aantal vreemdsoortige intrebancaire transacties waar zijn handtekening onder stond.

De lunch

Lewis gaf zo goed en zo kwaad een verklaring voor de transacties en zei vervolgens dat hij een dringende lunch afspraak had. Na de lunch zouden de accountants verder gaan. Op dat moment realiseerde Lewis zich dat de top van de ijsberg, die tenslotte 21,3 miljoen dollar groot zou blijken te zijn, snel aan het ontdooien was. Hij achtte het raadzamer om maar niet terug te keren van de lunch. Verder onderzoek in de affaire gaf aanwijzingen dat Lewis al ruim twee jaar bezig was met een gigantische fraude.

Dubbel boekhouden

Hij maakte gebruik van de in bankkringen gebruikelijke tussenrekening voor het geldverkeer tussen de kantoren van een bank onderling.

De vergissing

Volgens Richard Cooley, de chairman van Wells Fargo's Bank, was de opzet van Lewis zo simpel dat hij er maar eens in de vijf dagen tien minuten voor nodig had. Het plan kwam uit omdat hij zich een keer vergiste en de verkeerde informatie naar de tussenrekeningen stuurde. Door zijn positie als operations officer had Lewis een goede kennis van de boekhoudkundige systemen van de bijkantoren en bovendien was hij op de hoogte van de controlesystemen van de bank. Dit laatste behoort doorgaans niet tot het kennispakket van de willekeurige directeur van een bijkantoor, maar Lewis had zich zonder veel moeite deze procedures eigen gemaakt.

De methode

De Wells Fargo Bank is de elfde in grootte in de V.S. en heeft meer dan 380 bijkantoren. Ben Lewis werkte in zijn elfjarige carrière bij Wells Fargo onder meer op het computercentrum en wist uit die tijd de twee meest belangrijke beveiligingen tegen het oneigenlijk gebruik van de tussenrekeningen. Het transactieverkeer tussen banken en bijkantoren onderling is meer en meer gecomputeriseerd naarmate het geldverkeer de afgelopen jaren toenam. Als

voorbeeld een cheque van een rekening van bijkantoor A wordt ingewisseld bij bijkantoor B, dan voert B bij de tussenrekening een claim in op A. Binnen vijf dagen moest een post op de tussenrekening worden verwerkt anders zou er een melding uitgaan naar het controlesysteem. Lewis was hiervan op de hoogte en creëerde eigenhandig een creditnota voor het systeem op grond waarvan het saldo werd verhoogd van de rekening van Muhammad Ali Professional Sports Inc., een organisatie die bokswedstrijden organiseert. De bekende bokser heeft hieraan alleen zijn naam verbonden en heeft met de hele fraudezaak niets te maken, maar speculaties omtrent de mogelijke rol van Muhammad Ali gaven aan de hele affaire nog een extra pikant tintje. Nadat Lewis een creditnota had ingevoerd, gaf hij het systeem te kennen dat deze zou worden vereffend door een debetpost van een ander bijkantoor. Binnen de vijf dagen creëerde Lewis een nieuwe transactie die weer werd gevolgd door een nieuwe debetpost. Weer vijf dagen later bracht Lewis een creditpost in het systeem en zo kon hij onbeperkt doorgaan. Aldus stal hij miljoenen dollars uit het systeem zonder ooit aan een van de rekeningen van zijn bijkantoor te komen.

De "beveiliging"

Naarmate de bedragen van Lewis' transacties groter werden stuitte hij op een nieuwe veiligheidsmaatregel. De computer geeft een automatische waarschuwing bij iedere transactie die de 1 miljoen dollar te boven gaat. Lewis zijn oplossing was zeer eenvoudig en effektief, hij verdeelde zijn grote posten eenvoudig in delen van minder dan 1 miljoen dollar. Uiteindelijk was Lewis gedwongen om 25 verschillende transacties van elk bijna 900.000 dollar elke vijfde werkdag in het systeem in te voeren. Ook andere beveiligingsmaatregelen wist hij te ontlopen maar men is er nog niet achter hoe daarbij de vork in de steel stak. Op de een of andere manier moet hij gedurende zijn vakantie ook op kantoor zijn geweest.

Vakantie

De bank heeft een verplichte jaarlijkse vakantie van twee weken en Lewis moet deze hebben opgenomen anders zou dat zijn opgevallen. Waarschijnlijk is hij gedurende zijn vakantie toch elke vijfde werkdag op kantoor geweest om de nodige transacties in de computer in te voeren. Lewis wist ook de verplichte functierotatie van de bank te vermijden. Bij dit systeem worden periodiek de taken van de belangrijkste functionarissen doorgeschoven, juist om eventuele fraudemogelijkheden te voorkomen. Waarschijnlijk heeft Lewis kans gezien deze voorschriften in zijn bijkantoor niet toe te passen.

Het hele systeem werkte twee jaar lang feilloos totdat Lewis in januari een fout maakte en de verkeerde transactie in de computer invoerde. Voor het eerst in zijn "carrière" bereikte een van zijn creditposten wel degelijk het andere bijkantoor en de desbetreffende kantoormanager belde Lewis voor een verklaring. Hij kon hier geen adequate verklaring voor geven en de bal begon te rollen.

Geld naar Zwitserland

Vooralsnog ziet het er niet naar uit dat Wells Fargo z'n 21 miljoen dollar terug kan krijgen. Harold Smith de chairman van Muhammad Ali Professional Sports heeft waarschijnlijk het merendeel van de buit veilig in Zwitserland weten te brengen. ■

BOEKEN

door J. Philippo

In de AC-bibliotheek zijn in de afgelopen maanden een drietal boeken opgenomen, welke zich bezighouden met de ontwikkeling van een informatiesysteem, de controle op de projectorganisatie, waarin een systeem ontwikkeld wordt en de accountantscontrole van informatie (lees jaarrekening) uit geautomatiseerde systemen.
Deze boeken zijn respectievelijk uit Nederlandse, Amerikaanse (internationale?) en Engelse bron.

AC 318 Organisatie en informatie-ontwikkeling - J.W. Ganzevoort en A. van der Heijden

1980

Dit handboek, geschreven door twee medewerkers van de Organisatiegroep van Klynveld Kraayenhof & Co., gaat over het bepalen van de behoefte aan informatie, die mensen in organisaties hebben.
De informatiebehoeftebepaling is een fase in het proces van de ontwikkeling van informatiesystemen, welke vitaal blijkt te zijn voor de effectiviteit van de systemen. Er dient dan echter een voorwaarde vervuld te worden, zoals de schrijvers als hun primair uitgangspunt nemen: "de leden van een organisatie kunnen hun informatiebehoeften alleen dan formuleren, als er duidelijkheid bestaat omtrent hun functie en taken, hun plaats in de structuur van de organisatie en over de processen, die zich in de organisatie afspelen".

De voorgestelde ontwikkelingsmethode is gericht op een leerproces; het doel is niet alleen "de informatiebehoeften" te bepalen, maar de gebruikers de kennis, vaardigheden en instrumenten te leren ontwikkelen om voortdurend informatie te kunnen aanpassen aan zich wijzigende omstandigheden. Participatie van gebruikers (management en medewerkers) staat centraal en kan bereikt worden via een projectorganisatie.
De methode heeft, met het oog op de massaliteit van de benodigde gegevens bij de ontwikkeling van informatiesystemen, de volgende opzet:

- gefaseerde aanpak, namelijk drie conditionerende fasen en drie constituerende fasen;
- geïntegreerd formulierenstelsel ter verhoging van de doelmatigheid;
- coderingsstelsel voor de bestaande informatie, de informatiebehoeften en de gedefinieerde informatie;
- handleiding door middel van beschrijving van de methode en hulpmiddelen (deel I van het boek) en een praktijkhandleiding (deel II).

De zes fasen van de ontwikkelingsmethoden zijn ieder in een afzonderlijk hoofdstuk besproken; zij zijn

1. Introductie en afstemming
2. Inventarisatie van organisatie en informatievoorziening
3. Vastlegging van de organisatie
4. Inventarisatie van de informatiebehoeften
5. Definiëren van de informatie
6. Opstellen van de informatiegids.

Hoofdstuk 8 geeft de mogelijkheden voor de verdere ontwikkeling van het informatiesysteem, namelijk het opstellen van het automatiseringsplan, het invoeringsplan en het organisatieveranderingsplan, waarvoor in de fasen 1-6 de basis is gelegd.

Niet alleen de methodische aanpak, maar ook de ervaringen van de schrijvers op dit gebied - welke regelmatig blijken - doet het boek aanbevelen in handen van hen, die de ontwikkeling van een informatiesysteem vanaf het begin goed willen doen. Daarnaast is het - ter indoctrinatie - een zeer goed boek voor opleiding, vooral dank zij het praktijkboek, dat op verhalende wijze de methode weergeeft.

AC 307 Project auditing methodology - W.S. Turner
1980 (453 blz.)

In dit boek beschrijft W.S. Turner, een medewerker van Pandata van de CAP/Gemini/Sogeti-groep, de project auditing methodology, welke gebruikt werd om projecten - welke door de groep met SDM (System Development Methodology) werden uitgevoerd - te beheersen.
De reden, waarom men dit nodig achtte, hoewel SDM een uitgebalanceerde ontwikkelingsmethode is, was het feit, dat de ontwikkeling van een informatiesysteem een complex proces is, dat door een relatief kleine groep wordt uitgevoerd.
De beschreven audit-methode is meer een praktische dan een theoretische benadering. Project auditing is een nieuw gebied; ongetwijfeld zullen de aangegeven technieken nog uitgebreid of gewijzigd worden.

Om het gebied meer te omschrijven geeft de schrijver de volgende definities:

- Een project-audit is het formele en systematische onderzoek naar de uitvoering van een gestart project ten opzichte van de gestelde eisen zoals de tastbare resultaten van het verrichte werk, het project-management, projectmethoden en -technieken en de organisatie en controles (beheersing).
- Een project audit is een activiteit van afweging tegen van tevoren vastgestelde en relevante standaards. Deze dienen te zijn vastgelegd in het projectcontract tussen de cliënt c.q. gebruikers en het projectteam en dat in een projectorganisatie wordt gerealiseerd.

In de situatie waarin de eindgebruikers of de projectorganisatie niet zijn gedefinieerd of waar geen contract en projectorganisatie aanwezig is, zal geen project-audit mogelijk zijn.

