KMG Klynveld Kraayenhof & Co.
Automatisering & Controle-groep

COMPACT

86/1

Computer en Accountant

Schutz vor EDV-Kriminalität- ein Entschleierungsversuch
door Max F. Bretscher
KMG FIDES Treuhandgesellschaft Zürich

Accountant - automatisering en continuïteit
door drs. H. C. Kocks

Beoordeling betrouwbaarheid van een (geautomatiseerd) informatiesysteem: de CASA-methode
door A. H. C. Koedijk

Indentification and Evaluation of Operating System Controls (using IBM's Multiple Virtual Storage (MVS) operating system as an example)
door H. Weerd

Nummer 40 12e jaargang winter 1985/1986

COMPACT

C O M P U T E R E N A C C O U N T A N T

INHOUDSOPGAVE

nummer 40 **12e jaargang** **Winter 1985/1986**

ISSN 0920-1645

COMPACT

Winter 1985/1986

VAN DE REDACTIE

Voor u ligt ditmaal op tijd de nieuwste aflevering van Compact. Het is nummer 40 tevens de laatste van de 12e jaargang en eerste uitgave van 1986 (86/1).

Het is een themanummer dit keer dat aansluit op het vorige nummer. De grondgedachte daarvan vormt "Heroriëntering" of wel "Opnieuw bezinnen". Het denkproces heeft zich voortgezet en de neerslag daarvan tekent zich verder af in dit winternummer 1985/1986:

"De aanpak van de accountantscontrole en EDP-auditing".

De vier hoofdartikelen houden verband met elkaar als ware het een vierluik:
- behoedt u voor computerfraude;
- hoe ver reikt de verantwoordelijkheid van de accountant;
- hoe nu met systeembeoordeling zonder je te verliezen in details;
- hoe wordt een diepgaande EDP-audit uitgevoerd.

Voor de samenvatting van de artikelen verwijzen wij naar de volgende bladzijde.

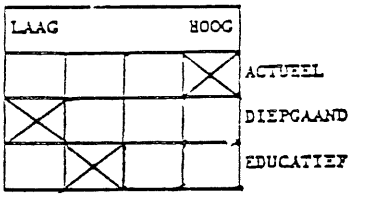
Het geheel wordt voorafgegaan door een tweetal actualiteiten: KMG K memory nr. 4 en het nieuwe AC-factsheet. De hoofdartikelen worden gevolgd door de rubrieken Micro (introductie FAT), Boeken, Tijdschriften, ABC-Nieuws en Onderwijs (inhoud cursus CASA).

J.C. Boer geeft een verduidelijking op zijn artikel in de vorige Compact. U kunt dit lezen onder de rubriek "Schrijvers reageren".

Bij ieder hoofdartikel wordt door de redactie een waardering ter zake van actualiteit, diepgang en educatie gegeven. Wij richten ons daarbij op het belang dat het artikel heeft voor de controlerende/certificerende accountant ofwel algemeen accountant.

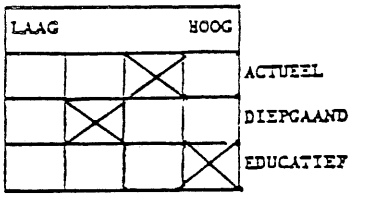
De kwalificatie laag←→hoog is niet synoniem met slecht of goed, technisch of niet-technisch.
Het "raampje" geeft simpel de mogelijkheid voor de lezer om vooraf te kunnen toetsen of het artikel geschikt is om te lezen gezien zijn intentie.

"Schutz vor EDV-Kriminalität - ein Entschleierungsversuch" door Max F. Bretscher
KMG FIDES Treuhandgesellschaft Zürich



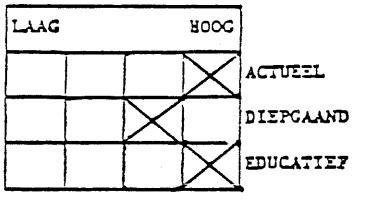
In den folgenden Betrachtungen werden Straftatbestände vorgestellt, wo ein Computer, Programme oder EDV-Datenträger eine ausschlaggebende Rolle spielen. Da einerseits wenige Gerichtsurteile vorliegen, welche die Straffähigkeit gewisser Tatbestände bezüglich EDV-Kriminalität untermauern, andererseits die diesbezüglichen Gesetze derzeit noch ein gewaltiges Vakuum aufweisen, sollen hier u. a. moralisch fragwürdige Handlungen zur Darstellung gebracht werden, und zwar auch wenn diese nicht unbedingt zu einer gerichtlichen Verurteilung führten bzw. führen müssen.

"Accountant - Automatisering en continuïteit"
door H.C. Kocks



Het is de bedoeling een bespiegeling te houden over de vraag of de accountant uit hoofde van de controle van de jaarrekening, aandacht dient te besteden aan de continuïteitsaspecten van de geautomatiseerde gegevensverwerking. De meningen hierover zijn (sterk) verdeeld. De voorstanders vinden wellicht steun in de literatuur waar sinds de invoering van automatisering "betrouwbaarheid en continuïteit" niet meer los van elkaar te vinden zijn. De tegenstanders beroepen zich nogal eens op het feit dat het slechts om de "cijfers" gaat. Argumenten voor en tegen zullen in dit artikel worden aangedragen alsmede een aantal raadgevingen.

"Beoordeling betrouwbaarheid van een (geautomatiseerd) informatiesysteem: De CASA-methode *"
door A.H.C. Koedijk

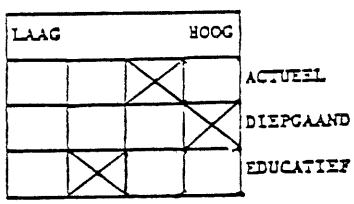


In dit artikel wordt een beschrijving gegeven van de in de cursus CASA (Cursus Aanpak Systeembeoordeling en Accountantscontrole) overgebrachte en toegepaste methode voor het beoordelen van de betrouwbaarheid van een (geautomatiseerd) informatiesysteem. Deze methode betreft een in de praktijk ontstane, op een functionele benadering gebaseerde werkwijze, die de laatste jaren meer systematisch is uitgewerkt.

* Zie ook de rubriek Onderwijs.

Reeds hier wordt benadrukt dat, hoewel de methode "redeneert" vanuit in de computer vastgelegde gegevensverzamelingen (een steeds normaler wordende situatie), de methode in principe voor elk onderzoek naar betrouwbaarheids-aspecten van de Administratieve Organisatie toepasbaar is. Immers, een functionele benadering impliceert dat (zeker in eerste aanleg) meer wordt gekeken naar de functie (met andere woorden het "wat") en minder naar de wijze waarop (met andere woorden het "hoe").

"Identification and Evaluation of operating system controls (using IBM's Multiple Virtual Storage (MVS) operating system as an example)" door H. Weerd



Dit artikel vormt een der bijdragen - namelijk te zamen met het boek "Auditing the Technical EDP Organisation" van mw. M.E. van Biene-Hershey en de voordracht van H.J. Dain over het onderwerp "Change Management at N.V. Philips Computing Centre Eindhoven - op het Symposium "Auditing van de EDP-organisatie", georganiseerd door de Sectie EDP-auditing van het Nederlands Genootschap voor Informatica op 3 december 1985 in de RAI te Amsterdam.

Het in het Engels geschreven artikel geeft de controle-aanpak specifiek voor MVS weer. Het gaat om een diepgaand onderzoek, waarbij de schrijver niet kan ontkomen aan het gebruik van geheimtaal.

In een tiental hoofdstukken wordt de problematiek uit de doeken gedaan:

1. Introduction
2. Risk areas
3. The technical support function
4. MVS
5. Installation management and change management
6. Some Major Threats/Controls
7. Security policy for a MVS-installation
8. Computer Security Audit
9. MVS Security Audit
10. To conclude

COMPACT

Winter 1985/1986

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

Deze informatie is in de eerste plaats bestemd voor diegenen, die in de algemene controlepraktijk werkzaam zijn. De in dit tijdschrift weergegeven meningen mogen niet altijd gezien worden als officiële zienswijzen van KMG Klynveld Kraayenhof & Co. De in de rubrieken besproken artikelen worden soms geheel opgenomen of verkort aangehaald, tevens als regel voorzien van commentaar.

Redactie:
A.H.C. Koedijk
A.W. Neisingh,
Prof. D. Steeman
H.J.M. van der Wielen (secr.).

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

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

ISSN 0920-1645

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

ACTUALITEITEN

KMG Computer Newsletter

K Memory wordt uitgegeven door de Practice Development Unit, KMG Executive Office, onder supervisie van J.H. Urbanus als lid van de Computer Audit Subcommittee (CASC).

Het blad is in eerste aanleg voor intern gebruik binnen KMG. Voor belangstellenden - ook voor onze cliënten - is een exemplaar van de jongste editie van december 1985 beschikbaar.

De inhoud kan als volgt worden samengevat:

KMG Communications
Electronic Communications grow throughout KMG.

Envoy 100 is een electronic mailbox-systeem dat een groot aantal gebruikers binnen KMG met elkaar verbindt. In verband met de grote tijdsverschillen ten gevolge van de geografische spreiding van de KMG-kantoren is het systeem belangrijk voor de communicatie.
Oorspronkelijk opgezet als een eenvoudige "boodschappendienst" kent het systeem een groot aantal specifieke toepassingen (zie K Memory).

KMG Training and education
An integrated training function.

Door het Training and Education Committee (TEC) is nagegaan hoe de opleiding binnen KMG het best gestalte kan krijgen.
Uitgaande van de viervoudige doelstelling:
- verbetering van het gehalte van onze dienstverlening aan cliënten;
- verhoging van de vorm van de dienstverlening, in het bijzonder die van Opleiding;
- de verworvenheden aanvaard door KMG, verspreiden en laten accepteren in een hogere mate dan tot nu het geval is;
- het enthousiasmeren van toekomstige medewerkers.

Hiertoe is gebruikersvriendelijke programmatuur ten behoeve van de accountant ontwikkeld alsmede cursuscycli die bloksgewijze zijn opgebouwd.

KMG Computer services
KMG Norway en KMG UK hebben ieder belangen verworven in softwarehouses.
Noorwegen: KMG Dataplan A.S.
Engeland: Informatics unit van KMG Thomson McLintock.
Ieder van de eenheden beslaan een relatief groot gebied van deskundigheid (zie K Memory).
Over KMG in Banking berichtten wij u reeds in het vorige nummer van Compact.

Onder het hoofd Bytes & Pieces een kort bericht over een nieuw Microcomputer Handboek, vooralsnog alleen in Deens en over de nieuwe naam van CARS.

De nieuwe naam voor dit audit software-pakket is geworden GRACE - Generator of Reports for Auditors in a Cobol Environment.
Het idee is gelanceerd door "onze" Hans Veenman, redacteur van de rubriek Micro in Compact, tevens de EDP-auditor die leiding geeft aan onze research-groep op het gebied van de micro en de accountantscontrole.

2. Ons nieuwe FACT-sheet is recent verschenen, zie bijgaande afdruk van de Nederlandse tekst. Voor belangstellenden zijn ook de Franse, Duitse en Engelse versies beschikbaar.

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

Winter 1985/1986

KMG Klynveld Kraayenhof & Co.
Accountants
Automatisering & Controle-groep
Voor de beoordeling van automatiseringsorganisaties
en -informatiesystemen

Factsheet

In 1973 heeft KMG Klynveld Kraayenhof & Co. een afzonderlijke groep, de Automatisering & Controle-groep geformeerd. Dit om het hoofd te bieden aan gerezen controle/beveiligings-problemen veroorzaakt door de automatisering van informatieverzorging alsmede om een passend antwoord te kunnen geven op de toekomstige nieuwe ontwikkelingen op dat gebied.

Opdrachten tot onderzoek en/of assistentie ter zake van automatisering en controle alsmede verzoeken tot opleiding op dit gebied bereiken ons van verschillende categorieën opdrachtgevers, te weten:
1. Collega's binnen de KMG-controlepraktijk zowel in Nederland als daarbuiten;
2. Het management van bedrijven, instellingen of vanwege de overheid;
3. Partijen die gezamenlijk gebruik maken van computercentra en/of netwerken;
4. Interne controle- en accountantsdiensten.

Hoofdactiviteiten

Algemeen
Controle van de jaarrekening
- ondersteuning van de collega's, die belast zijn met opdrachten voor de algemene jaarrekeningcontrole, speciaal bij onderzoeken van:
  - automatiseringsorganisaties, computer operations;
  - informatiesystemen (in exploitatie, in het stadium van voorbereiding);
- ondersteuning inzake het gebruik van de computer (mainframes zowel als micro's) voor het toetsen van de automatiseringsorganisatie en voor bestandsonderzoeken.

Opleiding/voorlichting
- samenstellen gevolgd door het geven van AC-cursussen of presentaties dan wel het geven van adequate training (zie onze brochures op dit gebied);
- het publiceren van een intern vaktijdschrift COMPACT met relevante AC-informatie;
- het uitgeven van brochures/boeken op AC-gebied:
  - Kleinschalige automatisering;
  - Computerbeveiliging;
  - SWIFT;
  - Database & accountant;
  - Uitkomsten van een in 1983 verricht onderzoek naar grensoverschrijdend gegevensverkeer in Nederland.

Research
Het plegen van research is gericht op beveiligings- en controleproblematiek van:
- Data base management systems;
- Operating systems;
- Data-communication;
- On-line operations;
- Risk management/Risk analysis;
- Audit micro.

→

Bijzondere opdrachten
Door de verkregen technische deskundigheid als gevolg van ervaring en research worden regelmatig ook opdrachten uitgevoerd welke buiten de jaarrekeningcontrole liggen, zoals op het gebied van:
- beveiliging van gegevens en rekencentra;
- privacy;
- grensoverschrijdend gegevensverkeer;
- beoordeling van doelmatigheid en doeltreffendheid van EDP-organisaties en processen;
- zelfstandig onderzoek naar betrouwbaarheid van opzet en werking van automatiseringsorganisaties en informatiesystemen, gevolgd door een mededeling ten behoeve van derden over betrouwbaarheid, beveiliging en back-up;
- optreden als deskundige in arbitrages;
- technische en operationele reviews (audits) ter zake van automatisering;
- enquêtes met uitwerking daarvan met behulp van zelf ontwikkelde programmatuur;
- risico-analyse, onderkenning van continuïteitsbedreigende factoren ten gevolge van automatisering.

Diverse activiteiten
- Beschikbaar stellen aan onze cliënten van computer-software voor controledoeleinden.

Bemanning

De AC-groep wordt centraal geleid door 6 vennoten en bestaat verder uit:
- 13 EDP-auditors;
- 16 aankomend EDP-auditors;
- 23 programmeurs.

Derhalve 58 personen die zich in volledige dagtaak met het vakgebied automatisering en controle bezig houden. Daarnaast zijn AC-accountants, verspreid over de vestigingen van KMG voor een deel van de beschikbare tijd met AC-werk belast.
Allen hebben een gerichte opleiding ontvangen op het gebied van:
- beoordeling van automatiseringsorganisaties en informatiesystemen;
- controle met behulp van de computer.

Bovendien krijgen jaarlijks 10 stagiairs de gelegenheid om onder deskundige leiding hun stage-opdrachten uit te voeren. Deze opdrachten houden nauw verband met de werkterreinen van de AC-groep.

6 januari 1986

dass durch relativ kleine, aber gezielte Einzelschläge erheblicher Schaden angerichtet werden kann.

Beispiele:

1. Ein entlassener Systemprogrammierer hatte in seinem Betriebssystem eine «Zeitbombe» gelegt. Einige Zeit nach seiner Entlassung «verlangte» das Betriebssystem eines Tages die wichtigsten Datenträger und löschte sie ohne Warnung (Wisconsin 1973).
2. Eine Handgranate in ein Fernverbindungszimmer z. B. einer Bank oder gar in deren Computer hat effektvolle Konsequenzen (hypothetisch).

1.2. Erpressung

Die Konzentration des Know-How und des Datenmaterials erleichtert die «Entführung» und die Erpressung mit dem gestohlenen Datenmaterial. Fehlende Dokumentation schafft zudem eine wesentliche Personenabhängigkeit, welche durch skrupellose Programmierer ausgenützt werden kann. Mittels Entführen wichtigen Personals sind weitere Erpressungen möglich.

Beispiele:

1. Operators einer Handelsfirma entwendeten alle Stamminformationen sowie die Bücher ihres Arbeitgebers (18 Magnetbänder) und versuchten damit eine Million Gulden zu erpressen (Niederlande 1968).
2. Ein externer Programmierer versuchte bei seinem Auftraggeber ein zinsloses Darlehen (Fr. 25 000) zu erhalten. Mit Hinweis, ausser ihm könnte im Programmierbüro ohnehin niemand die Buchhaltung des Auftraggebers über die Bühne bringen, war eine erpresserische Drohung mit dem «Gesuch» verbunden (Zürich 1974).

1.3. Diebstahl

Das Rechenzentrum, insbesondere mit Datenfernverarbeitung, ist einem neuartigen Delikt ausgesetzt: dem Zeitdiebstahl. Durch unerlaubte Benützung von Speicherplatz, Rechenzeit, Ein- und Ausgabematerial entgehen Rechenzentren teilweise erhebliche Einnahmen. Die EDV-Datenträger ermöglichen es ausserdem, grosse Mengen an Datenmaterial auf unauffällige Art und Weise zu entwenden. Obschon das gestohlene Material (Datenträger) wenig kostet, kann die Information, welche sich darauf befindet, von sehr grossem Wert sein. So kann neben Datenmaterial im engeren Sinne auch Know-How in Form von Programmen oder Plänen auf den unscheinbaren Datenträgern festgehalten sein.

Beispiele:

1. Ein EDV-Leiter benützte die Anlage seines Arbeitgebers, um für seinen Freund die Buchhaltung (mail-order-house) zu führen. Wegen Speicherplatzproblemen beantragte er die Anschaffung neuer Platteneinheiten. Eine schnellere Zentraleinheit wurde ebenfalls bewilligt und angeschafft. Zum Schluss benützte der Besitzer des Rechenzentrums seine Anlage noch zu 20 %, zahlte aber 100 % (New York 1981).
2. Eine Hardwareteileprüferin eines Computerherstellers sandte u. a. perfekte Computerteile (mit Spezialkennzeichen) auf den Schrotthaufen. Ihr Mann als Schrotthändler kaufte die Teile auf und betrieb ein lukratives «Occasionsgeschäft». Beim Entdecken des Plans besass der Schrotthändler ein Warenlager von über 5 Mio. $, hatte Debitoren von über 2 Mio. $ und hatte Einnahmen von mehreren Dollar-Millionen bereits getätigt (Burlington USA 1982).

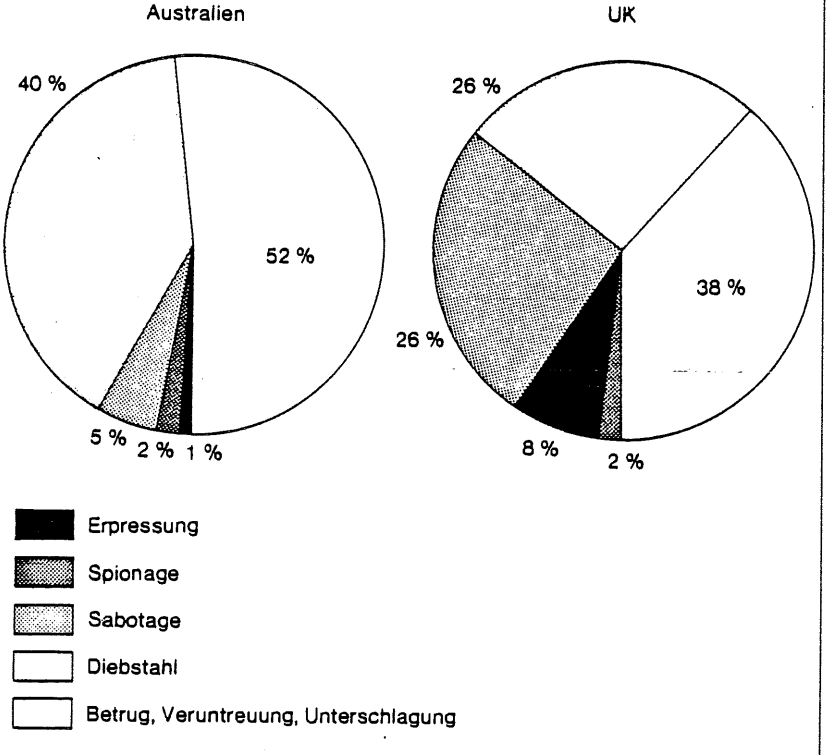
1.4. Spionage

Sie ist im Zusammenhang mit EDV sehr oft verwandt mit Diebstahl, indem die geheimen Informationen auf einem Datenträger festgehalten sind, der dann entwendet wird. Die bei Computern eingesetzte Fernübertragungstechnik besitzt weiterhin verletzliche Stellen, indem *die Leitungen* (heutzutage auch ohne «Anzapfen») abgehört werden können.

Beispiele:

1. Ein Programmierer eines Mikrocomputerherstellers machte sich

Darstellung 1:
Verteilung festgestellter Computerkriminalität (Anzahl Fälle in %)



selbständig. Er hatte dabei mehrere Disketten mitlaufen lassen, die es ihm erlaubten, innert kürzester Zeit «Piratenprodukte» auf den Markt zu werfen, wobei er durch geringfügige Änderungen den Copyrightschutz zu umgehen suchte (San Francisco 1980).

2. 1978 versuchte ein amerikanischer Ex-Projektleiter in Amsterdam einem Ostagenten ein Band mit militärischen Geheimnissen bezüglich der Cruise-Missile zu «verkaufen». Der Fall wurde entdeckt, als sich herausstellte, dass das Band irrtümlicherweise leer war . . .

1.5. Betrug, Veruntreuung, Unterschlagung, Fälschung

Die Computertechnik eröffnet neue Möglichkeiten, sich unrechtmässig Geld zu verschaffen. Hauptschuldig daran ist wohl nach wie vor der Mythos, welcher die Unfehlbarkeit des Computers umschwebt. Es ist denn auch diese Begleiterscheinung, welche der Behauptung Vorschub leistet, es gäbe gar keine spezielle *EDV*-Kriminalität. EDV schafft die Gefahr von Funktionenkumulationen, welche ihrerseits Vermögensdelikte begünstigen. Daneben ist aber zu beobachten, dass mit der Computertechnik auch neuartige Deliktsgebiete eröffnet werden:

- Datenträger-Manipulationen
- Handling-Manipulationen
- Programm-Manipulationen

Beispiele:

1. Ein Operator verändert die Begünstigtenadresse auf dem Kreditorenzahlungs-DTA-Band und lässt sich so über Fr. 100 000 gutschreiben (Basel 1979).
2. Ein Programmierer entzieht sich seiner Steuerschulden durch Programm-Manipulationen (Bellinzona 1974).

2. Die Sicht des Kriminellen

Darstellung 2 zeigt eine Zusammenfassung dieses Blickwinkels. Nimmt man für einige Momente (und sei es nur aus didaktischen Gründen) die Position des EDV-Kriminellen ein, so ergeben sich folgende Szenarien:

2.1. Der Saboteur

Seine Absicht ist es, den «normalen», ordnungsmässigen Betrieb einer Organisationseinheit zu stören oder gar zu unterbinden. Sein Vorgehen ist dabei nicht zimperlich, sondern meist mit Gewalt verbunden. Die Ziele seiner Handlungen sind

- Zerstörung oder Verfälschung von Rohstoffen, Zwischen- und Endprodukten,
- Lahmlegen der Produktionsmittel,
- Verhindern des ordnungsmässigen Ablaufs von Fertigungsprozessen,
- Unbrauchbarmachen von Transportmitteln,
- Verbarrikadieren von Transportwegen.

Auf die EDV übertragen gelten die gleichen Ansätze und Elemente:

- «Materialien» der EDV sind *Daten* und *Programme*,
- Prozesse werden durch *Programme* auf *Rechnern* ausgeführt,
- Produktionsmittel sind *Computer* und *Menschen*.
- Transportmittel sind *Menschen* oder *Leitungen*,
- Transportwege sind *Kanäle* (z. B. Telephonleitungen).

Grundsätzlich ändert sich für den Saboteur demnach kaum etwas. Seine Tätigkeiten, soweit sie physischen Charakter aufweisen (z. B. Zerstörung von Datenträgern oder Computern), bleiben sogar praktisch identisch mit den «konventionellen» Zielen. Beim Verfälschen bzw. Zerstören magnetisierter Informationen dagegen bedient sich der Saboteur vornehmlich der EDV selbst für sein destruktives Tun.

Eine computerspezifische Form des Legens von Zeitbomben ist dabei der Einsatz von «Computer-Viren». Es wird die Tatsache ausgenützt, dass die Integrität eines internen EDV-Systems (Betriebssystem, Compiler, Programm-Bibliothek) in den wenigsten Fällen angezweifelt wird. Besonders perfid ist die Tatsache, dass die Verfälschung oft nicht offensichtlich ist, wie dies z. B. bei zerbrochenen Fensterscheiben der Fall wäre.

2.2. Der Erpresser

Aufgrund der Tatsache, dass dem rechtmässigen Besitzer eine Sache vorenthalten wird, oder infolge eines unangenehmen (Mit-)Wissens versucht der Erpresser, sein Gut zu «verkaufen». Die vorstehenden Beispiele illustrieren deutlich, dass die EDV keine vordergründige Rolle spielt bei den kriminellen Handlungen:

- Die vorenthaltenen Daten waren auf Magnetbändern (physisch) entwendet worden.

Darstellung 2:
Die elf Gebote des EDV-Kriminellen

1. Suche die schwächste Stelle im EDV-System und nütze sie aus.
2. Suche Dir ein Opfer aus, das unter Funktionenkumulation im EDV-Bereich eine Tugend sieht.
3. Verhindere das Einbauen von Kontrollen oder gar Abstimmkreisen im EDV-Bereich.
4. Wiege das Opfer im Sicherheitsgefühl, dass der Computer alles richtig macht.
5. Erwecke beim Opfer die Überzeugung, dass es ohne Dich in der EDV nicht geht, dass es sich aber auf Deine Zuverlässigkeit verlassen kann.
6. Sorge dafür, dass Dein Opfer keine Stellvertreter für Dich ernennt oder ein Ausweichprozedere vorsieht.
7. Erkläre dem Opfer, dass eine tagfertige Dokumentation unwirtschaftlich oder gar gefährlich ist.
8. Schaffe eine derartige Unordnung im EDV-Bereich, dass eine Entdeckung unwahrscheinlich ist, und Du auf keinen Fall als Täter in Frage kommst.
9. Nütze die Wiederverwendbarkeit der Datenträger und lösche sie rechtzeitig.
10. Arbeite allein. Steht die Entdeckung Deiner Tat bevor, fälsche die Unterlagen so, dass sich die Spur im Nichts verliert. Vermeide es, die Schuld jemandem bestimmten zuzuschieben. Er könnte sich wehren (Boomerangeffekt).
11. Hüte Dich vor der EDV-Revision.

- Anstelle des exklusiven Wissens des Programmierers könnte die (lediglich *einem* Spezialisten bekannte – als Beispiel sei das «verlorene» Geheimnis der Stradivari-Geigen angeführt –) Tätigkeit in einem Fertigungsprozess stehen.

Es ist somit lediglich das EDV-spezifische Gut (Information in magnetischer Form festgehalten bzw. Wissen bezüglich EDV-Technik), welches in dieser Hinsicht die EDV-Kriminalität auszeichnet. Darin unterscheidet sich aber die EDV kaum von einem anderen Spezialistengebiet wie Chemie, Baustatik, Motorenbau, Geologie usw. Es wird aber m. W. nicht von einer z. B. speziellen «Geologie-Kriminalität» gesprochen, wenn ein Geologe absichtlich am falschen Ort nach Mineralöl graben liesse.

2.3. Der Dieb

Das «Hauptproblem» bei der Entwendung von Gütern (Waren, Geld, immaterielle Werte) ist dieses, möglichst unentdeckt an das Gut zu gelangen, es an sich zu nehmen und ebenso unentdeckt wieder zu verschwinden. Muss dabei Gewalt (insbesondere gegen Personen) angewendet werden, so handelt sich die Straftat wohl eher um Raub. Diese letztere Art von Kriminalität dürfte in ihrer EDV-spezifischen Ausprägung aber eher selten sein.

Welche Hindernisse können dem Dieb im Wege stehen?

- Verschliessungsmechanismen aller Art: Mauern, Schlösser, Zäune;
- Bewachungspersonal;
- Bewachungseinrichtungen (Alarmanlagen);
- Dumme Zufälle.

Es ist demnach seine Aufgabe, diese Hindernisse zu kennen, den einfachen Weg (die schwächste Stelle) zu suchen und sich entsprechend zu verhalten. Einfach, nicht?

Welche Besonderheiten sollte er nun beachten, wenn ein Computer im Spiel ist? Der einfachste Weg zum zu entwendenden Gut führt oft über den Computer, weil viele Leute vergessen, Verschliessungsmechanismen zu installieren. Sie übersehen auch, dass bei Computern dieser Mechanismus oft Passwortsystem heisst und dass die Passwörter wie Schlüssel gehütet werden sollten. Es ist häufig einfacher, ein Passwort zu erfahren, als eine Schlüsselkopie anzufertigen. Umgekehrt ist es viel einfacher, Schlösser mit Dietrichen zu knacken, als Passwörter durch Zufall zu entdecken.

Wenn der Computer selbst das zu entwendende Gut ist, so ist dies ein gewöhnlicher Sachdiebstahl und hat wohl nichts mit EDV-Kriminalität zu tun.

Immer häufiger werden (immaterielle) Werte dem Computer zur Aufbewahrung anvertraut. Daten und Programme können grossen Werte darstellen. Sie werden auf Datenträgern festgehalten. Diese wiederum sind oft so unscheinbar, dass sie unbemerkt mitgenommen werden können. Die Schwierigkeit liegt also nur noch darin, an den Datenträger heranzukommen, ihn evtl. zu kopieren und damit zu verschwinden. Somit reduziert sich auch hier die EDV-Kriminalität zum Sachdiebstahl.