- Project-audit is ontworpen als een praktische, kostenbewuste, onafhankelijke en betrouwbare bron van informatie omtrent het project. Het is bedoeld als basis voor te nemen beslissingen door management; het ontslaat management niet van de verantwoordelijkheid om beslissingen te nemen.

Indeling van het boek

A. Project auditing baseline principles and concepts. Hierin worden de basis-criteria gedefinieerd waartegen de uitvoering van de audit geëvalueerd kunnen worden en dat verder dient ter "common understanding" tussen de audit report lezers en de auditor.

B. The project audit report. Dit hoofdstuk geeft een beschrijving van de inhoud van het report. Het kan de auditor dienen als hulp bij het verzamelen van gegevens en analyse daarvan, alsmede als gids voor het schrijven van het report.

C. Project auditing procedures. Een leidraad voor de auditor tijdens de fasen en stappen in het onderzoek. Het bevat een aantal checklists en formulieren voor de uitvoering.

D. Contract analyse. Hier wordt de basis gegeven voor de analyse van de contractdocumenten, waarin eenduidig door beide partijen het op te leveren produkt is beschreven en aanvaard.

E. Project audit service. Hier wordt de project-audit-organisatie van CAP/Gemini/Sogeti in Europa beschreven, welke echter door elke project-auditor (-groep) kan worden nagevolgd.

In appendices worden audit tools, een bibliografie en een index gegeven. Gedegenheid en vakkennis zijn de kenmerken van het boek en vooral ook praktische aanpak, welke ook blijkt uit de volgende zinsnede:

"The financial auditor has the advantage that the records of the company are kept in formats which are often governed by law and are otherwise governed by a limited number of standard alternatives accepted by the accounting profession.
The project auditor will have to deal with record keeping systems which are not governed by generally accepted standards in regard to their form or content. Even within a company the record keeping systems may vary from project to project. The project auditor, thus, should use the guidance of this book as a standard of reference for the form and contents of the records that should be used by the project".

AC 267 An audit approach to computers - B. Jenkins en A. Pinkney 1978 (435 blz.)

De nadruk, die de ondertitel "A new practice manual" geeft, is aanleiding eens terug te grijpen naar het in 1966 verschenen boekje onder dezelfde titel van de hand van Pinkney. En dan blijkt wel degelijk dat inderdaad nu een manual is verschenen, waarvan de accountant - zowel externe als interne - gebruik kan maken voor de aanpak van zijn controle.

In hoofdstuk 1 zijn de fasen van aanpak voor de controle weergegeven; daar deze een weergave zijn van de Engelse benadering, zijn zij ook in deze taal opgesomd.

1. Understanding and recording the system
2. Evaluation of Internal Control
   - User controls and programmed controls
   - Integrity controls
3. Functional tests (door anderen ook wel compliance of procedure tests genoemd)
4. The audit response to internal control weaknesses
5. Validation procedure (door anderen ook wel verification of substantial tests genoemd).

In de hoofdstukken 2 t/m 9 worden de bovengenoemde fasen uitgewerkt, waarbij naast de algemeen voor de accountant geldende aanpak de specifieke aanpak bij geautomatiseerde systemen is vermeld.
Daarenboven wordt in appendices bij de hoofdstukken meer detailinformatie gegeven.
De hoofdstukken 10 t/m 12 behandelen de bijkomende onderwerpen zoals het gebruik van de computer (10), serviceverwerking (11) en beveiliging (12), terwijl het boek wordt afgesloten met "Organisatie en training bij computer auditing".

Enkele opmerkingen ten aanzien van de genoemde fasen

Ad Evaluation of internal control

- Deze fase wordt gestart met het opstellen van een Internal Control Questionnaire op basis van de in de eerste fase vergaarde informatie. De schrijvers propageren het opstellen van een ICQ per applicatie. De ICQ is gebaseerd op het principe van "Control Objectives". In een appendix is een voorbeeld gegeven van de control objectives zoals deze gelden voor de activiteiten van de meeste industriële en handelsondernemingen. Voor een aantal van deze objectives zijn in een tweede appendix de relevante computer ICQ vragen opgegeven. De ICQ wordt gebruikt voor evaluatie van zowel het manuele als "computer"gedeelte van de applicatie.

- De schrijvers geven de volgende definities ten aanzien van de Internal Control:
  - User controls: manual controls carried out on data being processed
  - Programmed procedures: steps in the computer programs that may assist in the control of the data being processed
  - Integrity controls: those general controls, mainly in the computer department, that are concerned with computer programs and files, divided into:
    .. implementation controls
    .. program security controls
    .. computer operations controls
    .. data file security controls.

Ad Functional tests

Deze dienen: "to provide evidence that controls on which the auditor wishes to place reliance have continued to operate properly throughout the period under audit".
Bij het uitvoeren van de functionele testen bevelen de schrijvers een voorgeschreven documentatie aan, waarin onder meer worden opgenomen:

- een beschrijving van de test;
- referentie naar de bijbehorende delen van de ICQ;
- aangeven van de diepgang en omvang van de test en de periode waarover;
- opmerkingen over de uitvoering en de resultaten.

Conclusie

De schrijvers stellen, dat dit boek bestemd is voor:

- accountants, zowel externe als interne;
- managers en systeembouwers, welke in eerste instantie verantwoordelijk zijn voor de op te nemen interne controle;
- opleidingen, zowel voor de docenten als hun studenten.

Zij zijn daarin geslaagd, zij het dat het boek voorafgaande kennis vereist, namelijk ten aanzien van automatisering en accountancy, en als geheel toch vooral gericht is op de eerste groep.

P.S.

Een uitvoeriger bespreking van dit boek is te vinden in Edpacs van oktober 1980.

LITERATUUR

door J.C.P.M. Vermeeren en drs. B.M. de Vries

Your client's computer: a silent audit partner - K.W. Clowes, PhD, CA
CA Magazine, August 1980 - S 538

Trefwoorden: D 10, 12, 40, 50; H 30

In dit artikel over het gebruik van de computer bij het accountantsonderzoek worden een aantal stellingen aangetroffen die bij wijze van inleiding van dit excerpt woordelijk worden weergegeven.

- The innovative use of computers can help make an extensive substantive and analytical testing approach far more effective and efficient.
- Not many public accounting firms are fully exploiting the many audit opportunities computers offer.
- In designing computerized analytical review procedures auditors are limited only by their imagination.
- User instructions are usually well documented and don't demand a high level of EDP expertise.

Het uitgangspunt van de in dit artikel neergelegde gedachten is samengevat in de hier opgenomen schema's (Figure 1 en Figure 2).
In het eerste schema wordt de relatie gelegd tussen de mate van interne controle, de mate waarin daarop wordt gesteund en de te verrichten eigen actie ter verkrijging van de deugdelijke grondslag voor het accountantsoordeel.
In het tweede schema wordt een vergelijking weergegeven tussen een drietal mogelijke benaderingen van de accountantscontrole. De hoogte van de kolommen geeft daarbij de tijdsbesteding aan. Uit de keuze van de mogelijke benaderingen mag een voorkeur voor eigen actie worden afgeleid.

In het artikel wordt niet in de eerste plaats ingegaan op de alom bekende en beschreven "gereedschappen" zoals test-decks en accountantspakketten ten behoeve van bestandsonderzoeken, doch op een aantal minder bekende hulpmiddelen die in het algemeen beschikbaar zijn en aangewend kunnen worden bij de accountantscontrole, te weten:

- utility-programma's,
- de toepassingssoftware van de klant,
- de "report writers" en "query" talen.

N.B.: Voor de meeste van de hierna te behandelen technieken en hulpmiddelen kan ook gebruik gemaakt worden van standaard audit programmapakketten.

Figure 1

Audit Assurance and Emphasis

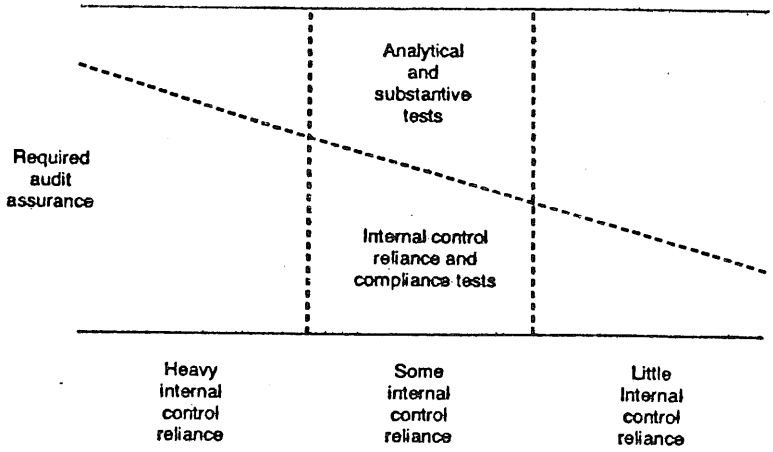
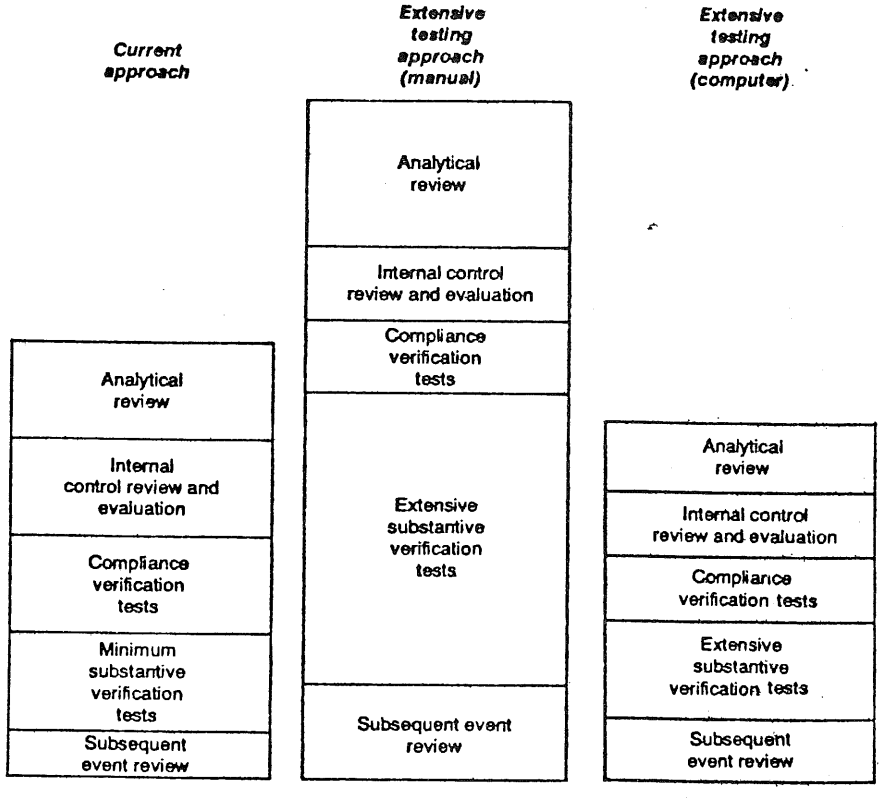