2.4. Der Spion

Er ist ein (verbotener) Kundschafter. Er gewinnt seine Kenntnisse durch Abhören oder Einsichtnahme, wenn er darüber hinaus nicht Diebstahl, Entführung, Erpressung oder Raub begehen will.

Seine grössten Gegner bei diesen Tätigkeiten sind somit Verschluss und Verschwiegenheit, seine besten «Verbündeten» die Sorglosigkeit und die Schwatzhaftigkeit (der anderen).

Daran änderte sich mit der Einführung der EDV überhaupt nichts. Die Gebote von Verschwiegenheit und Schutz vor Einsichtnahme durch unbefugte Dritte erweiterten sich aber auch auf diese Technologie, was leider oft übersehen wird:

- «Geschwätzige Computer» können «abgehört» werden (Telephonleitungen),
- Datenträger sind leicht zu kopieren und dann unbemerkt «einzusehen».

2.5. Der Betrüger

Es handelt sich hier beim Delikt praktisch eigentlich immer, wenn auch abgeleitet, um unrechtmässige Aneignung von Geldwerten, oder ganz einfach Diebstahl. Demnach gelten ähnliche Anmerkungen wie jene, die auf den Dieb zutreffen. Eines der Hauptprobleme des Betrügers ist denn auch häufig, überhaupt an das ertrogene Geld heranzukommen.

Die Ansatzpunkte des Betrügers bei Einsatz von EDV beziehen sich auf die drei Grundelemente der EDV:

- Eingabe
- Verarbeitung
- Ausgabe.

Man kann sich tatsächlich fragen, was denn daran so besonders sei:

- Belege lassen sich auch ohne EDV fälschen,
- Buchhalter kannten absichtliche Fehlbuchungen (ohne Journal) schon lange vor dem Bau des ersten Computers,
- Absichtliche Bewertungsfehler (zum Beispiel) haben mit EDV schon gar nichts zu tun.

Ja, die Behauptung ist wohl eher zutreffend, die EDV gestalte die Verarbeitung von Informationen sicherer (und dämmt damit die Kriminalität ein), indem viele Kontrollen erzwungen werden könnten. Als triviales Beispiel sei die «plumpe» Buchhaltungsfälschung der absichtlichen einseitigen Buchung erwähnt, die mit einem EDV-bedingten Zwang der Soll-/Habengleichheit verunmöglicht ist. Richtig eingesetzt nützt die EDV der Sicherheit mehr als dem Kriminellen!

3. Worauf achtet also der EDV-Kriminelle?

Sorglosigkeit des Opfers ist einer der Hauptangelpunkte, wo Sünden im Hinblick auf EDV-Kriminalität begangen werden. Dazu ist auch die *Vertrauensseligkeit* auf das «Gute im Menschen» zu zählen: Über 80 % der entdeckten EDV-Täter waren zum ersten Mal der Versuchung eines Deliktes erlegen; über 70 % der Täter waren zum Zeitpunkt

Darstellung 3:

Massnahmen zur Verhinderung von EDV-Kriminalität

	von aussen	von innen
● Physische Massnahmen gegen unbefugten Zutritt	x	(x)
● Logische Massnahmen gegen unbefugten Zugriff	x	x
● Systematisches Projektvorgehen und Änderungswesen	(x)	x
● Vermeidung von Funktionenkumulationen		x
● Einbau erzwungener Kontrollen	(x)	x
● Häufige Einhalteprüfungen bezüglich der Kontrolltätigkeiten	(x)	x
● Intensive und laufende Personalbetreuung		x
● Versicherungen	(x)	(x)

des Deliktes schon seit mehr als 5 Jahren im betreffenden Betrieb tätig!

Abhängigkeit ist eine weitere Eigenschaft, welche sich nicht nur im Zusammenhang mit Erpressungen auszahlt. Oft ist es für das Opfer einfacher, die erlittenen Verluste hinzunehmen, als den Parasiten abzuschütteln. Zu diesem Problemkreis gehören auch Stichworte wie fehlende Stellvertretung oder mangelhafte Sicherheitskopierung.

Betrug, Veruntreuung, Diebstahl usw. können vor allem dort über längere Zeit unentdeckt betrieben werden, wo *Funktionenkumulationen* vorhanden sind. Der Täter arbeitet gerne alleine und möchte den Überblick über seine Aktivitäten behalten. Mit dem Einzug der EDV wurden etliche «natürliche» Trennungen abgeschafft, ohne dass sich das potentielle Opfer dessen bewusst ist. Dasselbe gilt für *fehlende Kontrollen* gegen unabsichtliche bzw. bewusste Fehler von ausserhalb oder innerhalb des Betriebes.

Viele Täter sind sich bewusst, dass ihre Verfehlungen unter Umständen plötzlich aufhören (müssen). *Fehlende Dokumentation, unvollständige Aufzeichnungen* und allgemeine Unordnung erschweren oder verhindern eine schnelle und wirksame Verfolgung (vgl. *Darstellung 2).*

4. Wie sich dagegen schützen?

Eine Verfahrensprüfung als Schwachstellenanalyse kann Möglichkeiten aufdecken, welche die negativen Auswirkungen von EDV-Kriminalität frühzeitig offenbaren. Durch geeignete Massnahmen, nicht zuletzt aufgrund von Vorschlägen dieser Gutachter, werden die Risiken kleingehalten oder gar verhindert (vgl. *Darstellung 3).* Spezialisten der EDV-Revision sind dazu ausgebildet, derartige Analysen anzustellen und entsprechende Verbesserungsvorschläge zu erarbeiten.

Wenn Risiken nicht durch (zusätzliche) Kontrollen vermindert werden können, ist es eventuell angezeigt, den Abschluss einer einschlägigen *Versicherung* zu erwägen.

An erster Stelle liegt m. E. aber die laufende und gutmeinende *Personalbetreuung.* Systeme und Mechanismen aller Art funktionieren nur, wenn sie befolgt werden. Das Einhalten dieser Massnahmen und die vernünftige Reaktion im Ausnahmefall ist aber eben weitgehend vom gesunden Menschenverstand und dem guten Willen der beteiligten Personen abhängig. Zur erfolgreichen Abwehr von EDV-Kriminalität von innen und aussen ist ein gutes Betriebsklima Voraussetzung. ☰

Literatur

Brandt Allen: «The Biggest Computer Frauds . . .» im Journal of Accountancy, Mai 1977.

Cohen Fred: «Computer Viruses, Theory and Experiments», University of Southern California, 1984.

Fitzgerald Kevin J.: «Computer-related Crime in Australia» in EDPACS, August 1984.

Kuong Javier F.: Computer Security, Auditing and Controls, Wellesley Hills (Mass.), 1974.

Wong K. K.: «U. K. Computer Fraud Survey» in EDPACS, März, Mai und Juni 1984.

Zweifel Sibylle: Buchführungsdelikte mittels EDV . . ., Zürich 1984.

SOMMAIRE

Mesures de protection contre la criminalité T.E.D.

Une analyse des points faibles peut révéler à temps les conséquences négatives de la criminalité T.E.D. Par des mesures appropriées, nos pas seulement basées sur des propositions d'experts, les risques diminueront, voire disparaîtront. Ces mesures peuvent être les suivantes:

- entrée interdite à toute personne étrangère au service;
- mesures logistiques contre toutes mainmises indésirables;
- avancer régulièrement dans les projets et modifier systématiquement les données qui peuvent l'être;
- éviter les cumuls de fonctions;
- mise en place de contrôles obligatoires;
- fréquentes vérifications de l'efficacité des contrôles;
- attention soutenue portée au personnel;
- contracter des assurances.

Les spécialistes en révision de l'informatique sont formés de telle manière qu'ils peuvent procéder à de telles analyses et proposer des améliorations.

Si les risques ne peuvent être diminués par des contrôles ou par des contrôles complémentaires, il convient de conclure une assurance.

Il est évident que la confiance que l'on a au personnel est un élément primordial. Les systèmes et le mécanisme ne fonctionnent que s'ils sont suivis. L'observation des mesures décrites et une réaction judicieuse aux cas d'exceptions dépendent de la bonne compréhension et volonté des participants. Un climat sain dans l'entreprise permet une défense efficace contre la criminalité interne et externe.

MB/EK

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

COMPACT

Winter 1985/1986

ACCOUNTANT - AUTOMATISERING EN CONTINUITEIT

door drs. H.C. Kocks

Inleiding

Het is de bedoeling een bespiegeling te houden over de vraag of de accountant uit hoofde van de controle van de jaarrekening, aandacht dient te besteden aan de continuïteitsaspecten van de geautomatiseerde gegevensverwerking. De meningen hierover zijn (sterk) verdeeld. De voorstanders vinden wellicht steun in de literatuur waar sinds de invoering van automatisering "betrouwbaarheid en continuïteit" niet meer los van elkaar te vinden zijn. De tegenstanders beroepen zich nogal eens op het feit dat het slechts om de "cijfers" gaat. Argumenten voor en tegen zullen in dit artikel worden aangedragen alsmede een aantal raadgevingen.

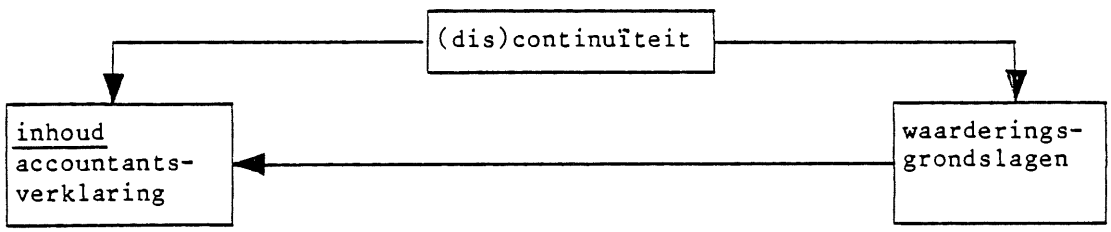
1. De going concern-gedachte

Op basis van de going concern-gedachte wordt als argument gehanteerd dat de accountant uit hoofde van de controle van de jaarrekening aandacht dient te besteden aan de continuïteit van de geautomatiseerde gegevensverwerking. Immers, indien van dreigende discontinuïteit sprake is, zal dit van invloed zijn op de waarderingsgrondslagen alsmede op de af te geven verklaring. Deze algemeen gestelde lijn wordt dus doorgetrokken naar dreigende discontinuïteit als gevolg van de geautomatiseerde gegevensverwerking. De vraag is derhalve of dit algemeen principe zonder meer van toepassing is op het deelgebied automatisering. Hiervoor gaan we terug naar de literatuur over accountant en continuïteit in algemene zin. Over dit onderwerp is in de literatuur weinig te vinden. Toonaangevend is echter de "Meningsuiting" van het NIvRA in 1977 die als titel draagt "De inhoud van de accountantsverklaring bij de jaarrekening van ondernemingen met continuïteitsproblemen".

De publicatie 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 publicatie ligt opgesloten. De drie (kern)begrippen waar het in de "Meningsuiting" om draait zijn: (dis)continuïteit, 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 figuur 1).



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

Gezien het voorgaande blijft de vraag wat onder dreigende discontinuïteit moet worden verstaan en welke aspecten de accountant in ogenschouw moet nemen om vast te kunnen stellen of er sprake is van dreigende discontinuïteit.
De "Meningsuiting" zegt hierover het volgende:
"De continuïteit van een onderneming wordt bedreigd indien het gevaar bestaat dat de onderneming niet langer in staat zal zijn onder andere 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.." (einde citaat).

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 beperkt de accountant zich tot financiële aspecten (de symptomen).

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 van dreigende discontinuïteit) van financiële of niet-financiële aard zijn?

De meningsuiting geeft hierop een duidelijk antwoord.
Een situatie van discontinuïteit ontstaat indien niet meer aan de financiële verplichtingen kan worden voldaan. De oorzaken kunnen velerlei zijn doch de vertaling naar de controle van de jaarrekening wordt door de accountant gemaakt via de financiële "symptomen" die in de meningsuiting worden genoemd.
Bepalend voor de inhoud van de af te geven verklaring is of de jaarrekening een getrouw beeld geeft van vermogen en resultaat en of de cliënt ten tijde van het afgeven van die verklaring aan haar financiële verplichtingen kan voldoen. Indien deze symptomen aangeven dat er twijfel ten aanzien van de continuïteit van de onderneming is gerechtvaardigd zal dat van invloed zijn op de af te geven verklaring.
Daarop is derhalve niet van invloed of al dan niet getroffen maatregelen voldoende zijn om de continuïteit van de geautomatiseerde gegevensverwerking in redelijke mate te waarborgen. Uit dien hoofde kan (en mag) dreigende discontinuïteit met betrekking tot geautomatiseerde gegevensverwerking niet tot de controle van de jaarrekening worden gerekend.

2. Het deelaspect Automatisering

Uit het voorgaande blijkt dat de beroepsorganisatie een duidelijk (afgebakend) standpunt inneemt. De vraag is of dit terecht is. In feite wel, maar stel dat dit standpunt niet terecht zou zijn. De vraag komt dan op waarom dan het aspect automatisering wordt gelicht uit het grote scala van niet financiële oorzaken. Onmiskenbaar is dat de continuïteit van de bedrijfsvoering in toenemende mate afhankelijk wordt van de automatisering, maar automatisering is daarmee niet het alleen zaligmakende deelgebied. Door het feit dat de accountant alleen aan dit aspect aandacht besteedt kunnen valse verwachtingen - zowel bij de leiding als bij derden - worden gewekt. Stel dat uit een onderzoek naar de continuïteit van de geautomatiseerde gegevensverwerking (door een deskundige) blijkt dat aan de door het management gestelde eisen wordt voldaan. Het order-, verkoop- en distributiesysteem is geautomatiseerd en vitaal voor de continuïteit van de bedrijfsvoering. Uit de resultaten van het onderzoek mag worden afgeleid dat - gezien de getroffen maatregelen - dit systeem met betrekking tot de continuïteit geen problemen voor de bedrijfsvoering oplevert.
Indien echter ten aanzien van de voorraden (opslag, bewaking) onvoldoende maatregelen zijn getroffen ligt daar het continuïteitsprobleem. Moet de accountant dan ook al die continuïteitsaspecten bij de controle van de jaarrekening betrekken (zijdelings gebeurt het via het hoofdstuk "verzekeringen" maar dit geldt eveneens voor automatisering). Dit zal zijn deskundigheid te boven gaan. Om een evenwichtig oordeel te kunnen vellen zal de accountant dan de niet financiële aspecten inzake eventuele discontuïniteit van de totale onderneming in ogenschouw moeten nemen. Zoals reeds gezegd kunnen en zullen dan de deskundigheidsgrenzen worden overschreden.

3. Normen

Bij het afgeven van oordelen ligt daaraan ten grondslag dat een feitelijke situatie wordt getoetst aan een norm. Voor de controle van de jaarrekening wordt die norm mede aangelegd door de accountant. Voor de bepaling van die norm zijn de accountant hulpmiddelen aangedragen. Door het afgeven van een verklaring geeft de accountant te kennen dat binnen de gestelde normen (door de wet, beroepsregelingen, etc.) de jaarrekening een getrouw beeld geeft van het vermogen en resultaat.

Bij een onderzoek naar de continuïteit van de geautomatiseerde gegevensverwerking zal het uiteindelijk ook tot een oordeel moeten leiden. Indien de accountant meent dat onderzoek uit hoofde van zijn controle van de jaarrekening te moeten verrichten zal hij daarvoor zelf een norm moeten bepalen. Hier ligt een knelpunt.
Objectieve normbepaling ontbreekt hier evenals hulpmiddelen waarmee de accountant een objectieve norm kan bepalen. Hiermee wordt gesuggereerd dat wanneer die objectieve normbepaling wel mogelijk zou zijn het probleem voor de accountant zou zijn opgelost. Niets is minder waar.
Uit hoofde van zijn attest-functie wordt de accountant niet gevraagd of de mate waarin de continuïteit van de geautomatiseerde gegevensverwerking is gewaarborgd voldoet (binnen gestelde grenzen) aan de door de accountant gestelde norm. Het enige wat een accountant in deze kan en mag doen is de feitelijke situatie toetsen aan een door het management gestelde norm.

Door het management gedefinieerde normen ontbreken meestal eveneens. Door zelf een norm te bepalen voor de te onderzoeken situatie - welke in belangrijke mate kan afwijken van die van het management - beweegt de accountant zich op het terrein van het management. Om te onderzoeken of in casu aan de gestelde is voldaan, is bepaalde deskundigheid nodig.

De uitkomsten van een onderzoek naar de mate waarin de continuïteit van de geautomatiseerde gegevensverwerking is gewaarborgd (i.c. voldoet aan managementnorm) kunnen resulteren in het aanpassen van de norm alsmede het aanbrengen van verbeteringen in het stelsel van getroffen maatregelen.
De mogelijkheid is echter eveneens aanwezig dat - om welke reden dan ook - de situatie ongewijzigd blijft. Het management aanvaardt dan echter bewust het risico van tekortkomingen in de getroffen maatregelen.

Voornamelijk op basis van kosten-nut-verhoudingen zal het management bepalen welke van de drie zal worden geëffectueerd. De uiteindelijke vraag waar het echter om gaat is of, zelfs indien de feitelijke situatie niet aan management eisen voldoet, dat invloed zal hebben op de te hanteren grondslagen en de af te geven verklaring. Het antwoord is negatief. Het enige punt waaraan de accountant aandacht dient te schenken - tevens om zijn eigen fungeren te beschermen - is het management ervan te doordringen dat het haar verantwoordelijkheid is en niet die van de accountant. Wel kan de accountant het management ondersteuning bieden bij het bepalen van - een voor dat bedrijf - haalbare norm.

4. Het gewekte vertrouwen

Uit literatuur over automatisering en controle blijkt nogal eens dat accountants zich een bepaalde deskundigheid aanmatigen als het om automatisering gaat. In de inleiding is reeds gesteld dat in de vakliteratuur als het over automatisering en controle gaat het woord betrouwbaarheid hand in hand gaat met continuïteit. Hiermee wordt derhalve tevens gesuggereerd dat de accountant deskundigheid bezit met betrekking tot de continuïteitsproblematiek ten aanzien van de automatisering.

Het mag dan zo zijn dat een aantal gespecialiseerde accountants die deskundigheid bezitten; tot de normale accountantsuitrusting behoort deze zeker (nog) niet. Gezien in het licht van de controle van de jaarrekening zitten hieraan gevaarlijke kanten. De indruk kan worden gewekt - bij de leiding en bij derden - dat de accountant dit gebied tot zijn jaarrekeningcontrole rekent (en dient te rekenen) en dat het afgeven van een verklaring impliciet inhoudt dat dit terrein ook is afgedekt.
Indien de accountant uit hoofde van de controle van de jaarrekening "enige" aandacht schenkt aan dit aspect - omdat het onderdeel is van administratieve organisatie en interne controle van de cliënt - en daarover rapporteert aan de leiding, kan eveneens de indruk worden gewekt dat het onderzoeken van de continuïteit van de geautomatiseerde gegevensverwerking tot de jaarrekeningcontrole-arbeid behoort en dat behoudens de door de accountant gemaakte signaleringen/opmerkingen de zaak wel voor elkaar is. Het alom gewekte vertrouwen inzake (gesuggereerde) deskundigheid van de algemene accountant op het gebied van automatisering loopt de accountant hier voor de voeten.
Zoals gesteld zijn voor dergelijke onderzoeken specialisten nodig die wel aanwezig zijn binnen verbijzonderde afdelingen van accountantskantoren en interne accountantsdiensten. Op verzoek ondersteunen zij de controlerend accountant.

Om dit gewekte vertrouwen niet te beschamen is het aan te bevelen bij aanvaarding van de opdracht tot controle van de jaarrekening of in jaarlijkse gesprekken met de opdrachtgever dit punt te bespreken en aan te geven dat de primaire verantwoordelijkheid voor de continuïteit van de geautomatiseerde gegevensverwerking (uiteraard) bij het management ligt en niet in de certificerende arbeid van de accountant is begrepen.

Wel kan - zoals reeds vermeld - de accountant (in casu de specialisten) onderzoeken of de feitelijke situatie aan de door het management gestelde eisen voldoet. Voorwaarde hierbij is wel dat een management-norm is aangegeven, al dan niet met ondersteuning van de accountant bepaald. Bij het ontbreken ervan dient de accountant zich af te vragen welke risico's hij loopt bij het aanvaarden van een dergelijke opdracht.

5. Consequenties voor de controle van de jaarrekening

Tot nu toe is gesproken over argumenten waaruit naar voren komt dat de accountant uit hoofde van de controle van de jaarrekening zich nagenoeg afzijdig moet houden als het gaat om (de beoordeling van) de continuïteit van de geautomatiseerde gegevensverwerking. Er zijn een drietal argumenten aan te voeren waarom eigenlijk wel aandacht aan dit continuïteitsaspect zou moeten worden besteed:

a. De basis voor de controle van de jaarrekening wordt gevormd door de administratieve organisatie en de daarin opgenomen maatregelen van interne controle van de desbetreffende onderneming.
Daarom verricht de accountant primair een onderzoek naar de AO en IC om - gezien zijn opdracht - een doelmatige controle te kunnen uitvoeren.
Tot deze AO behoort de "automatisering" waarvan ook het continuïteitsaspect deel uit maakt. Dit is een deelgebied dat echter voor de verdere uit te voeren controlewerkzaamheden van minder (of geheel geen) betekenis zal zijn. Het zal derhalve, evenals andere minder relevante deelgebieden, "globaal" worden onderzocht. Het probleem ligt hier bij de interpretatie van "globaal". Wat is "globaal" en welke verwachtingen worden gewekt bij het management indien erover wordt gerapporteerd (management-letter).

b. Niet voorbij mag worden gegaan aan het feit dat de accountant voor zijn controle-arbeid zelf gebruik maakt van die geautomatiseerde gegevensverwerking. De administratie van nagenoeg alle cliënten is geautomatiseerd. De accountant zal derhalve moeten nagaan wat de invloed in deze op zijn controle zal zijn indien de continuïteit in de gegevensverwerking en -verstrekking wordt doorbroken. Dit zou bijvoorbeeld bij verlies van gegevens in het meest extreme geval tot gevolg kunnen hebben dat een ander oordeel moet worden afgegeven wegens het ontbreken van "evidence" (bijvoorbeeld verschuiving van goedkeurend naar oordeelsonthouding). Door die oordeelsonthouding - alsmede de interpretatie ervan door derden - zouden kredietfaciliteiten kunnen worden beperkt, waardoor - in het ergste geval - de continuïteit van het bedrijf in gevaar kan worden gebracht.

c. Het derde argument - als aanvulling op het gestelde onder b. - is dat bij het niet voldoen aan de continuïteitseisen (gesteld vanuit de administratie) het moeilijker wordt de controle uit te voeren zoals gewenst en dat deze met extra kosten gepaard gaat.

Het lijkt aanbevelenswaardig deze punten met de opdrachtgever te bespreken om duidelijkheid te creëren.

6. De natuurlijke adviesfunctie

Naast de controlefunctie heeft de accountant nog altijd de daarin opgenomen "natuurlijke" adviesfunctie. Door het onder punt 4 uiteengezette "gewekte vertrouwen" verwacht de opdrachtgever ook op bepaalde zaken de automatisering betreffende te worden geattendeerd. Blijft de accountant op dit punt in gebreke dan zal dat - zeker ingeval van calamiteiten etc. - een beschuldigende vinger van de cliënt tot gevolg hebben. Dit attenderen geldt voor de automatisering "in house" maar krijgt een extra dimensie als de geautomatiseerde verwerking bij derden plaatsvindt. Attentiepunten in deze zijn de continuïteit van de geautomatiseerde gegevensverwerking alsmede de geheimhoudingsaspecten ten aanzien van gegevens.

7. De gevraagde adviesfunctie

In paragraaf 4 is terloops aangestipt dat binnen de grotere accountantskantoren alsmede de interne accountantsdiensten de benodigde specialistische kennis wel aanwezig is in de vorm van EDP-audit groepen. Daar is wel de kennis en ervaring aanwezig om een deskundig oordeel te geven over de mate waarin de continuïteit van de geautomatiseerde gegevensverwerking in bepaalde situaties is gewaarborgd. Dit is enerzijds geëffectueerd om toch de accountant in de algemene controlefunctie - indien nodig - deskundige ondersteuning te kunnen geven (de cliënt is koning) anderzijds een gevolg van het betreden van het terrein van de bijzondere EDP-audit (gevraagde adviesfunctie).

In de praktijk valt waar te nemen dat in toenemende mate een beroep wordt gedaan op de specifieke deskundigheid. Zowel de ontwikkelingen in het maatschappelijk verkeer als het feit dat ingezien wordt dat de automatisering steeds belangrijker wordt voor de continuïteit van de bedrijfsvoering, geven voeding aan het feit dat het management zich meer bewust wordt van de risico's die uit hoofde van automatisering worden gelopen.
De opdracht tot controle van de jaarrekening hoeft niet beperkt te blijven tot alleen de werkzaamheden om tot een oordeel (verklaring) omtrent de cijfers te komen. De cliënt kan wel degelijk een ruimere opdracht verstrekken en de accountant verzoeken om - bijvoorbeeld jaarlijks - te toetsen of de uit oogpunt van de continuïteit getroffen maatregelen van geautomatiseerde gegevensverwerking aan de door het management gestelde eisen voldoen. Bovendien kan de cliënt verzoeken om ondersteuning bij het definiëren van de management-norm en het "realiseren" van een adequaat stelsel van maatregelen. De continuïteitsproblematiek met betrekking tot automatisering heeft veel organisatorische aspecten. Om een adequaat stelsel van maatregelen te kunnen effectueren is een goede kennis van het bedrijf onontbeerlijk. De kennis van de controlerend accountant aangevuld met de specifieke kennis van de EDP-audit specialisten is een goede combinatie om ten aanzien van deze materie op optimale wijze in de gevraagde adviesfunctie van de cliënt te voorzien.

8. Conclusie

Misschien heeft de (accountant)lezer nu meer problemen dan voorheen. Maar één punt is duidelijk. De continuïteitsproblematiek ten behoeve van de geautomatiseerde gegevensverwerking kan en mag niet tot de controle van de jaarrekening worden gerekend. Wel wordt de accountant in toenemende mate geconfronteerd met de vraag wat te doen uit hoofde van de natuurlijke adviesfunctie waarbij in casu de noodzaak van deskundigheid naar voren komt. Bij die vraag spelen bovendien de ontwikkelingen in het maatschappelijk verkeer alsmede het gewekte vertrouwen in toenemende mate een rol.

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

COMPACT

Winter 1985/1986

BEOORDELING BETROUWBAARHEID VAN EEN (GEAUTOMATISEERD) INFORMATIESYSTEEM: De CASA-methode *

door A.H.C. Koedijk

1. ALGEMEEN

Inleiding

In dit artikel wordt een beschrijving gegeven van de in de cursus CASA (Cursus Aanpak Systeembeoordeling en Accountantscontrole) overgebrachte en toegepaste methode voor het beoordelen van de betrouwbaarheid van een (geautomatiseerd) informatiesysteem. Deze methode betreft een in de praktijk ontstane, op een functionele benadering gebaseerde werkwijze, die de laatste jaren meer systematisch is uitgewerkt.
Reeds hier wordt benadrukt dat, hoewel de methode "redeneert" vanuit in de computer vastgelegde gegevensverzamelingen (een steeds normaler wordende situatie), de methode in principe voor elk onderzoek naar betrouwbaarheidsaspecten van de Administratieve Organisatie toepasbaar is. Immers, een functionele benadering impliceert dat (zeker in eerste aanleg) meer wordt gekeken naar de functie (met andere woorden het "wat") en minder naar de wijze waarop (met andere woorden het "hoe").

Variatie in breedte en diepgang

Afhankelijk van de situatie, bij voorbeeld een onderzoek uitsluitend in het kader van de jaarrekeningcontrole of een alles-omvattend onderzoek in (speciale) opdracht van de "gecontroleerde", zal de breedte en diepgang van het onderzoek kunnen varieren. De CASA-methode verschaft dan ook in een aantal fasen de mogelijkheid om verengingen in het onderzoek aan te brengen.

Algemeen accountant versus EDP-auditor

De CASA-methode is ontworpen voor de algemene accountant, die naar heden ten dage mag worden verwacht wel over basiskennis van automatisering beschikt. Gebleken is, dat problemen bij systeemonderzoeken meer voortvloeien uit het ontbreken van "materiekennis" (kennis over de bedrijfsprocessen) dan uit het ontbreken van kennis over automatiseringstechniek. Dat betekent, dat de reeds bij de algemene

* zie ook de rubriek Onderwijs

accountant aanwezige materiekennis bij het onderzoek van informatiesystemen van groter belang is dan de bij EDP-auditors aanwezige automatiseringskennis.
De onontkoombare invloed van de automatiseringstechniek op de betrouwbaarheid noopt echter veelal wel tot behoefte aan bijstand van de EDP-auditor. De CASA-methode zal derhalve duidelijke momenten moeten kennen, waarop de inbreng van deze specialist gewenst/noodzakelijk zal kunnen zijn; daarnaast zal de inzet van deze specialist zo gericht en derhalve efficient mogelijk moeten kunnen geschieden.

Het is echter aan de primaire uitvoerder van het onderzoek, de algemene accountant dus., om te bepalen wanneer en in hoeverre deze inzet vereist is. Dit betekent, dat de automatiseringskennis van de algemene accountant zodanig moet zijn, dat deze hiertoe in staat is. In dit kader is inzicht in de "migration of controls" van bijzonder belang. In dit artikel wordt op dit onderwerp vrijwel niet ingegaan.