Figure 2

Hypothetical Audit Examination



ad Utility-programma's

Hierbij te denken aan sorteer-, samenvoeg-, kopieer-, print- en directory- en programma-uitlijstprogrammatuur.

ad Toepassingssoftware van de klant

Bijna zeker bevat de bibliotheek met toepassingsprogramma's van de klant betrekkelijk kleine programma's die specifieke bestanden lezen, totalen opbouwen en overzichten aanmaken. Vaak zullen deze met weinig of geen verandering dienstbaar kunnen worden gemaakt voor de accountantscontrole.
Het opsporen van dit type programmatuur kan gebeuren met behulp van directory lists, systeem- en programmadocumentatie of door middel van interviews.

ad "Report writers" en "query" talen

In deze sector liggen voor de accountant de grootste kansen. Het gebruik is doorgaans gemakkelijk te leren en vele pakketten voorzien in interactief gebruik.

Alle drie genoemde technieken zijn toepasbaar op de zes elementen van de accountantscontrole aangegeven in exhibit 1 hieronder.

Exhibit 1

Major Audit Activities

Analytical review
Audit work intended to provide the auditor with an overall understanding of a client's operations and environment, identification of matters of potential significance for financial statement purposes, identification of significant accounting transactions or balances, and ratio and trend analysis of financial and operating data to assist in assessing the reasonableness of financial statements.

Review and evaluation of internal control
The identification of general and specific control features and deficiencies that could have an effect on the reliability of accounting data, preliminary evaluation of the adequacy of controls to ensure a high level of reliability of accounting data, and development of a preliminary audit plan for the nature, extent, and timing of subsequent audit work.

Compliance verification of key controls
Assessing the proper functioning of critical controls identified in the review and evaluation of internal control—i.e., those controls on which the auditor wishes to rely for the purpose of determining the nature, extent and timing of further audit work.

Limited substantive verification of transactions and balances
Limited direct tests of accounting data in situations where the auditor's preliminary evaluation of controls was that they were adequate to ensure a high level of reliability of accounting data and where the results of compliance verification of key controls suggest that they were functioning effectively throughout the period of reliance.

Extensive substantive verification of transactions and balances
Extensive direct tests of accounting data in situations where the auditor's preliminary evaluation of controls was that they were not adequate to ensure a high level of reliability of accounting data or where compliance verification work suggested that apparently adequate controls might not have functioned effectively throughout the period of reliance.

Review of subsequent events
Determining the possible existence of matters subsequent to the financial statement date which might require either adjustment to or disclosure in the financial statements.

Toepassing bij de "analytical review"

De computer kan door de accountant worden gebruikt met behulp van utility-programma's, verbouwde toepassingsprogramma's of report writers die:

- de transactie- en "master"-bestanden tellen en rubriceren;
- uitzonderlijke posten selecteren;
- posten selecteren die aan door de accountant geformuleerde maatstaven voldoen.

N.B.: Voor het gebruik van utilities wordt als voorbeeld gegeven:

- op grootte sorteren met behulp van een sorteerprogramma;
- afdrukken op volgorde van grootte van een gewenst aantal posten met behulp van een afdrukprogramma.

Toepassing bij de beoordeling van de interne controle

Het gebruik van de computer richt zich hier op in de programmatuur ingebouwde controlemaatregelen en de ingebouwde totaalafstemmingen. Met name bij online-toepassingen neemt het belang van deze controles toe. De toepassing van test-data-methoden in combinatie met een controle op de wijzigingen in de programma's, gebaseerd op directory list, van programmabibliotheken, kan een belangrijke bijdrage leveren voor de zekerheid voor het bestaan van deze ingebouwde interne controlemaatregelen.

Toepassing met betrekking tot "compliance verification"

Op dit gebied kan de computer worden ingeschakeld bij het aanwijzen van te controleren steekproeven. De eerder aangeduide simulatietechnieken kunnen ook dienstbaar gemaakt worden om de goede werking van de ingebouwde controlemaatregelen te toetsen.

Toepassing ten behoeve van "substantive testing"

De uit te voeren onderzoeken zijn onder andere tellen, waarnemen (bijvoorbeeld inventariseren) saldobevestigingen, herbewerking van processen en detailonderzoek. Al de drie genoemde categorieën hulpmiddelen kunnen worden ingeschakeld, waarbij de voorkeur uitgaat naar retrievalpakketten.

Toepassing bij feiten na de balansdatum

De technieken die reeds besproken werden met betrekking tot de "analytical review" kunnen hier evenzeer worden aangewend. Bij een doorlopende opdracht gebeurt dit eigenlijk vanzelf al.

De in het artikel genoemde technieken vereisen een zekere kennis van de geautomatiseerde gegevensverwerking. Indien die niet aanwezig is dan zal de assistentie van computer-audit-specialisten ingeroepen moeten worden. Van meer belang dan de kennis van de automatisering is de

opstelling van de controlerende accountant zelve. Zij zullen, aldus de schrijver, een initiërende rol in dezen moeten spelen. Dusdoende wordt de computer van een bron van verwarring en ongemak een gewaardeerde medestander.

De schrijver van dit artikel is een lid van CICA's Auditing Standard Committee.

Noot: Naar onze mening wordt te eenzijdig aangegeven welke uitwerkingen met behulp van de computer mogelijk zijn, waarbij de technieken niet in een organisch verband met de overige controlemaatregelen worden geplaatst.

Noot: Het gebruik van utilities en door de cliënt ontwikkelde toepassingsprogramma's kan een inbreuk betekenen op de onafhankelijkheid van de accountant. Bij de keuze uit de alternatieve technieken zullen de voorwaarden waaronder deze kunnen worden toegepast steeds moeten worden afgewogen.

Corporate Control with distributed Data Processing and Storage - Dr. Peter Sewera
Data Report VIII (1980) No. 2, blz. 19/24 - S 532

Trefwoorden: A 50; A 12

In dit artikel wordt een vrij compleet overzicht gegeven van een bedrijfsbeheersingssysteem met toepassing van gedistribueerde gegevensverwerking en opslag. Het onderhavige bedrijf, een grote papierfabriek, laat zich typeren als een vrij kapitaalintensieve industrie met een in hoge mate gemechaniseerd produktieproces.
Het artikel is met name belangrijk omdat het in kort bestek een inzicht geeft in de invloed van deze vorm van gegevensverwerking op de organisatie en de taakverdeling tussen het centrale computercentrum en gedecentraliseerde computers (samengevat in een tabel).
De administratief-organisatorische maatregelen worden in het artikel vanuit de optiek van bedrijfsbeheersing en niet zozer vanuit de controle-optiek behandeld.

Les plans de recourement face aux situations d'urgence - André Pérès, CA
CA-magazine, août 1980 - S 539

Trefwoord: B 49

Inleiding

"Voorkomen is beter dan genezen" is de ondertitel van dit artikel over beveiligingsmaatregelen tegen voorvallen die door hun aard de voortgang van de informatieverwerking kunnen verstoren en daarmede de onderneming in een noodsituatie kunnen brengen.

Te zamen dienen de preventieve en herstelmaatregelen een verantwoorde beveiliging tegen mogelijke - voorzienbare en onvoorzienbare - rampen te leveren. Met andere woorden, de daaruit voortvloeiende schade te minimaliseren. Uiteraard dienen de maatregelen in hun samenhang economisch verantwoord te zijn (denk aan: risico-analyse).

De te treffen herstelmaatregelen dienen in een plan te worden samengevoegd, waardoor in geval van nood de te nemen beslissingen tot een uiterst minimum worden beperkt.

De doelstellingen van het herstelplan zijn:

1. Waarborgen van een zodanig snel herstel van de informatieverzorging dat de schade voor de onderneming geminimaliseerd wordt. Er is dus een relatie tussen de wenselijke snelheid en de schade door vertraging.
2. Waarborgen dat op qua aard en omvang verschillende rampen op de geeigende manier wordt gereageerd.
3. Het plan dient als informatiemiddel.

Samenstellende delen

Het plan omvat de volgende gebieden:

- programmatuur en documentatie,
- bestanden,
- personeel,
- hardware,
- specifieke formulieren.

Daar de schrijver in dit overzichtsartikel vrij indringend op de materie ingaat, terwijl het merendeel van zijn opmerkingen algemeen bekend en aanvaard is, zal hierna slechts op saillante punten worden ingegaan.

- Programmatuur en documentatie
  Afgezien van de zelf ontwikkelde programmatuur dient ook de als pakket verkregen toepassingsprogrammatuur en systeemsoftware te worden beveiligd. Het is immers niet zeker in hoeverre de oorspronkelijke leverancier nog de gekochte versie kan leveren. In hoeverre waren de pakketten toegespitst op de specifieke situatie?

- Bestanden
  De schrijver ziet deze als het centrale punt, de bestaansreden voor de automatisering. De beveiliging is een kwestie van techniek (en geld). Bijzondere aandacht dient te worden besteed aan de bewaarplaats.

- Personeel
  De situatie na de ramp dient met straffe hand te worden geleid. De herstelwerkzaamheden dienen te worden gecoördineerd door één functionaris die alle nodige beslissingen kan en mag nemen. (Overleg en afstemming tussen de diverse functies dient plaats te vinden op het moment van opzet van het plan.)

- Hardware
  Het hareware-probleem is tweeledig:
  . Hoe kan zo snel mogelijk een in principe gelijke configuratie worden verkregen?
  . Hoe kan eventueel een andere configuratie gebruikt worden?

Verwerking tijdens de herstelperiode

Bij het opstellen van het plan zal een inzicht moeten bestaan met betrekking tot de informatieverwerking tijdens de herstelperiode. De keuze van de alternatieve oplossingen kan alleen zinvol gemaakt worden als een duidelijk inzicht bestaat ten aanzien van die delen van het proces, die van wezenlijk belang zijn en die delen, die in noodsituaties tijdelijk gemist kunnen worden. Dit zal leiden tot een rubricering in prioriteitsklassen. Per klasse kan dan de behoefte aan machinetijd, doorlooptijd, omvang, maximale vertraging en dergelijke worden vastgesteld. Soms zullen noodversies van systemen nodig blijken.

De plaats waar de verwerking in de herstelperiode plaatsvindt kan

- voortvloeien uit wederzijdse afspraken met andere ondernemingen (zijn die afspraken werkelijk afdwingbaar);
- zijn een ander computercentrum binnen hetzelfde concern;
- bij een softwarebureau in gehuurde tijd plaatsvinden (is er wanneer de ramp geschiedt inderdaad vrije capaciteit aanwezig);
- zijn een gezamenlijke met anderen opgezet back-up-centrum (al of niet geoutilleerd). Een uitwerking is de zogenaamde empty shell approach, bestaande uit een leeg, voor gemene rekening opgezet computercentrum in combinatie met afspraken met de leverancier voor prompte installatie van de gewenste configuratie.

De toetsing van het plan

Er zal doorlopend op toegezien moeten worden dat het plan in ieder detail uitvoerbaar blijft.
Daarvoor is controle nodig op de volledigheid en juistheid van de back-up-bestanden, de beveiliging van de externe opslagplaats, de consistentie van het plan zelf, en de uitwisselbaarheid van de eigen en uitwijkconfiguraties.

Het verdient aanbeveling de noodsituatie en de daaropvolgende herstelprocedure van tijd tot tijd te oefenen. Voordeel: ervaring en toetsing gaan hand in hand.

Planningcommissie

Het opzetten van het plan kan het beste door een commissie geschieden, omdat

- de benodigde kennis en ervaring nodig voor het opstellen ervan zelden in één persoon is verenigd;
- de tegenstrijdige belangen, die met name in de gebruikssfeer zullen bestaan, beter kunnen worden afgewogen.

Minicomputer audit concerns - Carl R. Wolf
Edp Auditor Update, May 1980, page 16 - S 536

Trefwoord: E 13

Inleiding

Het gestelde in dit artikel richt zich op de stand-alone-toepassing van minicomputers in gedistribueerde gegevensverwerking.

Voordelen

Genoemd worden voordelen ten aanzien van:

- prioriteitsstelling bij systeemontwikkeling;
- betere, meer op het specifieke bedrijfsonderdeel toegesneden gegevensverwerking.

Nadelen

- Geen of minder keuze in standaardtoepassingspakketten.
- Beperkte uitwisselbaarheid programma's met andere machines (back-up).
- Verhoogde opleidingskosten voor programmeurs en bedieningspersoneel.
- Machinegebondenheid van programma's en van bestanden kan aanzienlijke conversieproblemen veroorzaken.
- Verlies van consistentie tussen de op verschillende plaatsen bijgehouden gegevensverzamelingen kan voorkomen.

Controle-overwegingen

- De aan gegevensverwerking inherente risico's worden mede gedecentraliseerd. Fraude, misbruik van computers, fouten en vergissingen.
- Functiescheidingen boeten aan kracht in.
- Toegangsbeveiliging en noodvoorzieningen komen in een geheel andere omgevingsinvloed.
- Het ontbreekt vaak aan wachtwoordbeveiliging.
- Onder druk van technische beperkingen kunnen toereikende ingebouwde controles en audit trails ontbreken.
- Systeemdocumentatie en ontwikkelingsstandaarden kunnen onvoldoende zijn.

Op grond van de hiervoor kort aangegeven voor- en nadelen en controle-overwegingen komt de schrijver tot een aantal aanbevelingen, die behartigingswaardig zijn. Deze aanbevelingen zijn alle van organisatorische en/of interne controle aard.

1. Er dienen algemene grondslagen en regels te worden gedefinieerd die voor de gehele onderneming gelden.
2. Er dient een goede kosten-/batenanalyse ten grondslag te liggen aan iedere aanschaf van een minicomputer.
3. Er dient een lijst te zijn van de toegelaten leveranciers voor machines en programmatuur.

4. Een algemeen voorschrift ten aanzien van de te gebruiken programmeertaal. Uitzonderingen behoeven speciale goedkeuring.

5. Een minimumvoorschrift ten aanzien van systeemontwikkelings- en documentatiestandaarden kan node gemist worden.

6. Onmiddellijk na de invoering dient een onafhankelijke controle op documentatie, functiescheidingen en noodvoorzieningenplanning te worden verricht.

De naleving van deze zes punten dient centraal te worden verricht.

Noot: Hoewel geen van de bovengenoemde zes punten wezenlijk nieuw is, dient te worden bedacht dat de zaken door de veranderde functionele verdeling en de omgeving waarin de computers worden toegepast wel zijn veranderd. Hierdoor verandert ook de aan deze punten te geven uitwerking.

NIEUWS
Automatisering
Beveiliging
Controle

door drs. H.C. Kocks

Automatisering

Op 30 januari 1981 heeft IBM het programmaprodukt SQL/Data Systema geannonceerd (SQL staat voor Structured Query Language; uit te spreken als "sequel").
Dit produkt is volgens IBM "a relational data base system". Het is ontworpen voor de volgende apparatuur: System 370 (model 138, 145, 148 en 158), de 3031, 3033-S, 4331 en 4341 of compatible processors gesupport door VSE/Advanced Functions Release 3. Zoals gebruikelijk volgen op aankondigingen commentaren en reacties. Hieronder een reactie van de "trendvolgers" van IBM onder de titel "Independents React to SQL" door Rita Shoor.

Independents React to SQL

By Rita Shoor
CW Staff

How do the independents who produce IBM-compatible high-level query software feel about SQL/DS IBM's entry into the relational software market [CW, Feb. 9]?

Whether SQL/DS is looked upon as a high-level combination query/report generator package or the first step on the road to a relational data base management system (DBMS), it was evident that all of the software houses are keeping a close watch on IBM. "Obviously, anything IBM does is competitive," summarized Bill Rabkin from Cullinane Database Systems, Inc.

Interviews with nine vendor representatives, however, left the general impression that most did not view the product as any sort of threat — at least on a short-term basis.

Many of the respondents mentioned what they considered to be two major drawbacks. First, the initial release of SQL/DS, scheduled for February 1982 availability, is limited to the DOS market. And "the DOS environment doesn't take advantage of a relational model," according to the spokesman for Software AG.

The second perceived disadvantage is that SQL/DS, like IBM's Query by Example (QBE), works with the data base via an extraction facility rather than through a direct interface. This leads to problems with data redundancy and incompatibility and is, in fact, a "very antiquated" way of handling queries against the data base, Software AG noted.

While the immediate impact of SQL/DS on the independents was not expected to be significant, the firms were less certain of how to predict the long-term effects of IBM's announcement.

Frank Fish, vice-president of marketing for Mathematica, Inc.'s Products Group (MPG), speculated that the product's official release may have been a move intended to delay the purchase of independent software by current IBM customers. However, he predicted that the long-term effect might be positive for IBM's competitors since it increased market awareness of non-procedural languages with an end-user orientation.

Software AG also called SQL/DS a "boost to the independents" and claimed the announcement signified a reaffirmation that IBM realizes it needs an alternative to IMS.

Another opinion was offered by a product manager from Cincom Systems, Inc. Rather than viewing SQL/DS as a high-level query facility, "we think IBM is delivering a prototype of the system that will eventually replace IMS and DL/1," he said. He predicted a long-term impact on the DBMS market with little or no short-term impact for query software vendors.

COM, 23 maart 1981

In Compact nr. 22 is een artikel opgenomen (pag. 44) over de (on)bekwaamheid van de programmeur. Voor betere opleiding en permanente educatie werd gepleit. Hoe die opleiding er echter wel uit moet zien, lijkt niet eenvoudig. Dat bleek tijdens een gehouden bijeenkomst van computerwetenschappers (wat dat ook moge zijn) te Melbourne. Het volgende (verkorte) artikel geeft een impressie van hoe "computerwetenschappers" een programmeursopleiding invullen.

Forum oneens over programmeuropleiding

Er zullen in de jaren tachtig meer programmeurs nodig zijn, aldus een forum van prominente computerwetenschappers tijdens een onlangs in Melbourne gehouden bijeenkomst. Men was het er echter niet over eens wat voor soort mensen er moeten worden gerecruteerd, hoe zij moeten worden voorbereid en opgeleid of wat zij zullen gaan doen.

Het probleem is een opleidingsprobleem met vele facetten, aldus dr. Heinz Zemanek, voorzitter van het forum en IBM fellow in Wenen. Zowel jongere als oudere medewerkers moeten worden opgeleid om met computers te werken en zij moeten zijn voorbereid op veranderingen, zo voegde hij hieraan toe.
Een goede universitaire vooropleiding zou programmeurs helpen zich aan te passen aan de veranderingen, die onvermijdelijk zullen plaatsvinden in de loop van hun leven, terwijl degenen, die alleen maar een vakopleiding hebben gehad, hiertoe wellicht niet in staat zullen zijn.
Programmatuuronderhoud zal altijd noodzakelijk blijven. Voor dat werk, aldus dr. Herbert R. J. Grosch, consultant en voorheen direkteur van de Association for Computing Machinery, zou men willekeurige mensen kunnen nemen en ze een snelle opleiding kunnen geven.

Voor het meer creatieve werk zijn echter mensen met een universitaire vooropleiding en een goede theoretische ondergrond nodig, zo vonden de leden van het forum.
„Programmeren is niet anders dan elke willekeurige andere intellectuele activiteit", zo betoogde professor W. Turski van het Instituut voor Informatica te Warschau. "Om dit werk goed te kunnen doen, moet je het eerste leren", zo vond hij. Hij beschreef programmatuuronderhoud als "mensonwaardig werk".
Hoewel sommigen uit het gehoor vragen stelden over het gebruik van programmapakketen en andere technische oplossingen, zoals report generators en vraagtalen om de hoeveelheid Colbolcode, nodig voor het verrichten van bepaalde taken, te verminderen, werd hierop alleen maar ingegaan door H. Remus van IBM's Teresa laboratorium.