2. DE CASA-FASERING

Fasen

De volgende fasen worden onderkend:

I	Understanding the business & the overall system
II	Keuze van het te onderzoeken systeem ("Target system")
III	Algemene maatregelen: inventarisatie
IV	Understanding the target system
V	Opstellen raamwerk interne controle-eisen
VI	Inventarisatie bestaand interne controlestelsel
VII	Evaluatie interne controlestelstel
VIII	Opdracht aan EDP-auditor
IX	Opstellen/aanpassen Controleprogramma
X	Uitvoeren Controleprogramma (inclusief eventuele computer assisted audit techniques)

De CASA-methode voor systeemonderzoek omvat de fasen IV tot en met VIII; deze fasen worden behandeld in het volgende hoofdstuk (III). Het accent zal daarbij liggen op fase IV, daar deze fase het meest vernieuwend wordt geacht.

Hieronder volgt een korte beschrijving van de overige fasen.

Bedacht dient te worden dat de fasen I en II niet altijd behoeven te worden uitgevoerd daar uitvoering hiervan reeds in het verleden kan hebben plaatsgevonden in welk geval de organisatie reeds "door en door" bekend zal zijn.

Fase I: Understanding the business & the overall system

In de Cursus CASA wordt voor het verkrijgen van inzicht in en begrip van de organisatie (bedrijfsprocessen) en, op een hoog niveau, het informatiesysteem, de PRISMA-methode (produkt van KMG Klynveld Bosboom Hegener) gehanteerd. Ook de PRISMA-methode is gebaseerd op het onderkennen van (bedrijfs)functies. De PRISMA-methode wordt ondersteund door een geautomatiseerd documentatiesysteem. Dit systeem, APS+, biedt de mogelijkheid de verschillende PRISMA-schema's grafisch in te voeren en af te drukken.

Functionele benadering

Ofschoon het begrip "functie" in principe een top-down begrip is (functie: een deel van een systeem, dat de onderzoeker in het kader van het onderzoek niet verder onderverdeelt), en de PRISMA-methode ook een top-down methode, is het voor een goed begrip van belang te vermelden, dat het begrip "functie" ook enigszins een bottom-up karakter heeft. Het begrip "functie" kan namelijk worden gedefinieerd als "een cluster (groep) van gelijksoortige activiteiten (verrichtingen)". Maar juist door dit groeperen wordt uiteindelijk een globaal inzicht verschaft, dat, naar behoefte, verder kan worden gedetailleerd, eventueel tot op het laagst denkbare niveau.

Het schijnbaar tweeslachtige karakter van het begrip functie zal eveneens naar voren komen bij de latere behandeling (hoofdstuk III) van de CASA-methode. Ook wordt nu reeds gewezen op het verschil tussen het hierna behandelde "Bedrijfsfunctie"-begrip en het bij de CASA-methode te behandelen begrip "(Beheersbare) Systeemfunctie".

Een groep van gelijksoortige bedrijfsactiviteiten wordt door PRISMA "Bedrijfsfunctie" genoemd, dit in tegenstelling tot "Posities" (afdelingen, personen; met andere woorden het organisatieschema).

Fase II: Keuze van het te onderzoeken systeem ("Target system")

Resultaat van Fase I is onder meer inzicht op een conceptueel niveau in:
-de informatiestromen tussen bedrijfsfuncties onderling en tussen de bedrijfsfuncties en "het informatiesysteem" (dat hier gezien kan worden als het volledige stelsel van handmatige en geautomatiseerde applicatiesystemen);
-de gegevensverzamelingen.

Het begrip gegevensverzameling is eveneens een conceptueel begrip; een gegevensverzameling bevat als het ware een registratie van "eigenschappen" van "objecten" (objecttypen zijn bij voorbeeld Personeel, Klant, Factuur, Leverancier, Artikel). Hoe deze gegevensverzamelingen hun weerslag vinden respectievelijk hebben gevonden in bestanden,

wordt in een latere fase vastgesteld.

Toepassing van risico-analyse zal leiden tot het definieren van welke gegevensverzamelingen in het kader van de accountantscontrole van belang zijn (relevantie in het kader van de verantwoording).

De "target" gegevensverzamelingen zullen vervolgens gerelateerd worden aan de in "het informatiesysteem" van de organisatie aanwezige fysiek bestaande hoofdbestanden en mutatie- dan wel transactiebestanden, waarna de "target"-bestanden bekend zijn.

Vervolgens zal worden vastgesteld welke werkelijk bestaande applicatie(sub)systemen deze bestanden muteren en raadplegen, waarna de "target"-(sub)systemen bekend zijn. Deze (sub)systemen vormen dan object van onderzoek door de accountant, indien althans wordt gekozen voor een systeemgerichte controlebenadering. Wanneer wordt gekozen voor een gegevensgerichte controlebenadering kan na het vaststellen van de "target"-bestanden en een analyse hiervan voortgezet worden met fase IX.

Het gebruik van de term (sub)systemen duidt er reeds op, dat een verenging tot slechts een deel van het applicatiesysteem dat zal behoeven te worden onderzocht, hier al mogelijk is. Voorts zal op basis van aanwezige bedrijfsrisico's, controledoelstellingen en controlerisico's een nadere definiering van breedte en diepgang van het uit te voeren onderzoek moeten worden vastgesteld.

Fase III: Algemene maatregelen: Inventarisatie

Het betreft hier een eerste beoordeling van de automatiseringsorganisatie en van de organisatie van de automatisering. De vereiste diepgang blijft hier buiten beschouwing; in elk geval zal echter duidelijk moeten worden, of er al dan niet een verhindering is om systeembeoordeling als controlebenadering toe te passen.

(Voor de fasen IV tot en met VIII: zie het volgende hoofdstuk).

Fase IX: Opstellen/aanpassen Controleprogramma
Fase X: Uitvoeren Controleprogramma

Op deze fasen wordt in dit artikel niet ingegaan.

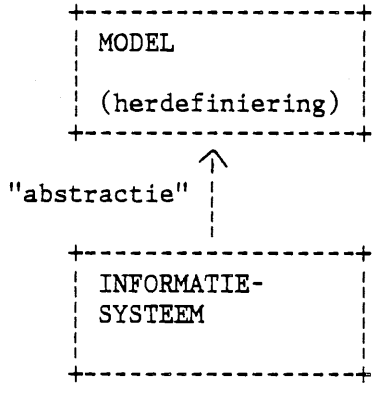
3. DE CASA-METHODE

Inleiding

De CASA-methode betreft een op een functionele benadering gebaseerde aanpak voor het beoordelen van informatiesystemen. Doordat het een functionele benadering betreft is sprake van een top-down methode. Hieruit vloeit voort, dat niveaus van detaillering per "functie" naar behoefte mogelijk zijn.
Tevens vloeit uit de functionele benaderingswijze per definitie voort, dat geabstraheerd wordt van de technische uitwerking; aangezien er echter uiteindelijk een oordeel moet worden gevormd over een op een bepaalde wijze technisch geimplementeerd systeem, kan dit abstraheren van techniek vanzelfsprekend niet altijd tot het einde toe vol worden gehouden. Daar waar de techniek in de beschouwing moet worden betrokken (fase VI), kan inzet van een daarop gespecialiseerde EDP-auditor noodzakelijk zijn.
Primair richt de CASA-methode zich op het beoordelen van de opzet van het systeem. Uiteraard wordt ook het verifieren van het bestaan van bepaalde controlemaatregelen als onderdeel van het onderzoek beschouwd. De "werking" wordt voor zover nodig getest uit hoofde van fasen IX en X.

Fase IV: Understanding the target system

In deze fase wordt een model van (de opzet van) het geselecteerde applicatiesysteem vervaardigd door de onderzoeker (de algemene accountant). Het systeem wordt als het ware geherdefinieerd en wel op zodanige wijze, dat het model de "beheersbare systeemfuncties" (waarover zo meer) duidelijk zichtbaar maakt.



Waarom is deze herdefiniering nodig?

Nog los van de omstandigheid, dat systeemdocumentatie veelal onvolledig, verouderd, te gedetailleerd of dergelijke is, is deze systeemdocumentatie in ieder geval gewoonlijk meer gericht op programma-onderhoud en daarom meer op het trajectmatige (dus de wijze waarop iets werkt) georienteerd en minder op het functionele.
Zelfs indien er een functionele systeembeschrijving (functioneel ontwerp) aanwezig is, zal doorgaans ook deze documentatie niet zonder meer voldoen aan wensen van accountants. Dit wordt veroorzaakt door de vage definitie van het begrip functie. De doelstelling zal per onderzoek, project en dergelijke varieren; per geval zal dan ook de definitie van het begrip functie nader moeten worden uitgewerkt. Voor de CASA-methode heeft dit geleid tot het invoeren van het begrip "beheersbare systeemfunctie".

Het begrip beheersbare systeemfunctie wordt onder handhaving van de top-down gedachte als volgt gedefinieerd:

> Op grond van
> -gelijksoortigheid van toe te passen interne controle-technieken ten aanzien van de volledigheid en de juistheid en
> -relaties met bevoegde bedrijfsfuncties
> samengebundelde systeemverrichtingen.

Deze definitie omvat een concrete en werkbare "vertaling" van de doelstelling van het accountantsonderzoek, namelijk een oordeel over de betrouwbaarheid van het informatiesysteem. Dit betekent overigens, dat als het onderzoek zich op andere aspecten richt, bij voorbeeld effectiviteit of efficiency, de CASA-methode dan niet zonder meer toepasbaar is. Een bijstelling van het functie-begrip zal als eerste stap noodzakelijk zijn.

Voorbeeld

Een artikelrecord bevat de volgende gegevens:

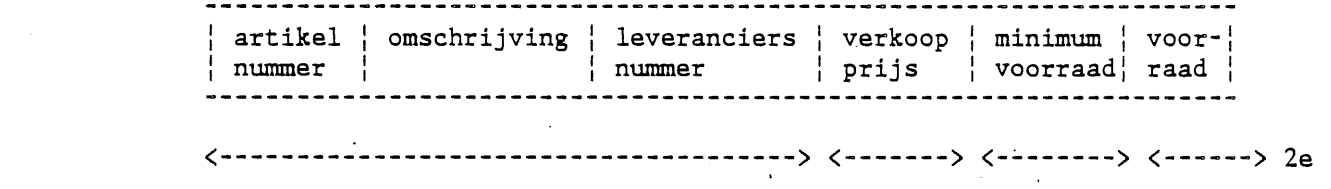
artikel nummer	omschrijving	leveranciers nummer	verkoop prijs	minimum voorraad	voor-raad

<----------> <-----> 1e

Stel een applicatiesysteem dat het artikelbestand "update".

Op grond van het onderscheid tussen zogeheten "vaste" gegevens en "variabele" gegevens wordt uit hoofde van de definitie van beheersbare systeemfunctie een eerste onderscheid gemaakt in twee systeemfuncties.

De achterliggende gedachte is, dat ten aanzien van deze twee soorten gegevens in het algemeen verschillende soorten interne controletechnieken zullen worden toegepast. Mutaties op vaste gegevens immers zijn in het algemeen qua aantal relatief gering; bovendien leidt een fout in het wijzigen van vaste gegevens al gauw tot een "waterval" van fouten (een systematische fout). Een foute wijziging in de verkoopprijs zal bijvoorbeeld kunnen leiden tot een groot aantal foutieve facturen.
Fouten in het wijzigen van de variabele gegevens zijn uiteraard ook niet leuk, doch vormen een incidentele fout. Bovendien worden dit soort fouten nogal eens door andere maatregelen gedetecteerd (bij voorbeeld de verbanden tussen de geld- en goederenbeweging, inclusief voorraadopnames). Daarnaast kan worden gesteld, dat transacties die leiden tot wijziging van de variabele gegevens in het algemeen qua aantal relatief groot zijn. (We hopen, dat we een artikel vaker verkopen, dan dat we de prijs ervan moeten wijzigen).
Voor de interne controle betekent dit, dat wijzigingen in de vaste gegevens veelal in de greep worden gehouden door middel van visuele detailcontrole op de output (meer in het algemeen gesteld: integrale controle op de juistheid en de autorisatie), terwijl wijzigingen in de variabele gegevens meer door middel van totalen en verbanden in de greep zullen worden gehouden.



Bij nadere beschouwing valt echter een verdere opsplitsing van, in dit geval, de vaste gegevens door te voeren. Dit gebeurt dan uit hoofde van de definitie op grond van de relaties met de bevoegde, van elkaar te scheiden, bedrijfsfuncties. Het is bijvoorbeeld denkbaar dat van elkaar gescheiden moeten worden:
-artikelnummer, omschrijving, leveranciersnummer;
-verkoopprijs;
-minimumvoorraad.

Stappen in Fase IV

De volgende stappen worden binnen deze fase onderscheiden:

1. Analyse van de inhoud van hoofdbestanden.
2. Definieren van de gegevensstromen.
3. Definieren van de systeemfuncties.
4. Verificatie.

Stap 1

Als concreet uitgangspunt voor deze stap worden de recordlay-outs van de fysiek aanwezige hoofdbestanden (masterfiles) benut. Een hoofdbestand is: een reservoir met gegevens van een langdurige betekenis (stam- en standengegevens). Dit in tegenstelling tot een transactie- of mutatiebestand, waarin zich gegevens met een tijdelijke betekenis bevinden, namelijk ten behoeve van het bijwerken van de gegevens in hoofdbestanden.
Ten behoeve van het verkrijgen van begrip van de in de recordlay-outs voorkomende gegevens (velden, rubrieken, items) is het noodzakelijk interviews te houden. In eerste aanleg komen voor deze interviews in aanmerking de eindgebruikers, die tenslotte maximaal over de benodigde materiekennis beschikken. Voor puur automatiseringstechnische velden zal een interview met automatiseringsmensen als aanvulling nodig kunnen zijn.

Uiteindelijk gaat het erom, dat de in de hoofdbestanden voorkomende gegevens worden gegroepeerd volgens de in de vorige paragraaf beschreven gedachtes.

Indien het ingewikkelde gegevensopslagstructuren betreft, bij voorbeeld data bases, kan enige bijstand van een EDP-auditor bij het "lezen" van de recordlay-outs wenselijk zijn.

Stap 2

Gerelateerd aan de in de vorige stap onderscheiden gegevensgroepen in de hoofdbestanden kunnen de "gegevensstromen" (gegevensgroepen in invoer en uitvoer) worden gedefinieerd; dit zijn de in het model te onderscheiden (conceptuele) mutaties en transacties.
Een bottom-up verificatie kan geschieden aan de hand van overzichten van de (werkelijke) transactiesoorten, menuschermen en dergelijke.
Naast het onderscheid tussen mutaties/transacties op vaste/variabele gegevens, dienen te worden onderscheiden door de computer gegenereerde transacties, zoals bijvoorbeeld prolongatiepremies, genereren van inkooporders en dergelijke. Voor deze groep door de computer gegenereerde transacties gelden weer andere beheersmaatregelen (standenregisters, programmatests).