De Automatisering Gids, 11 februari 1981

EZ-subsidie van f 2,5 mln voor automatisering in midden- en kleinbedrijf

Ondernemingen uit het midden- en kleinbedrijf, die in een samenwerkingsverband van minimaal vijf bedrijven uit dezelfde branche willen gaan automatiseren, kunnen daarvoor binnenkort financiële steun gaan aanvragen bij het ministerie voor Economische Zaken.

Op het ministerie wordt gewerkt aan een beschikking, die na goedkeuring door minister Van Aardenne over enkele weken zal worden gepubliceerd in de Staatscourant. Deze beschikking zal een subsidieregeling voor automatiseringsprojecten in het midden- en kleinbedrijf omvatten. Bedrijven met automatiseringsplannen krijgen daarin de mogelijkheid voorgespiegeld, 30 tot 40% van de kosten voor een zogenaamde haalbaarheidsstudie van hun project, en van de kosten voor de ontwikkeling van de benodigde software bij het ministerie te declareren.

Maximaal wil het ministerie van EZ een bedrag van f 300.000 subsidiëren. Deze subsidiemogelijkheid geldt niet voor de zogenaamde hardware. Dat houdt in, dat de bedrijven de kosten voor de benodigde apparatuur geheel voor eigen rekening zullen moeten nemen. Voor de gehele regeling heeft EZ in 1981 een totaalbedrag van zo'n f 2,5 mln beschikbaar.

De regeling valt in twee delen uiteen. De samenwerkende ondernemingen uit het midden- en kleinbedrijf kunnen ten eerste een subsidie van 30% krijgen op de kosten van een voorstudie naar de haalbaarheid van het voorgestelde automatiseringsproject.
Deze studie moet duidelijk maken, dat het project een zinvolle zaak is, die past binnen de mogelijkheden van de betrokken bedrijven, aldus een woordvoerder van het ministerie. Op dit punt denkt EZ aan een maximumsubsidiebedrag van f 50.000.

Als deze studie positief uitvalt, kan vervolgens in de tweede fase, die van de daadwerkelijke uitvoering van het project, 30 tot 40% van de softwarekosten worden gesubsidieerd. Dit geldt ook voor de kosten die moeten worden gemaakt, als een extern softwarebureau deze programmatuur (dat zijn de bedienings- en toepassingsinstructies voor de apparatuur) moet gaan ontwikkelen.
Hierbij geldt een maximumsubsidiebedrag van f 250.000 tot f 300.000. Het totale project mag het ministerie maximaal f 300.000 gaan kosten. Is er al geld beschikbaar gesteld voor de eerder genoemde voorstudie, dan moet dit bedrag van die f 300.000 worden afgetrokken.

In het regeringsstandpunt van september vorig jaar over het rapport van de Commissie-Rathenau (die de gevolgen van de invoering van microelektronica in ons land had bestudeerd) werden dit soort subsidie-activiteiten voor het midden- en kleinbedrijf al aangekondigd.

Het Financieele Dagblad, 5 maart 1981

Annonceringen/Nieuwtjes

Softwaregenerator uit Engeland

Twee Engelsen zijn er in geslaagd, om een programma te ontwikkelen, waarmee een computer in alledaagse spreektaal kan worden geprogrammeerd. De heren D. James en S. Bambury hebben in totaal 18 maanden aan hun systeem gewerkt. Als naam hebben zij gekozen voor "The last one", omdat dit programma in principe het laatste is, wat ooit door een mens geschreven hoeft te worden.
Het programma begint met een vraag-en-antwoord spelletje, om de wensen van de gebruiker te inventariseren. Aan de hand van de hieruit komende gegevens, wordt binnen enkele minuten een foutloos computerprogramma gegenereerd. Op het moment is het systeem nog niet geschikt voor commercieel gebruik, omdat nog steeds een goed opgeleide systeemanalist nodig is, om de juiste antwoorden op de vragen te formuleren.
Beide ontwerpers hopen echter, binnen een periode van zes maanden, het programma zover verbeterd te hebben, dat ook een leek het kan gebruiken. Dat "leek" moet dan worden opgevat als iemand, die wel enige ervaring heeft gehad met een computer. James en Bambury zijn van mening, dat hun "last one" de bestaande softwaregeneratoren verre overtreft.
De marketing van het systeem zal worden verzorgd door een nieuw op te richten firma, de de naam DJ-AI zal gaan dragen. Een en ander zal pas in de tweede helft van dit jaar worden geëffectueerd.

De Automatisering Gids, 11 maart 1981

Miljoenenschuld brengt Infotech op rand van afgrond

Infotech, een Britse onderneming op het gebied van cursussen, conferenties en publikaties, zal binnenkort officeel failliet worden verklaard. De 113 medewerkers hebben reeds ontslag aangezegd gekregen. De financiële schuld van Infotech bedraagt momenteel zo'n vier miljoen gulden.

Computable, 20 februari 1981

Pergamon Press is nieuwe eigenaar van Infotech Ltd

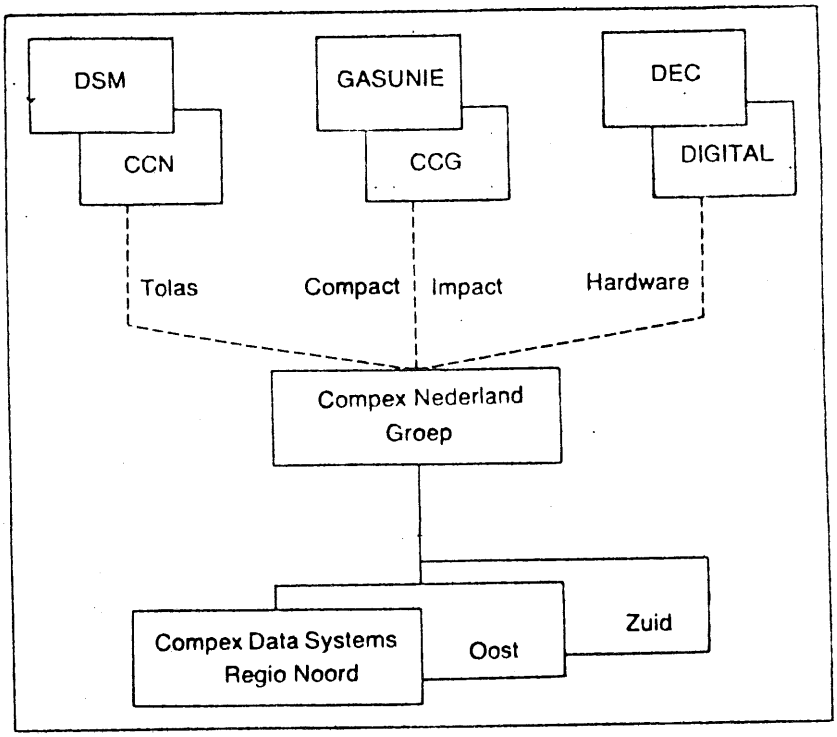
Doorgaan met derde van staf

Infotech Limited, de Britse organisator van informaticaconferenties die door een miljoenenschuld ten dode leek te zijn opgeschreven, is gered - althans voor een deel - door het Engelse uitgeversconcern Pergamon Press. Het bedrijf zal, zo schrijft het weekblad Computer Talk, in sterk gestripte versie doorgaan.

Compex Data Systems verwerft exklusieve rechten van Compact

Bedrijfsinformatiesysteem op Dec Datasystem 500

"We streven naar totaaloplossingen op minisystemen. De nadruk ligt op de programmatuur met de apparatuur in de staart van de oplossing." Deze woorden van J. Baay, commercieel directeur, en J.L. van der Woude, algemeen directeur van Compex Data Systems geven inhoud aan de bedrijfsfilosofie van het met drie regiocentra in het oosten van ons land opererende systeemhuis. De Oem-leverancier van Digital-apparatuur fungeert tevens als programmatuurhuis voor IBM, Honeywell Bull, Univac en H-P systemen. De 75 medewerkers van de Compex Groep bezitten gemiddeld 9,1 jaar automatiseringservaring en tien procent van het personeel is academisch geschoold. Aan de totale omzet van vijftien miljoen gulden werd door de programmatuurhuisactiviteiten bijna zeven miljoen bijgedragen. Gat in de markt volgens Compex is de verkoop van minisystemen via de kantoorboekhandel met serviceverlening vanuit de eigen regiocentra.



Computable

PTT houdt proef met Intelpost

In de omgeving van Amsterdam is de PTT met Intelpost een proef gestart naar de bestemmingen Londen en Toronto.
Intelpost is een internationale dienstverlening die schriftelijke berichten snel over grote afstanden kan vervoeren, doordat zij gebruik maakt van facsimile apparatuur.
De koppeling van telecommunicatietechniek aan de snelle postale distributie maakt het mogelijk om de berichten, die worden aangeboden in Amsterdam, op dezelfde dag af te leveren in Londen en Toronto. Intelpost kan alle vormen van schriftelijke informatie, tot maximaal A-4 formaat, verzenden, zoals overzichten, grafieken, geschreven of getypte brieven etcetera.
Er wordt gebruik gemaakt van een Rapicom 500 T/R facsimilesysteem, waarvan de transmissiesnelheid ongeveer een minuut, per A-4 vel, bedraagt.

Tijdens de proef in de regio Amsterdam kan men de berichten op zes verschillende postkantoren aanbieden. Van daaruit worden zij vervoerd naar het Intelpostcentrum aan de Oosterdokskade. Via de facsimile apparatuur worden de berichten dan overgebracht naar de Intelpostcentra in Londen en Toronto. De afzender ontvangt het originele stuk retour, terwijl de overgebrachte copie per expresse bij de buitenlandse geadresseerde wordt afgeleverd. Het hele gebeuren kan uiteraard ook plaatsvinden vanuit Londen en/of Toronto, waarna de ontvangst geschiedt in Amsterdam.
De proef met Intelpost duurt voorlopig tot eind dit jaar en zal gedurende deze periode worden uitgebreid met een aantal bestemmingsplaatsen. ●

De Automatisering Gids, 11 februari 1981

De strijd om het eigendom van software gaat onverminderd voort. In het volgende artikeltje worden een aantal aspecten inzake dit onderwerp aangeroerd. Echter zonder dat tot een conclusie wordt gekomen. Eenvoudig is de materie dan ook geenszins.

Who owns software?

Computer technology is outpacing lawmakers and raising unique issues with respect to fraud, criminal evidence, protection of privacy, copyright, etc. The size of the challenge can be gauged by the fact that a satellite hovering 22,000 miles above Europe could beam computer data to 38 countries. Each country operates its own laws, mostly making no specific reference to computers and mostly backed by very little case law to indicate how they apply to computers.

There is a consensus that something needs to be done. But the experts cannot agree what the problems are, let alone how to tackle them. Consider how to interpret copyright law when it comes to computer software, the programming instructions that tell a computer what to do.

In Britain, a committee was set up in 1973 to consider copyright law generally. The committee issued its report in 1977. It proposed that the law should state that copyright applies to computer software. Four years have passed and nothing has emerged, not even an oft-promised green paper from the government.

Meanwhile, the problems are growing. Easily copiable software has become more readily available: for example, standard software packages, recorded on magnetic tape, can be bought on the high street and are little harder to copy than a much less valuable tape recording of somebody's music.

The growing use of data bases is also causing problems. Consider a hypothetical case. Suppose a famous chef writes a recipe book; a computer programmer records the book in computerised form and writes software to turn the book into a data base that can be interrogated; a gourmet then quizzes the computer. It is

clear neither whether the computer's answers are covered by copyright nor, if they are, who owns the copyright. Does it belong to the chef, the programmer, the gourmet or some combination of the three?

Confusion is further increased because some of the technical jargon used in the computer industry—words like "editing" and "compiling"—has a totally different meaning to laymen and copyright lawyers.

Mr Alistair Kelman, a British lawyer, has proposed some ingenious legal terminology for drafting new codes to extend copyright protection to computer software. The most pressing problem he tackles is how to trace the ownership of computer software through all the technical steps of translation it may undergo when it is plagiarised. The end-result can look quite different to the original but still be effectively the same.

To the layman, translation might sound like a good word to describe the processes that go on. Yet some of these processes are quite different from translating a novel, which confers rights under copyright law. Mr Kelman proposes resuscitating an old word used by alchemists, transmutation, to describe computer translations.

His proposals have won sympathy from a number of leading European computer experts. But he has his critics. Some fear that radical changes in the law, made by parliamentarians who only half-understand the issues, may only make matters worse. Others argue that the shortcomings of existing law have been grossly exaggerated. None the less, there is growing evidence that software piracy is beginning to become a real problem.

Economist, 31 januari 1981

Beveiliging

Misbruik van computers blijft de aandacht trekken van veel mensen. Steeds wordt het oog gericht op een nieuwe categorie potentiële computermisbruikers. De laatste tijd zijn de programmeurs nogal negatief in de belangstelling (zie onder Automatisering en Compact nr. 22). Volgens onderstaand (verkort) artikel maken vooral programmeurs illegaal gebruik van de computer.

Illegaal gebruik van computers

Het misbruik maken van door de werkgever geboden faciliteiten komt waarschijnlijk in vele beroepen in meer of mindere mate voor. Bij programmeurs schijnt het echter schering en inslag te worden, getuige de uitspraken van een vooraanstaand softwaredeskundige in de Verenigde Staten.

Steeds meer programmeurs gebruiken clandestien de centrale verwerkingseenheid van hun werkgever voor het ontwikkelen van 'zwarte' programmatuur voor de huis- en microcomputermarkt, zo verklaarde een hoogleraar, dr. R. Stumpf, die tevens medewerker is van een adviesbureau, onlangs tijdens een bijeenkomst.

"Programmeurs gaan steeds meer 'zwart' programmeren", aldus dr. Robert Stumpf, lid van de faculteit van de California State Polytechnic University van Pomona. "Indien iemand een controle zou uitvoeren bij een paar van de grote computerinstallaties in Zuid-Californië en elders, dan vermoed ik dat je heel wat verwerkingstijd zal tegenkomen, die niet gemakkelijk kan worden verantwoord".

Vele van de goedkope programmapakketten, die momenteel verkrijgbaar zijn in de verschillende hobby computerwinkels in de Verenigde Staten, worden wellicht samengesteld door programmeurs, die een volledige dagtaak hebben, maar die hebben besloten om wat bij te verdienen, aldus Stumpf in een voordracht tijdens de onlangs gehouden Mini/Micro conferentie en expositie.

Deze programmeurs ontwikkelen gewoonlijk hun 'zwarte' programmatuur met behulp van de computer van hun niets vermoedende werkgever. Vervolgens verkopen zij de kant en klare programma's, die zij vaak hebben geschreven tijdens de normale kantooruren, op de vrije markt.

Commentaar:

In de aanhef van het artikel wordt gesproken over "het misbruik maken van door de werkgever geboden faciliteiten". De vraag is of dan nog van misbruik kan worden gesproken. Zolang de accountant met automatisering te maken heeft, beklemtoont hij de functiescheiding in een automatiseringsorganisatie tussen ontwikkeling (inclusief programmering) en produktie. Als deze functiescheiding aanwezig is en de procedures en voorschriften gericht op handhaving van die functiescheiding worden nageleefd, zijn situaties zoals geschetst in het artikel uitgesloten. Als kop van jut wordt hier m.i. onterecht de programmeur gebruikt. Veeleer dient de organisatie waarin die programmeur functioneert aan de kaak te worden gesteld.

Beveiligen Noodzaak

Beveiligen!! Een veel gebruikt woord in automatiseringskringen. Als deze kreet wordt geslaakt, komen uit diverse richtingen de volgende (vragende) antwoorden: Waarom?; Hoe?; en Wat zijn de gevolgen? Logische vragen die niet altijd even gemakkelijk zijn te beantwoorden vanwege het feit dat "het altijd nog goed is gegaan".
Is eenmaal het stadium bereikt dat de noodzaak van beveiligen wordt ingezien dan wordt iedereen overspoeld met procedures en voorschriften waaraan men zich "vanaf nu!" moet houden. Aan acceptatie van regels en voorschriften wordt gedaan door te stellen dat "het moet". In de praktijk kwam ik met betrekking tot die acceptatie het volgende tegen. Subtiele interviews en beschrijvingen van ongewenste situaties op een zodanige wijze dat de slogan "Beveiligen is noodzaak" kracht werd bijgezet.

Hier volgt de eerste van een serie die in volgende "Compacts" wordt voortgezet onder de leuze "Beveiligen Noodzaak". Het jaargetijde is niet maatgevend voor de artiesten in het stuk, maar U moet maar rekenen "speculaas is ook het hele jaar door verkrijgbaar!".

Vraaggesprek met Sinterklaas

De heer Sinterklaas is een exporteur van speelgoederen en aanverwante artikelen. Hij verblijft meestal in Spanje. Wordt echter begin december veelvuldig in Nederland gezien. Hij is specialist in het doorbreken van beveiligingsmaatregelen. Hij ziet altijd weer kans om zwaar beveiligde huizen binnen te dringen, om zijn goederen ongemerkt af te leveren.
Hij leek ons de aangewezen man om enige vragen over beveiliging te beantwoorden.

vraag: Wat zijn zo Uw gedachten over beveiliging?
antw.: Zoals U weet, zie ik al zo'n 1300 jaar kans om door alle beveiligingen heen te breken. Voor mij hoeft het dus niet. Ik realiseer mij echter dat het voor gewone stervelingen nuttig kan zijn om tegen de hebzucht van andere stervelingen beveiligd te worden.

vraag: Kunt U uit de historie wat voorbeelden van beveiliging geven?
antw.: Ik zou als voorbeeld de ommuurde steden willen aanhalen. Wat te denken van de Chinese muur, de Siegfried linie, de Maginot linie, de Atlantik wal, ...

vraag: Mijnheer Sinterklaas, dit zijn allemaal voorbeelden van beveiligingen die niet gewerkt hebben, dit komt wat negatief over en kan nooit de bedoeling van dit artikel zijn. Kunt U ook wat voorbeelden geven van beveiligingen die wel gewerkt hebben?
antw.: (na een lange pauze)
Ik heb in Europa een zwaar beveiligd Oost-blok zien ontstaan, gevolgd door een even zwaar beveiligd West-blok. Dit schijnt te werken. Het idee van een bewaakt blok binnen "'t suffertje" was dus niet helemaal nieuw voor mij. Het spreekt mij aan dat voor het beveiligen van dit blok geen geweld gebruikt wordt.

vraag: Had U anders verwacht? U weet dat onze medewerkers bij 't suffertje buitengewoon vreedzaam zijn.
antw.: (deze vraag waarschijnlijk niet helemaal begrepen)
De vreetzaamheid van de suffertjes is mij genoegzaam bekend. Ik vertoef namelijk wel eens in Uw kantine. Verbazingwekkend hoe snel Uw mensen reageren op het uitspreken van het woordje "TOSTI"! Ik zou .....