Stap 3

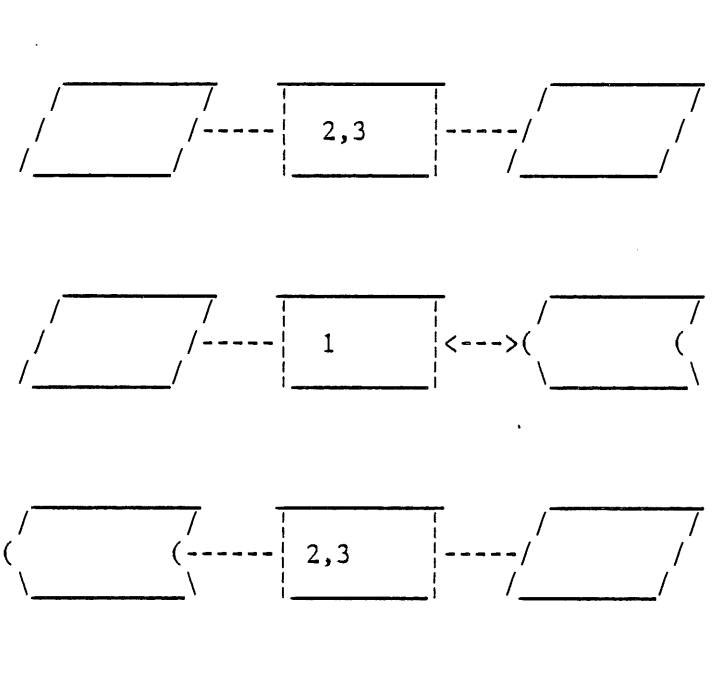
De koppelingen tussen de gegevensgroepen in de hoofdbestanden en de gegevensstromen worden gevormd door de systeemfuncties. Voor een goed begrip wordt opgemerkt, dat zo'n (conceptuele, ofwel modelmatige) systeemfunctie in werkelijkheid kan bestaaan uit:
-één applicatieprogramma, of
-meerdere applicatieprogramma's, of
-een deel van een applicatieprogramma.

Een systeemfunctie bestaat derhalve uit tot een groep gebundelde systeemverrichtingen. Hoe de bundeling tot stand komt wordt bepaald door de relaties met de gegevensgroepen in de hoofdbestanden (zie Stap 1).

De volgende typen systeemfuncties worden onderkend:
1. Opbouwen en onderhouden van gegevensgroepen in hoofdbestanden.
2. Uitvoeren van bewerkingen (reken- en beslissingsregels).
3. Verstrekken van informatie.

Qua relaties met gegevensgroepen in hoofdbestanden en met gegevensstromen zijn systeemfuncties alsvolgt te onderscheiden:

(de in de functies vermelde nummers
verwijzen naar de indeling hierboven)



voorbeelden

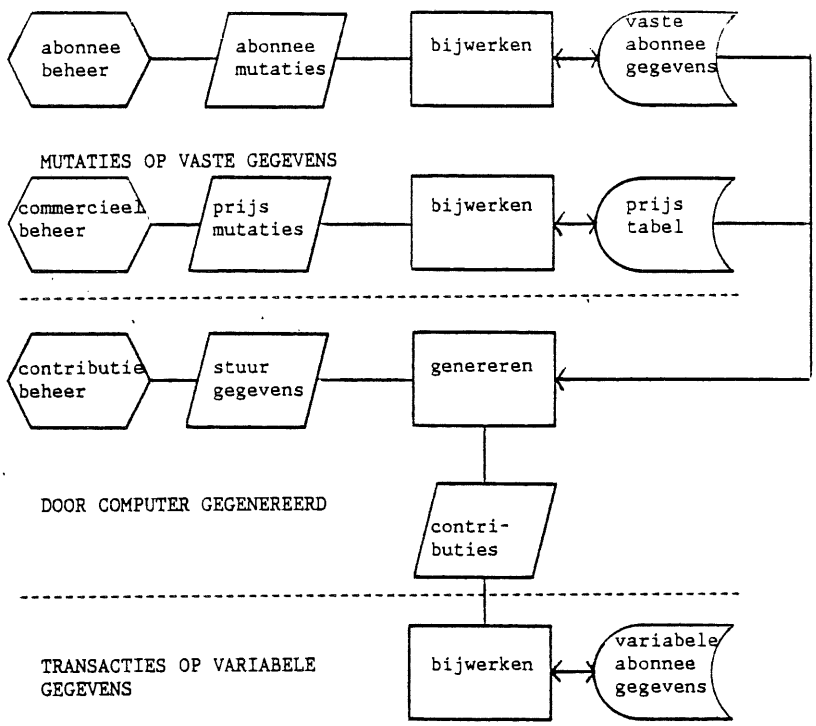
-periodiek overzicht transacties

-bijwerken artikel-prijzen
-verwerken verkoop-transacties

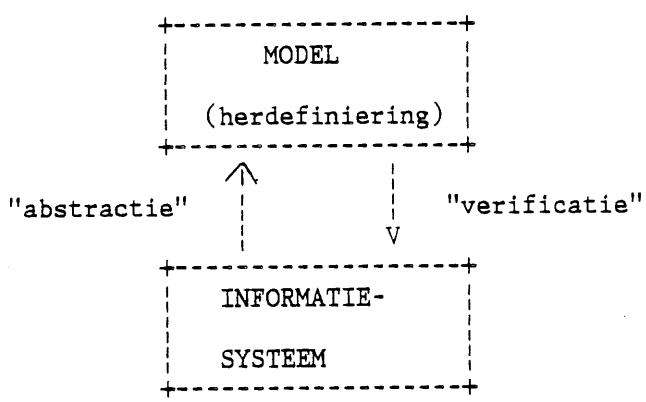
-debiteuren saldilijst
-voorraad inquiry
-genereren prolongaties

(N.B.: Bij elke functie is het denkbaar -waarschijnlijk-, dat bovendien nog (gegevensgroepen in) hoofdbestanden worden geraadpleegd; dit is in de schema's hierboven niet afzonderlijk tot uitdrukking gebracht).

Voorbeeld



Stap 4



Het model wordt voornamelijk opgebouwd door middel van interviews en "groene tafel denken" (oftewel het inzetten van menselijk logisch denkvermogen). Dit betekent, dat in deze "abstractie-fase" natuurlijk fouten kunnen worden gemaakt, bijvoorbeeld interpretatiefouten. Ook is het denkbaar, dat het model de werkelijkheid onvolledig weergeeft. Dit noopt tot verificatie van het model aan de werkelijkheid.

Een belangrijk middel hiertoe wordt gevormd door terugkoppeling naar de informanten. Het model moet voorgesteld worden als schematische weergave in combinatie met een verbale toelichting. (Voor schematische weergave is voor CASA een tekentechniek/conventie ontwikkeld, die sterk lijkt op de welbekende stroomschema's; u hebt er hierboven mee kennis gemaakt). Dit model, dat als het ware de functionele interpretatie van het over het systeem meegedeelde bevat, kan aan de informanten worden voorgelegd ter verificatie.
Daarnaast kunnen de reeds genoemde keuzemenu's, alsmede in- en uitvoerdocumenten, en dergelijke worden benut.
Voorts wordt op deze plaats herinnerd aan het concrete uitgangspunt, namelijk de beschrijvingen van de hoofdbestanden, dat voor al te grote dwalingen zal behoeden.

Nadere bepaling breedte en diepgang in Fase IV

Denkbaar is dat het uiteindelijk model functies zichtbaar maakt, die niet vooraf waren onderkend. Dit betekent, dat alsnog voor die functies moet worden bepaald of ze object van onderzoek zullen vormen of niet.

Fase V: Opstellen raamwerk interne controle-eisen

Deze eisen moeten in algemene termen worden gedefinieerd, niet in termen van interne controletechnieken. (Welke oplossing -technische uitwerking- een organisatie kiest, respectievelijk heeft gekozen, is in principe in eerste instantie háár aangelegenheid).

De eisen zijn globaal in twee groepen te verdelen:
1. Per in het model gedefinieerde systeemfunctie: de eisen ten aanzien van juistheid, volledigheid, geoorloofdheid (relatie met de bedrijfsfunctie), tijdigheid en controleerbaarheid;
2. De overall eisen (verbanden), die over de functiegrenzen heen gaan (bij voorbeeld ten behoeve van de Financiele Administratie in haar interne controlefunctie).

De eisen dienen gemotiveerd te worden in termen van
-bedrijfsrisico's (in rapportage naar de gecontroleerde toe), zodat management een goede basis krijgt voor de beslissing al of niet te voorzien in geconstateerde leemtes;
-controlerisico's (in interne rapportage), ten einde een goede basis te verschaffen voor aanpassing van het Controleprogramma.
Hiermee is dus een concreet, uitgewerkt alternatief gevonden voor de in de "mededeling"-tekst van NIvRA 26 gehanteerde "redelijkerwijs te stellen eisen".

Fase VI/VII: Inventarisatie en Evalutatie

Per eis wordt nu gericht geinventariseerd of maatregelen zijn getroffen die maken, dat aan de eis is "voldaan". Het gaat hier dus om het zoeken naar interne controletechnieken die in het systeem zijn opgenomen.
Het voordeel van de CASA-methode is, dat dit zoeken zeer gericht geschiedt: men weet precies in welke richting men moet zoeken.

Een eenvoudig formulier kan in het proces van onderzoek worden gehanteerd:

functie	eis	aangetroffen maatregel (interne controle-techniek)	evalutie

In deze fase zal de invloed van de automatiseringstechniek vanzelfsprekend merkbaar worden. Globaal is deze invloed in twee groepen te verdelen:
-de invloed van de verwerkingsmethode, met andere woorden het verschil tussen batch verwerking en on-line/real-time verwerking alsmede het scala aan variaties daar tussen;
-de verschuiving van controlemaatregelen vanuit de applicatie en de organisatie naar overkoepelende systeemsoftware ("migration of controls"); op dit moment is dit vooral van toepassing op in data base management en teleprocessing monitor software opgenomen controlemaatregelen.

(Op deze laatste groep controlemaatregelen wordt met name ingegaan in de KKC-cursus GGV, Controle bij Geïntegreerde Gegevensverwerking.)

Kennis van en inzicht in deze invloeden is van belang om te weten waar naar maatregelen moet worden gezocht.

Fase VIII: Opdracht aan EDP-auditor

Inzet van een op automatisering en controle gespecialiseerde EDP-auditor zal nodig kunnen zijn:
-ten aanzien van de naar overkoepelende systeemsoftware gemigreerde controlemaatregelen;
-indien de betrouwbaarheid (mede) afhangt van in de applicatieprogrammatuur opgenomen reken- en beslissingsregels, waarvan het bestaan moet worden geverifieerd door middel van testen/source-code-review;
-indien tevens gesteund moet worden op maatregelen en procedures in de automatiseringsorganisatie.

De inzet van de EDP-auditor kan nu echter zeer gericht geschieden; de specifieke deskundigheid van de EDP-auditor wordt maximaal gebruikt.

4. CASA: RAPPORTAGE

In de meest uitgebreide vorm van rapportage naar de gecontroleerde wordt de volgende rapportindeling voorgesteld:

1. Inleiding; kader: Jaarrekeningcontrole of specifieke opdracht
   Doel van het onderzoek
   Breedte (verwijzing naar bijlage 1) en diepte.
2. Oordeel/conclusie (verwijzing naar bijlage 2).
3. Voornaamste bevindingen en aanbevelingen.
4. Overige bevindingen en aanbevelingen.

bijlagen bij het rapport

1a. Functioneel systeemschema.
1b. Functionele systeembeschrijving.
2. Raamwerk van interne controle-eisen.
3. Inventarisatie en Evaluatie.

Bijlagen 1a/b vormen het automatisch eindproduct van fase IV (Understanding the system). Bijlage 2 vormt het automatisch eindproduct van fase V (Opstellen Raamwerk). Bijlage 3 vormt het automatisch eindprodukt van fase VI/VII/VIII (Inventarisatie en Evaluatie, EDP-audit).

Doordat in bijlage 1 duidelijk moet zijn aangegeven wat object van onderzoek is geweest, is daarmee impliciet aangegeven wat niet tot het onderzoek heeft behoord. (Bedacht moet worden, dat in de systeembeschrijving duidelijk moet zijn aangegeven, welke systeemverrichtingen zijn meegebundeld in de door de onderzoeker gedefinieerde systeemfuncties en welke daadwerkelijke transactiesoorten zijn meegebundeld in de gegevensstromen.)

5. CASA: SYSTEMEN IN ONTWIKKELING

In het voorgaande is steeds uitgegaan van operationele systemen. De CASA-methode kan echter eveneens worden toegepast bij systemen in ontwikkeling. Juist door de functionele benadering is de methode bijzonder goed toepasbaar in de eerste, meer conceptuele trajecten van de systeemontwikkelingscyclus.

In systeemontwikkeling wordt onderscheid gemaakt (fasering) in de totstandkoming van het logisch (functioneel) ontwerp en van het technisch ontwerp. De methode ondersteunt de accountant bij het participeren in de totstandkoming van het logisch ontwerp.

Indien de accountant niet actief deelneemt aan het ontwikkelingsproces kan na gereedkoming van het logisch ontwerp de CASA-methode voor wat betreft de fasen IV en V worden uitgevoerd, aannemende dat (tenminste voorlopige) beschrijvingen van gegevensverzamelingen bekend zijn.

Nadat het technisch ontwerp beschikbaar is gekomen, kunnen de door de accountant gestelde eisen worden vertaald in aanbevelingen omtrent op te nemen betrouwbaarheidsmaatregelen; met andere woorden er kunnen in dat geval oplossingsgerichte aanbevelingen worden gedaan.

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

o o o o o een fout in een vast gegeven o o o o o

'I believe you have a complaint about an inaccuracy on our data file, madam'

ACCOUNTANCY DECEMBER 1985

Naschrift van de schrijver →

NASCHRIFT BIJ ARTIKEL "DE CASA-METHODE"

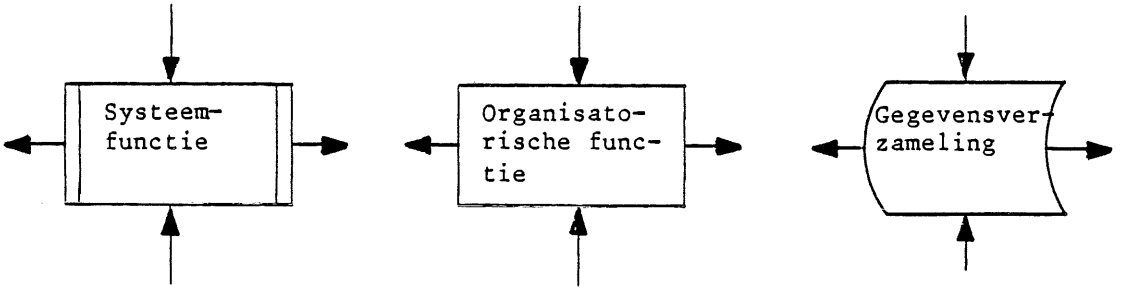
door A.H.C. Koedijk

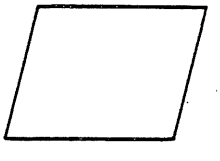
De in het artikel gehanteerde schematechniek voor het weergeven van de functies van een informatiesysteem heeft de (u waarschijnlijk vertrouwde) stroomschemavorm, zoals die in de huidige versie van de CASA-cursus wordt toegepast. Een dergelijk schema laat zich "normaal" lezen, namelijk van boven naar beneden en van links naar rechts, tenzij u door pijlen een andere richting wordt opgestuurd.