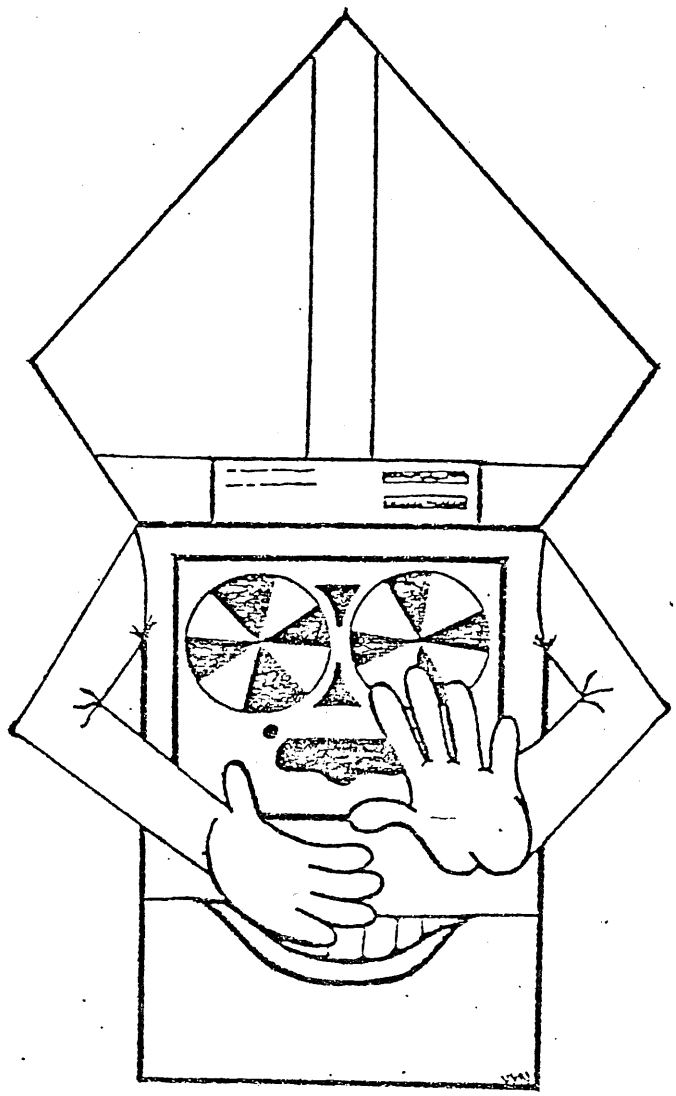
vraag: Mijnheer, wij dwalen af van het onderwerp beveiliging.
Bent U het eens met de stelling dat beveiliging niet nodig zou zijn als de mensen elkaar beter zouden verdragen?
antw.: Interessante zienswijze! Ik zou hier graag mijn paard als voorbeeld stellen.

vraag: Uw paard?
antw.: Ja, reeds eeuwenlang draagt hij mij naar verre verten. Ik zou mij geen ver dragender schepsel voor kunnen stellen.

vraag: Zou U een manier weten om ongemerkt het bewaakte blok binnen te dringen?
antw.: Eenvoudig. De verantwoordelijke man(nen) binnen Produktie speel ik mijn Zwarte Piet toe. Terwijl ieder druk bezig is die Zwarte Piet de deur uit te werken, ben ik ongemerkt waar ik wezen wil.
Ik heb trouwens voor 't suffertje het gehele jaar door een Zwarte Piet op "stand by" staan, zodat men elkaar in voorkomende gevallen de Zwarte Piet toe kan spelen. Deze "stand by"-regeling is nog niet goedgekeurd door mijn V.C.. Tot gisteren was, op mededelingen hierover, een embargo van toepassing.
Ik herinner mij .....

vraag: Wij dwalen af. Ik heb geen vragen meer. Heeft U de suffertjes nog iets te zeggen?
antw.: Ja.
1. Het aantal Zwarte Pieten is beperkt. Maak van hen dus spaarzaam gebruik.

2. Geloof niet langer in sprookjes. Geloof desnoods niet langer in Sinterklaas.
Maar blijf geloven in: BEVEILIGEN IS NOODZAAK.



BEVEILIGEN

NOODZAAK

Controle

Deze keer gewijd aan de third-party review. Een in Nederland vrij onbekend verschijnsel. In Amerika, zoals blijkt uit onderzoekresultaten, steeds meer toegepast. Gezien de steeds verder toenemende internationalisering van het accountantsberoep is gemeend hieraan aandacht te moeten schenken.
Maar wat is het nu eigenlijk, third-party review.
Een onafhankelijke accountant (niet de accountant van de onderneming waar in service wordt verwerkt) onderzoekt het servicebureau en geeft in een rapport zijn bevindingen weer ten behoeve van accountants van cliënten die gebruik maken van de diensten van het servicebureau. Dat het in de Amerikaanse beroepsuitoefening meer voorkomt blijkt wel uit het feit dat er door het AICPA regels voor zijn opgesteld. Onder andere regels voor de rapportering. Die regels zijn:

Content of Third-Party Report on Service Center Processing and Accounting Control. The report') of the third-party auditor should include the following:

1. A statement as to the scope of the examination and as to whether both a review of the system and tests of compliance were included.
2. The service center's system description, including the controls. This should either be included or incorporated by reference in the report.
3. The time period covered by the examination.
4. An opinion as to whether or not the system and system controls conform to the service center's system description during the period under review.
5. A disclaimer of opinion as to the adequacy of accounting control with respect to each user's application and with respect to the accounting controls of the service center itself.
   (Conclusions concerning these matters can be formulated only by the user auditor upon consideration of both his clients' internal accounting controls and those at the service center.)
6. Comments concerning unsatisfactory conditions in the accounting controls in the system and recommendations for correction. This would include reporting the absence or non-operation of controls in the following categories:
   a. Controls which the service center's management have represented are in existence but which are either not in existence or not in operation.
   b. Controls which the service center's management have not represented are in existence but which, in the judgment of the third party reviewer, are desirable.

') Guidelines for this form of report are contained in Statement on Auditing Standards No. 1, sections 640.17-640.18, pp. 180-181.

In 1978 zijn de resultaten gepubliceerd van een door het EDP auditing standards subcommittee van het AICPA ingesteld onderzoek naar de kwaliteit van de rapportering van de third-party review. De conclusie laten we hier volgen.

Summary and Conclusion

The survey made by the EDP auditing standards subcommittee has produced some interesting results. Although the extent of third-party reviews performed or the use of the reports by others could not be quantified, the survey indicated a substantial use of the third-party review. The auditors using the reports evaluated them and performed additional work where necessary but did not have any basic problems with the concept itself. These auditors, however, did indicate a need for the third-party auditors to clarify or emphasize certain aspects of the report. The auditors responding to the survey reported a benefit and need which indicated that the third-party review is an important concept, and, if used properly, it can be effective and beneficial. This, together with the growth in service centers' size and complexity, and the increase in the types and extent of transaction and balance processing services, indicates that the third-party review concept will become more important in the future.

Het third-party review rapport wordt als zeer belangrijk ervaren omdat het in feite de basis is waarop de accountant (van de cliënt die in service laat verwerken) zijn (eventueel) aanvullende werkzaamheden zal baseren. Het is de Amerikaanse accountant niet toegestaan in zijn accountantsrapport op te nemen dat hij gebruik heeft gemaakt van de resultaten van een onderzoek uitgevoerd als third-party review. De desbetreffende accountant is volledig verantwoordelijk voor zijn eigen jaarrekeningcontrole. In de Nederlandse opvatting zal dat niet anders zijn.

In de Journal of Accountancy van augustus 1980, geeft D.M. Stevens, CPA, in zijn artikel "Improving third-party review reports in audits of service-center-produced records" een aantal methoden om de "reports" te verbeteren. Hij omschrijft het doel van zijn artikel als volgt:

This article explores several methods of improving third-party review reports. It summarizes the reporting standards that can be derived from the literature published by the American Institute of CPA's and evaluates some actual reports to show to what extent these standards are currently being met.

Gedeeltelijk is het artikel van Stevens hieronder opgenomen.

Reporting standards

Statement on Auditing Standards no. 3, The Effects of EDP on the Auditor's Study and Evaluation of Internal Control, requires auditors of clients using EDP to perform a preliminary review of

- The flow of transactions through the accounting system.
- The extent to which EDP is used in each significant accounting application.
- The basic structure of accounting control.

Auditors need not test or rely on the internal controls that may exist within the computerized portions of the accounting system, but, in order to comply with generally accepted auditing standards, they must understand these three elements. Audit clients using in-house computer facilities are no different from those using the services of an outside data center: the requirement for the preliminary review and the need for understanding remains the same.

Since many companies may use the same outside data center, many auditors should obtain information concerning its operations. In such cases, the AICPA audit guide on Audits of Service-Center-Produced Records provides for a third-party review. The third-party reviewer performs work for the benefit of all auditors concerned with a given data center and issues a basic two-part document consisting of a descriptive supplemental report and an opinion on the reliability of the supplemental report. This document can then be used by all auditors concerned with the reviewed data center to attain the pre- liminary understanding required by SAS no. 3.

While the audit guide is quite specific concerning the form and content of the third-party reviewer's opinion, it provides only limited guidance for the form and content of the supplemental report. For the supplemental report to be useful the third-party reviewer must remember that he is to report for the benefit of other auditors who are making a preliminary review. He should therefore consider reporting sufficient information to provide an understanding of the three elements defined in SAS no. 3.

The third-party reviewer must judge what specific information is to be included in the supplemental report. Chapter 2 of the AICPA audit and accounting guide on The Auditor's Study and Evaluation of Internal Control in EDP systems provides separate lists of items which an auditor might consider in order to understand each of the three elements. However, because these lists are written for the benefit of all auditors, they cover information obtainable from individual clients as well as that available from the outside data center. The information needed to understand the extent of EDP use can generally be obtained from the client and therefore need not be addressed in the third-party reviewer's supplemental report. The ten factors listed in the guide (see figure 1) as essential to understanding the flow of transactions can generally only be obtained at the outside data center and therefore should be considered for inclusion in the supplemental report. The guide lists nine control questions in its discussion of the basic structure of accounting controls (see figure 2), that should be answered in the course of a preliminary review: the supplemental report should provide information concerning these questions.

In sum, third-party review supplemental reports should help auditors understand the flow of transactions and the basic structure of accounting control at a given data center when the reports provide the information called for in chapter 2 of the AICPA audit and accounting guide. Of course, certain factors and questions may be deleted or added to adequately describe the characteristics of a particular data center under review.

Figure 1 [1])

Flow of transactions

To understand the flow of transactions, the auditor might consider, but not necessarily limit attention to, the following factors:

1. Applications documentation
2. Activities and related source documents that start the flow of transactions
3. Non-EDP processing applied to the source documents
4. Conversion of data into machine-sensible form
5. Flow of machine-sensible transactions through significant accounting applications
6. Master files that may be used to supply additional information to support the flow of transactions
7. Procedures for the correction of errors
8. Output files that are created, or master files that are updated, as part of the processing of data
9. Output reports produced for significant accounting applications
10. Non-EDP processing of output reports

---

[1]) Source: Computer Services Executive Committee, The Auditor's Study and Evaluation of Internal Control in EDP Systems (New York: AICPA, 1977), pp. 10-11.

Figure 2[1])

Basic structure of accounting control

During the preliminary phase of the review, the auditor should seek answers to the following types of questions:

1. Do organizational controls within the data processing department seem to provide for adequate supervision and segregation of functions within EDP and between EDP and users?

2. Are there procedures that appear to provide controls over systems development and access to systems documentation?

3. Are there apparent controls over program and systems maintenance?

4. Do there appear to be controls over computer operations, including access to data files and programs?

5. Are there controls that seem to assure completion of file reconstruction and processing recoveries?

6. Do internal auditors apparently become involved in the review and testing of EDP accounting controls?

7. Do input controls provide reasonable assurance that data received for EDP processing have been properly authorized, converted into machine-sensible form and identified and that data have not been lost, suppressed, added, duplicated or otherwise improperly changed?

8. Do processing controls provide reasonable assurance that EDP has been performed as intended for the particular application; that is, are all transactions processed as authorized, with no authorized transactions omitted and no unauthorized transactions added?

9. Do output controls assure the accuracy of the processing result and that only authorized personnel receive the output?

---

[1]) Source: Computer Services Executive Committee, The Auditor's Study and Evaluation of Internal Control in EDP Systems (New York: AICPA, 1977), pp. 12-13.

Evaluation of existing reports

Ten third-party supplemental reports issued during the two years ended September 1978 were reviewed to determine if the factors and control questions listed in figures 1 and 2 were addressed. The reports were selected on the basis of their availability (the limited distribution and confidential nature of third-party review reports impedes sampling) and the desire to include reviews by larger accounting firms. Nine of these reports were prepared by six large firms. The majority of the data processing services described were provided to the banking and savings and loan industries, but consumer finance, credit union and stock exchange services were also represented. Each report was evaluated based on the information it provided concerning the ten factors and nine questions suggested in the audit and accounting guide; no attempt was made to evaluate the scope or clarity of information.

Although the sample size was small and results may not be representative, this evaluation does demonstrate a broad range of supplemental report coverage. Less than half of the ten reports appeared to address all the factors and control questions listed. The results also suggest that third-party review reports frequently do not provide information on the flow of machine-sensible transactions through described applications, the types of files that are maintained and used by the applications and the processing controls within the applications.

Testing

Third-party review supplemental reports could be improved and auditors would be more assured of receiving reports that provide an understanding of the flow of transactions and basic structure of accounting control in off-site data processing systems. However, the question of whether the controls identified in the report could be relied on would still remain.

The assessment phase of the review as discussed in SAS no. 3 is to be performed entirely by auditors who receive and use third-party review reports in the conduct of their engangements. They must consider both the information provided in the third-party report and information gathered directly from their clients to develop the most cost-effective audit approach. While the third-party reviewer performs certain tests to ensure that the supplemental report is reasonably accurate, these tests may not address the full period under audit. The mere fact that a third-party report is received does not mean auditors can rely on certain data center or application system controls.

A wider scope of testing may be necessary for this purpose. Third-party review reports would be more useful if they identified cost-effective tests that could be performed at the data center in order to allow reliance. If a broader scope of testing is desired, auditors using third-party reports could ask third-party reviewers to consider this need in their engagement planning.

EXTERNE CURSUSSEN 1981

door D. Steeman en H.J.M. van der Wielen

Het lijkt ons goed om U bekend te maken met het feit dat de AC-groep externe cursussen verzorgt. Hieronder volgt de toelichting zoals deze in onze brochure is weergegeven.

Inleiding

In voorgaande jaren organiseerden wij cursussen "Automatisering en Controle" (A&C). Doelgroep vormden voornamelijk de medewerkers van interne accountantsdiensten van onze cliënten.

Geleidelijk is gebleken dat ook functionarissen vanuit de gebruikershoek en vanuit de automatiseringsdiscipline belangstelling hebben voor deze cursussen.
Tevens is gebleken dat de ingangskennis op het gebied van de Administratieve Organisatie (AO) en Interne Controle (IC), welke door ons voor het doelmatig volgen van de A&C-cursussen noodzakelijk wordt geacht, veelal niet aanwezig en ook moeilijk te verkrijgen is.

In deze lacune wordt thans voorzien door een vijfdaagse cursus Inleiding Administratieve Organisatie, welke is ontwikkeld door de Organisatiegroep van KKC.
In deze cursus neemt de interne controle een belangrijke plaats in. Deze cursus wordt thans aangeboden als voorloper van de A&C-cursussen, waarvan wij ook dit jaar weer twee cursuscycli organiseren. De cursus kan ook heel goed worden gevolgd door functionarissen in het proces van informatieverzorging, waar aspecten van AO en IC aan de orde komen.

Ook de A&C-cursussen zijn verder vernieuwd en wel in de richting van Data Communicatie en Data Base en de daaruit voortvloeiende geïntegreerde verwerking.
Dit moge blijken uit de door medewerkers van The Plagman Group te verzorgen cursussen "Data Base Concepts for Auditors and Audit procedures in the Data Base Environment" en de geheel door de AC-groep ontwikkelde cursus "Controle bij geïntegreerde gegevensverwerking".

Als voorloper van de cursus AO hebben wij het doelmatig geacht de cursus Boekhouden, welke wij reeds enige malen als in house-cursus hebben verzorgd, thans ook open te stellen voor individuele inschrijving door personeel van cliënten. Hier denken wij met name aan functionarissen in automatiseringsafdelingen die het vak Boekhouden in hun opleiding tot programmeur of systeemanalist vaak onvoldoende gedoceerd krijgen.

Wij verwachten onze cliënten met dit programma van dienst te kunnen zijn en houden ons voor eventuele vragen gaarne beschikbaar.

D. STEEMAN

Korte beschrijving per cursus

Boekhouden (3 dagen)

Bijbrengen van de beginselen van het boekhouden, in het bijzonder bedoeld voor diegenen die met dit vak in hun opleiding nooit kennis hebben kunnen maken.

Administratieve Organisatie (5 dagen)

Presentatie van uitgangspunten van de AO in de verschillende bedrijfstypologieën en non profit instellingen alsmede in de informatiecycli binnen het informatieverzorgend systeem, toegespitst op de aspecten van betrouwbaarheid, tijdigheid en doelmatigheid.

Aanpak Automatisering in een projectorganisatie
(5 of 4 dagen naar keuze)

In een vijfdaagse cursus wordt - in het kader van het door de Organisatiegroep van KKC ontwikkelde projectbeheersings- en ontwikkelingssysteem PROBOS - een casus uitgewerkt, welke zich richt op de werkzaamheden, die in de verschillende fasen van een automatiseringsproject worden uitgevoerd.
De cursisten krijgen door het werken aan de casus inzicht in de problemen, welke zich bij de organisatie van de bouw en de realisatie van een nieuw systeem voordoen en kunnen daardoor als gebruiker meewerken c.q. als accountant zich op de juiste manier opstellen ten opzichte van een ontwikkelingsteam of een automatiseringsafdeling.

Daarnaast zullen een aantal korte theoretische inleidingen gehouden worden om de benodigde kennis over te dragen.
Tijdens de cursus wordt via handouts een documentatie van het systeem PROBOS opgebouwd.

Computer Control & Audit (2 x 3 dagen)

Het eerste deel van drie dagen is gebaseerd op de Computer Control Guidelines van het Canadian Institute of Chartered Accountants en richt zich op de betekenis en doelstellingen van maatregelen van interne controle in de automatiseringsorganisatie en de geautomatiseerde informatiesystemen.
In aansluiting hierop wordt in deel 2 met behulp van de Computer Audit Guidelines een techniek behandeld voor de beoordeling van de opzet en het nagaan van de goede werking van het stelsel van interne controle en de vaststelling van eventuele tekortkomingen.

The Data Base Environment
Concepts for Auditors (2 dagen)
Audit and Control course (3 dagen)

Gezien de toenemende betekenis van data base voor de informatieverzorging en derhalve voor de accountant dienen accountants zich de problematiek rond deze vorm van gegevensorganisatie en de consequenties daarvan op de administratieve organisatie geleidelijk eigen te gaan maken.
De know how van The Plagman Group die deze cursus voor ons verzorgt staat er borg voor dat de meest recente ervaringen uit de Verenigde Staten aan de deelnemers ter beschikking komen.

Inleiding COBOL (2 dagen)

Door middel van inleidingen en oefening in het lezen van programma's wordt de structuur van het programmeren in COBOL getoond. Ter voorbereiding op de cursus controle bij geïntegreerde informatiesystemen zal de wijze van vertaling van Data Base statements naar COBOL statements worden behandeld.

Controle bij geïntegreerde informatiesystemen (4 dagen)

Deze cursus kan op dit moment worden beschouwd als het sluitstuk van de basisopleiding van diegenen die zich met aspecten van interne controle in de informatieverzorging bezig houden. Zowel de invloed van het gebruik van data base management systemen als van data communicatie en de relatie hiertussen worden tegen de achtergrond van de eisen van betrouwbaarheid behandeld. Gezien het feit dat in de cursus met onder meer Data Dictionary rapporten en met Schema- en Subschema Listings wordt gewerkt is bekendheid met COBOL noodzakelijk. Hiertoe dient bovengenoemde Inleiding COBOL.

Alhoewel reeds een deel van het jaar verstreken is, volgt hieronder het gehele cursusschema 1981.

Cursusdata en plaats

De inschrijving kan zowel voor een aantal curussen als per cursus geschieden. De cursussen worden met uitzondering van Boekhouden en Inleiding COBOL gegeven in het Kongres- en vergadercentrum Koningshof, Locht 117, Veldhoven.

Serie 81.1	*Data 1981*	
Administratieve Organisatie	6-9 of 6-10	april
Computer Control	6,7,8	mei
Boekhouden	18,19,20	mei
Computer Audit	25,26,27	mei
The Data Base Environment	1,2,3,4,5	juni
Inleiding COBOL	1,2	september
Controle bij geïntegreerde informatiesystemen	7,8,9,10	september

Serie 81.2	*Data 1981/1982*	
Administratieve Organisatie	14-17 of 14-18	september
Computer Control	6,7,8	oktober
Computer Audit	3,4,5	november
Aanpak Automatisering	16,17,18,19,20	november
Inleiding COBOL	1,2	december
Controle bij geïntegreerde informatiesystemen	5,6,7,8	januari 1982

Indien U belangstelling heeft, kunnen wij U de brochure 1981 alsnog toezenden. Door de AC-groep worden ook meer gespecialiseerde cursussen verzorgd. Aangekondigd zijn:

- 2 - 6 november 1981, IMS concepts for Auditors;
- 30/11 - 4 december 1981, IMS DB AUDIT Workshop;
- 1 - 5 maart 1982, MVS Audit cursus.