Onder invloed van het beschikbaar komen van computerhulpmiddelen zal meer en meer worden overgegaan naar een andere schematechniek, die van het geautomatiseerde documentatiesysteem APS+.
De in APS+ toegepaste schematechniek is gebaseerd op de N2 (N square) chart van Lano. De N2 chart is geïntroduceerd door R.J. Lano in het boek "A technique for Software and Systems Design". Uitgeverij North Holland, Amsterdam, 1979. Deze chart wordt ook reeds in PRISMA gebruikt.
De toegepaste matrix-vorm leent zich beter om te worden geautomatiseerd dan de "free format" schematechniek uit de huidige cursus-versie.

Met betrekking tot de schematechniek gelden onder meer de volgende conventies:
- De organisatorische en externe functies, de systeemfuncties en de gegevensverzamelingen staan op de diagonaal van de matrix.
- Door functies opgeleverde (= uitgaande) gegevensstromen worden weergegeven op de regels van het schema (ofwel horizontaal).
- Door functies ontvangen (= ingaande) informatiestromen staan in de kolommen van het schema (ofwel verticaal).

Schematisch als volgt:



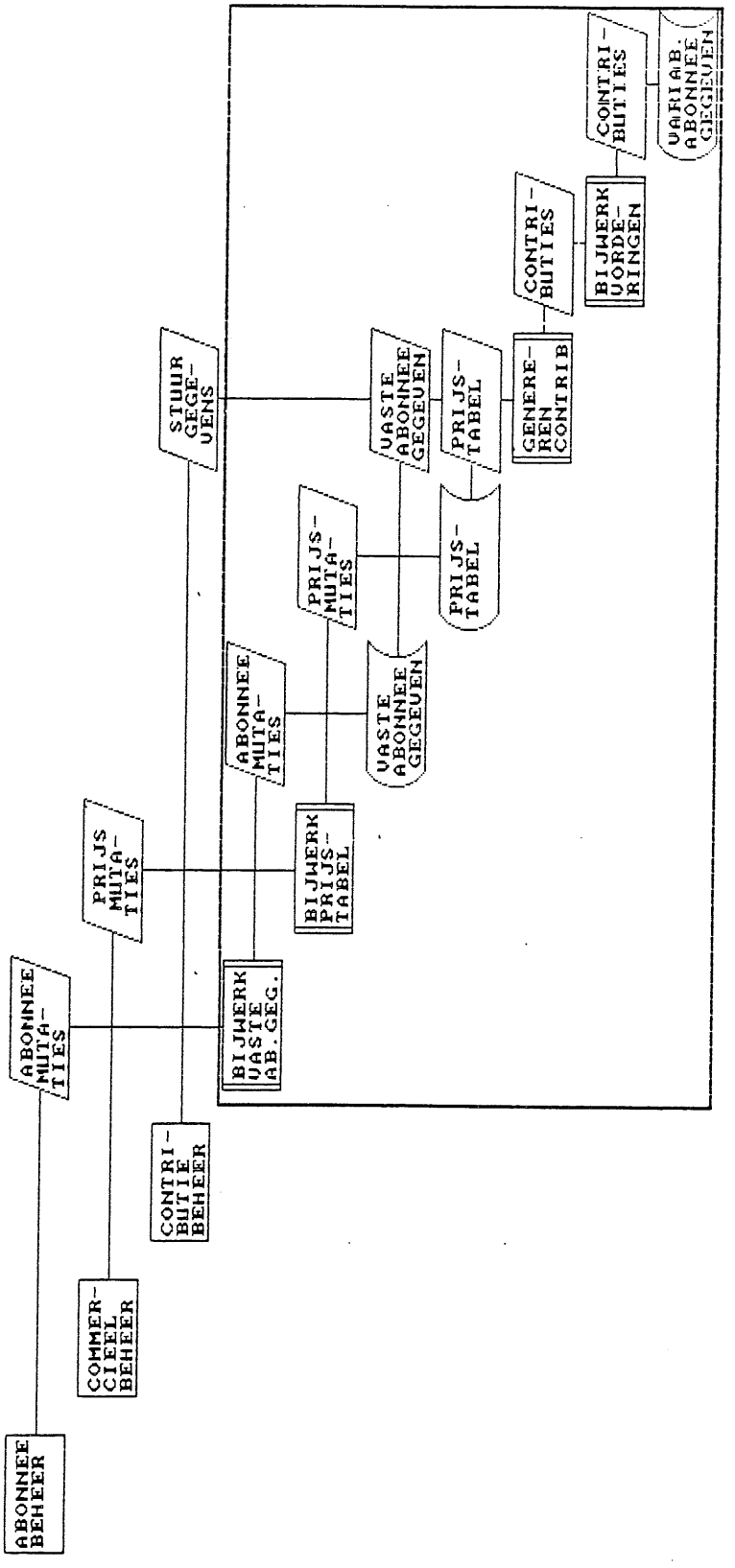
Daarnaast wordt het symbool  gebruikt voor de gegevensstromen.

Het voorbeeld inzake het abonneesysteem bij stap 3 van fase IV van bovengenoemd artikel is in de schematechniek APS+ weergegeven in schema 1 (zie volgende pagina). Schema 1 kan vereenvoudigd worden door samenvoeging van systeemfunctie en gegevensverzameling in één symbool; zie schema 2. De inzichtelijkheid van het schema wordt door de vereenvoudiging wellicht verbeterd omdat het schema minder symbolen bevat.

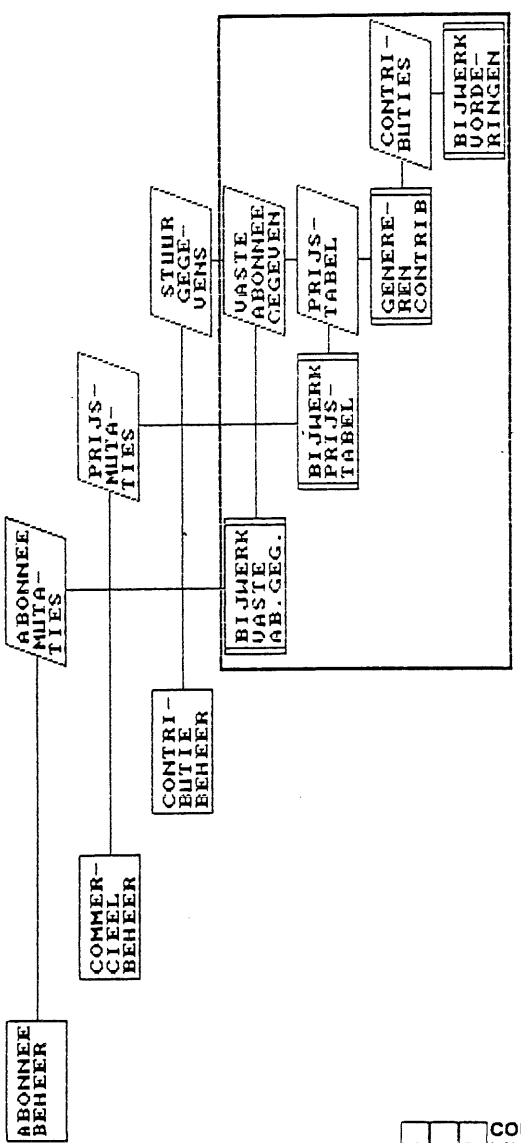
Overigens zij nog vermeld, dat APS+ ook de mogelijkheid biedt elke (sub)-functie als het ware "op te blazen" tot een nieuw schema, waardoor een goede "top-down benadering" mogelijk wordt.

Overigens zij nog benadrukt, dat het hier in APS+ uitgewerkte voorbeeld uitsluitend betrekking heeft op de CASA-fase "Understanding the target system". Maatregelen van interne controle zijn hierin nog niet weergegeven.

Schema 1: CASA-fase "Understanding the system"
schema in APS+



Schema 2: CASA-fase "Understanding the system"
gecomprimeerd schema in APS+



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

IDENTIFICATION AND EVALUATION OF OPERATING SYSTEM CONTROLS (USING IBM'S MULTIPLE VIRTUAL STORAGE (MVS) OPERATING SYSTEM AS AN EXAMPLE)

door H. Weerd

Dit artikel vormt een der bijdragen - namelijk te zamen met het boek "Auditing the Technical EDP Organisation" van mw. M.E. van Biene-Hershey en de voordracht van H.J. Dain over het onderwerp "Change Management at N.V. Philips Computing Centre Eindhoven - op het Symposium "Auditing van de EDP-organisatie", georganiseerd door de Sectie EDP-auditing van het Nederlands Genootschap voor Informatica op 3 december 1985 in de RAI te Amsterdam.

Het in het Engels geschreven artikel geeft de controle-aanpak specifiek voor MVS weer. Het gaat om een diepgaand onderzoek, waarbij de schrijver niet kon ontkomen aan het gebruik van "geheimtaal".

In een tiental hoofdstukken wordt de problematiek uit de doeken gedaan:

1. Introduction
2. Risk areas
3. The technical support function
4. MVS
5. Installation management and change management
6. Some Major Threats/Controls
7. Security Policy for an MVS installation
8. Computer Security Audit
9. MVS Security Audit
10. To Conclude

1. Introduction

The purpose of this paper is to present an overview of main security areas of an operating system, using MVS as an example. An overall approach for a computer security audit, including an evaluation of operating system controls (an MVS security audit), is outlined.

2. Risk areas

Within the domain of computer security, risks can be divided into six EDP risk areas, from where threats can arise.
These risk areas are:
1. ORGANIZATION: People and Procedures;
2. CORPORATE DATA;
3. APPLICATIONS;
4. SYSTEM SOFTWARE;
5. HARDWARE;
6. ENVIRONMENT.

Each risk area has its own characteristics for which security measures have to be taken to minimize the possible impact of threats.

Within the scope of this paper I will focus on the risk area of system software and its relation to the risk areas of organization, hardware and environment.

3. The technical support function

The major activities of the technical support function for an MVS installation are:
- planning for the implementation of new operating system software;
- planning changes to existing operating system software;
- planning hardware changes;
- tailoring the operating system to fit the devices of the installation;
- tuning the operating system to fit the workload of the installation;
- adapting the operating system to integrate with other software such as IBM subsystems or products delivered by other suppliers;
- providing technical support to other DP-departments.

In many installations the activities performed by the technical support function are only loosely controlled.

4. MVS

4.1 The MVS operating system

Multiple Virtual Storage (MVS) is the operating system supplied by IBM to operate and control its medium and large mainframes. The various system features are supplied in Selectable Units (SU's) and, in their complete form, are made up of millions of lines of coding and can occupy 16 mega bytes of core storage [0]. More recently IBM is providing its customers with "Custom-Built" MVS operating systems. A selection of the parts of the MVS operating system for a particular installation is then already done by IBM.

4.1.1 Systems datasets

Some of the main systems datasets are:

SYS1.NUCLEUS - Operating systems nucleus and initialization code
SYS1.LINKLIB - All executable programs that are frequently used
SYS1.LPALIB - Virtual link library (Pageable Link Pack Area): contains non I/O SVC modules
SYS1.SVCLIB - SVC I/O modules
SYS1.PROCLIB - Initial procedures library
SYS1.LOGREC - Log of major hardware and software errors
SYS1.PARMLIB - System parameters for initialization includes:
IEASYS - System parameters
SMFPRM - SMF parameters
IEAAPF - List of authorized libraries

VSAM Catalogue - Primary system catalogue
SYS1.HASPACE - JES dataset for spooling, input and output data
SYS1.HASPCKPT - Restart information for JES
SYS1.MANX/Y - SMF datasets
SYS1.SMPLOG - SMP log dataset
SYS1.CDS - Status of the distribution libraries

SYS1.UADS - TSO-user attributes
SYS1.VTAMLST - Description of the VTAM-applications

4.1.2 Dataset cataloguing

Disk datasets are automatically catalogued within MVS. However, tape label checking is restricted to the last 17 characters of the dataset name and can be bypassed by specifying Bypass Label Processing (BLP) at job submission.

MVS tape management facilities are clearly inadequate and most users acquire a tape cataloguing package which provides automatic librarian facilities and allows the full 44 characters of tape labels to be checked. An example of such a package is UCC1.

4.1.3 Mode of operation

Like most operating systems MVS allows programs to operate in either Authorized or Problem state. The latter is the normal operation of an application program within the boundaries of that program. Authorized state is a privileged operating mode which crosses the boundaries of application programs and virtual storage and allows MVS to control the mainframe and its peripheral devices. Programs able to operate in this state are able to issue commands to the operating system in the form of (restricted) Supervisor Calls (SVC's). These programs represent part of the system rather than applications software of the computer and must be defined to MVS as Authorized Programs and included in a library designated as authorized to the MVS Authorized Program Facility (APF).

4.1.4 Integrity of system software

One of the design objectives of IBM for the MVS operating system is the ability of the MVS system to protect itself against unauthorized user access, to the extent that security controls cannot be compromised. There should be no way for any unauthorized program, using the system interface to obtain control in an authorized state, to bypass store/fetch protection (to prevent write/read access to portions of main storage) or to bypass the access control system.
This ability of the MVS system is called the integrity of its systems software. IBM is committed to immediately correct any error or failure in the MVS system that compromises this integrity [6].

4.1.5 Job control handler

Job control statements are handled by a subsystem of MVS called Job Entry Subsystem (JES2).

The main functions of JES2 are to control local and remote job entry and output devices. JES2 serves as the point of entry for all jobs and can produce hard-copy job output. Jobs can be routed to another node in a network job entry system (NJE) for execution and/or output processing. The internal reader facility allows MVS-modules to submit system jobs, started tasks, and time-sharing log-ons. This facility also allows application programs to submit jobs.

JES2 reads jobs into the spool-file. Each JES2 processor has access to the spool-file and independently selects jobs for processing from the spool-file.
After job execution JES2 handles the spooling for printing and punching and finally purges the spool-file.

4.1.6 Access control

MVS provides limited access control facilities restricted to password protection of datasets, and password and identification checks of related systems software products such as communications software. This is clearly inadequate protection for a network of any size.

A number of software packages provide access control and related [1] functions on top of MVS. The market for these programs appears to be growing as users become more concerned about security. Examples are ACF2'), RACF, SAC, SECURE and Top Secret.

Basic functions provided by such packages are:
- authenticating users;
- maintaining access control information;
- checking authorization for system access;
- checking authorization for resource access;
- logging;
- producing reports.

The aim of Access Control Software (ACS) is to protect resources.
The problem is that a resource has to be identified to the ACS. For example an IMS-transaction can be protected with ACS, but the functions of which the transaction is composed can sometimes not be identified to the ACS.

4.1.7 Time sharing and programming aids facilities

Time Sharing Option (TSO) is an integral part of MVS and provides interactive computing for large systems. A TSO user has for example access to:
- 16 million bytes of address space.
- Comprehensive, easy to use edit facility: TSO/EDIT.
- Powerful command list facility (CLIST) which can be used to create and catalogue frequently used command procedures.
- Remote Job Entry (RJE) link from user libraries to JES.

') ACF2 release 3.1.3 has been evaluated by the American Department of Defense (DoD) against the requirements specified by the DoD.
The final evaluation report is available through SKK, the manufacturer of ACF2.

- Interactive System Productivity Facility (ISPF) described as a "dialogue manager" for interactive applications.
  Therefore in addition to facilitating the development of on-line applications ISPF is a powerful extension to TSO/EDIT in that it provides links to many systems facilities via easy to use menus or "panels".

TSO should only be used by experienced systems programmers familiar with the facilities available and with the installation itself. For this reason, it is normally considered from a security point of view to be too powerful for application programmers.

4.1.8 System logging

The console log of messages issued to and responses by the operators is written to a file called SYSLOG. MVS provides a facility for searching and inquiring on the console messages. Messages commence with a prefix followed by an identification code which can be interpreted from systems manuals. Important message prefixes are the following:
IEA - I/O Supervisor, Supervisor, Abend
IEC - End of volume, open, close, etcetera
IEE - Master scheduler
IEF - Job scheduler

At a more detailed level for process tracing purposes, the System Management Facility (SMF) writes records about systems events to an SMF file. This file is extremely complex and contains an ever increasing number of record types with different record lengths. IBM has only recently provided a facility to easily examine and interpret the wealth of data held within the file. The creation of this file is a heavy processing overhead and therefore the extent of logging can be defined by way of parameters.
Examples of SMF records are:
Record 0 - IPL record;
Record 4 - Step terminations;
Record 5 - Job terminations;
Record 14 - Input and read back etcetera;
Record 88 - Stop/start of the access control system;
Record 89 - Changes in access control system users attributes.

In addition to the SMF file, SYS1.LOGREC is the primary dataset for recording hardware and software errors that are of a serious nature.

4.1.9 Initial Program Load

The Initial Program Load (IPL) occurs when the operator initiates the loading of the operating system.

The loading is done in accordance with certain parameters defined in the systems parameter dataset IEASYS and various other parameter datasets such as the list of authorized programs. Unless restricted the operator can override system parameters to be effective until the next IPL.

4.1.10 System Utilities

Some of the main system utilities are:

IEBPTCH	- Prints datasets; determines contents of libraries.
IEHLIST	- Lists libraries and volumes; determines dataset organization; verifies data/password protection status.
IEHDASDR	- Dumps or restores disk volumes
FDR	- Dumps or restores datasets (copies data or programs)
AMBLIST	- Verifies object module; traces modifications to CSECT (Control Section) e.g. logged use of SPZAP.
IEBCOMPR	- Compares two copies of data.
AMASPZAP	- Inspects and modifies data.
IEHMOVE	- Moves or copies collections of data from one medium to another.
IEHPROGM	- Builds and maintains systems control datasets and data at organizational level; scratches/re-names datasets and maintains passwords.
IEBUPDTE	- Replaces, deletes, re-numbers or adds records to a file.

4.1.11 Systems modifications

The operating system can be modified with the use of the general purpose utility AMASPZAP (more commonly known as Superzap). IBM provides a product called the Systems Modification Program (SMP) which also uses AMASPZAP but provides a full trail of all activity. Clearly this should be the preferred alternative to the uncontrolled use of AMASPZAP.
The SMP provides two log files: the former (SYS1.SMPLOG) covers all activity whether successful or not and the latter, the Control Dataset (SYS1.CDS), records only successful modifications.

4.1.12 User exits

The operating system can for example be modified to handle an installation's own input/output (I/O) requirements through the user exits provided within MVS. This also tends to be the route into the operating system used by proprietary software packages, such as RACF and ACF2.

4.1.13 MVS/XA

XA stands for Extended Architecture and is one of the latest versions of MVS released by IBM. It requires a 30xx or a 438x machine to run and extends the addressing for Virtual and Real Storage from 24 bits to 31 bits (addressable Virtual Storage referred to as Virtual Storage Constrainer Relief - VSCR from 16 M bytes to 2 G bytes).

4.2 Components of MVS Modules

The functional components of system software are:

a. Data processing:
   - system control program;
   - job entry system.

b. Data transfer:
   - data communication system software.

c. Storage of data:
   - data management system software.

The MVS modules of the System Control Program can be aggregated into a model [2] containing the following components:

- system Nucleus;
- supervisor;
- installation extensions;
- APF applications;
- APF utilities.

4.2.1 The major interface between the hardware and the operating system is provided by the system Nucleus. The function of the Nucleus is to provide an environment in which processes can exist.

Subfunctions within the Nucleus are:

- Interrupt handlers, which are responding to signals both from the outside world and from the computer installation itself.
- I/O supervisor; the function of this element is to manage the population of I/O devices by submitting I/O requests to channels and devices, and by responding to signals from the devices notifying the system of their status.
- Dispatcher; it is the function of the dispatcher to allocate the central process among the various processes in the installation. It is entered whenever a current process cannot continue, or whenever there are grounds to suppose that a processor might be better employed for another process.

4.2.2 The supervisor provides functions needed for the multiprogramming environment. Subfunctions within the supervisor are:

- Paging, a function of the operating system in which secondary memory is made to appear as an extension of main memory;
- Swapping, a function of the operating system which, based on the values of the installation performance parameters, decides which address spaces are to swap in or out real storage for the use of the system resources;
- System Resource Manager, the function of SRM is to achieve an optimal use of processor time, real storage, and I/O resources based on the requirements in the installation performance parameters;
- Timer support, is an essential function for scheduling and the accounting of resources consumed by the various processes;
- Supervisor routines, include basic function such as the actual I/O to control the shared use of resources and to make application programming more easy for the programmers;
- Link Pack Area (LPA) modules, include about 3000 modules of IBM, which perform various operating system functions.

4.2.3 Of special interest for an MVS security audit are the installation extensions, such as user supervisor routines, user exit routines, I/O supervisor appendages, user entries in the Program Property table, APF applications, and APF utilities. These extensions are additions to the basic MVS System Control Program. If not correctly implemented within an organization, these extensions will jeopardize MVS security.

4.3 Interface to the MVS Operating System

The following interfaces to the operating system are available:

a. at system generation and system maintenance time:
   - the System Maintenance Program (SMP);
   - the sysgen macro instructions;
   - the I/O generation instructions.

b. at system initialization time:
   - the system parameters included in the members of SYS1.PARMLIB;
   - replaceable modules in LPALIB, LINKLIB, and other system libraries;
   - operator commands;
   - user exit routines (inserted at IPL time).

c. at JOB/STEP execution:
   - installation defaults for JCL and JES2 parameters;
   - operator commands;
   - user exit routines (executed at job/step execution);
   - APF-authorized utilities (Authorized Program Facility).

4.3.1 The System Modification Program is a tool for the systems programmer to generate an MVS operating system and install system modifications (SYSMODs) on an MVS operating system and associated system distribution libraries.

The distribution libraries are used to generate a new version of the operating system. The distribution libraries contain modules that are assembled or link edited during system generation (such as utility programs, data management routines, or error recovery routines) and modules that are copied from the distribution libraries into the system datasets (such as system macros, system parameters, or catalogued procedures).

The system generation process uses the distribution libraries to create a version of the operating system tailored to a target installation.

SMP maintains records of the contents and status of the distribution libraries in a Control Data Set (CDS).
The following entries are maintained:
- Assembler (ASSEM);
- Load module (LMOD);
- Macros (MAC);
- Modules (MOD);
- Distribution libraries (DLIB);
- Source (SRC);
- System modifications (SYSMOD);
- System entries.

Once a base system level has been generated, SMP is used to install subsequent system modifications to elements on the system libraries or distribution libraries. By installing the system modifications in the distribution libraries, future system generations performed using these distribution libraries will reflect in system libraries containing the modifications.
A system modification installed in the distribution libraries is considered to be permanent by SMP. SMP cannot be used to remove it.

System modifications are constructed using SMP modification control statements. The principal control statements are:
- ACCEPT: places SYSMODs into the distribution libraries;
- APPLY: places SYSMODs into the target system libraries;
- JCLIN: creates or updates the CDS;
- RECEIVE: starts processing of a SYSMOD by performing syntax and validity checking and saves the SYSMOD on the PTF data set (PTS);
- REJECT: deletes SYSMODs from the PTS;
- RESTORE: removes a modification from the target system libraries;
- UCLIN: updates SMP data sets.

In addition to the SMP modification control statements, other control statements are available. Depending on the type of update and option requested in the control statements SMP performs a number of functions to install the system modifications.

4.3.2 At system generation time and at system initialization time an MVS installation has the capability to define a list of authorized libraries from which the APF-authorized application program is effectively considered to be an extension of the basic MVS control program. An APF-authorized application program can perform operations in an authorized state where privileged instructions can be carried out. Using this state, security measures such as an access control system can be bypassed.
The first load module in a jobstep basically determines the authorization for that jobstep.

The integrity of APF application programs in additional APF libraries is not IBM's responsibility, but the programs in those libraries should be controlled by the organization of the MVS installation.

4.4 Security mechanism in MVS

In MVS a number of security mechanisms [3, 4 and 5] provide a separation between:
- control program processes and application program processes;
- memory locations and processes that are allowed to access data in those memory locations;
- application program processes.

By using the interface described above, the systems programmer can bypass security mechanisms in MVS. The use of the user interface finds its reflection in:
- user supervisor routines;
- user exit routines;
- I/O supervisor appendages;
- user entries in the Program Property Table (PPT);
- APF applications.

The user interface to the operating system is considered by IBM as "a mechanism under the customers' control". It is a management responsibility that this user interface is properly used. System software is the heart of a secure computer installation, therefore a change management procedure for the system software is one of the main areas of concern in an organization.

4.5 Definition of a Secure MVS Installation

An MVS installation can be considered secure [7] if it:
- controls the access to the system;
- protects processes belonging to different domains against uncontrolled interference;
- controls the access to, and sharing of, programs and data used by those processes.

The fundamentals for a secure MVS installation are:
1. An effective access control system;
2. MVS system integrity;
3. A proper change management procedure for systems software.

Besides establishing effective access control, management must focus on MVS system integrity and on a proper change management procedure.

> MVS system integrity is the ability of the system to perform according to its specifications (including its security mechanism), and to resist compromise of security control through misuse or manipulation.
> IBM has guaranteed the integrity of its basic MVS control program [6]. MVS integrity is further assured by an IBM commitment to accept as valid any Authorized Program Analyses Report (APAR) that describes the use of any user interface to bypass any access control or storage protection. If an APAR is found to have an impact on system integrity it is processed within IBM under a special confidential procedure until a fix is available.

5. Installation management and change management

The problem management has to deal with is to structure the organization of EDP to ensure that a secure MVS installation is generated and will be maintained.
Before an MVS installation is generated, requirements for the system parameters, the system extensions, and the APF libraries should be defined. After implementation the compliance with the requirements should be verified.

The change management organization should include:
- a separation between test and production installations;
- division of responsibilities between:
  - change request definition and planning;
  - implementation of the change;
  - verification that changes are implemented in accordance with the change request;
  - evaluation.

The "Information/Management" tool of IBM is useful to register and track the change requests.
Information/Management is a program product of IBM, which is used with Information/System.
It is a tool which provides an on-line facility to assist management to structure problem, change and configuration activities for a computer installation.

The problem management functions of Information/Management help to ensure system problems being resolved efficiently. It can also provide information about the causes of problems and their effects. By using the problem management functions, the management of an installation can obtain information that could support decisions to minimize the number and severity of future problems.

The change management functions of Information/Management help to co-ordinate changes to software and hardware components. It can help to ensure that all proposed changes are prepared and screened in a consistent manner in order to minimize the number of faulty changes that would result in service disruption.

The configurating management functions of Information/Management help to maintain a single, up-to-date inventory of the computer installation and the terminal network.

In many organizations the division of responsibilities in relation to the change management procedure is insufficient from an internal control point of view.

6. Some Major Threats/Controls

6.1 An undesired event, such as a breach of system security, is unauthorized system access using switched lines and dial-in terminals.

The basic procedure to protect an MVS installation using this facility is a call-back procedure from the host to the terminal location. This procedure can be carried out manually or it can be automated.
An article in DATAMATION (July 1, 1984, pages 116-128) gives an overview of Port Protection Devices and their characteristics which can be used to automate this procedure.

6.2 Another potential source of unauthorized system access can result from obsolete terminal user attributes.
The combination of obsolete terminal user attributes and switched lines with dial-in terminals poses an even greater threat to the system.
The procedure utilized to prevent this event is to delete terminal user attributes when employees leave the organization.
Special attention should be paid to procedures for temporary employees.

6.3 The next category of undesired events I would like to deal with in this paper are events which result in compromised MVS integrity.

Even though an installation has a properly installed access control system, controls can be bypassed when MVS integrity has been compromised.

There are various ways which can lead to this event. One of the most common causes is when application programs are given the capability of carrying out privileged instructions for reasons of efficiency. Using this capability, security measures can be bypassed. Another way in which MVS integrity can be compromised is the use of non-IBM APF-program products, for example, a performance monitor.

In the past, it was necessary in MVS/SP to load IMS applications in APF-authorized libraries for performance reasons. In MVS/XA it is no longer necessary to compromise MVS/XA integrity in this way, since it is possible to make a distinction between APF versus non-APF applications in the SYS1.LINKLIB, and its extensions.
To prevent an MVS installation from being compromised, management should include in its security policy provisions to ensure that MVS integrity will not be compromised and therefore a change management procedure must be established which accommodates this policy.

The change management procedure should include a decision on which program products may (or may not) be installed in the MVS installation from a security point of view.

7. Security Policy for an MVS installation

The level of security measures required will vary both in time and between organizations. Management can determine what should be an acceptable level of security for their organization by weighing the costs of security measures versus undesired events.

Using the set of security risk areas as presented above as a framework, some basic elements which could be included in a security policy are:

1. Organization:
   - division of responsibilities;
   - guidelines and procedures for EDP;
   - documentation standards;
   - contingency planning and testing;
   - insurance against fraud.

2. Corporate data:
   - storage of copies of files at an external location;
   - protection from unauthorized access;
   - proper record and audit-trail of changes.

3. Applications:
   - a balanced system of internal control procedures;
   - procedures for change management.

4. System software:
   - same as for applications and;
   - access to the system software must be controlled;
   - integrity of MVS must not be compromised by extensions to the installation.

5. Hardware:
   - access to the system hardware must be controlled;
   - internal back-up;
   - external fall back.

6. Environment:
   - physical access to the installation should be restricted;
   - transport of data over communication links must be protected against data and traffic disclosure;
   - access to the installation from third party information centers must be controlled.

The guidelines and procedures within the risk area Organization should cover the following subareas:

1. Identification - of system users, operators, data files, database transactions, system devices, system output products, input sources and telecommunications lines.

2.	Accountability	- of system users, operators, programmers and maintenance personnel.
3.	Authorization	- rules for the access levels of system users, devices and programs to system data and software.
4.	Access Controls	- for physical access, and for operational access to system components and resources.
5.	Operations Controls	- for ensuring that system devices, programs, operating interfaces and databases can control data and resources they share.
6.	Performance	- in carrying out system functions and operations correctly and consistently according to performance criteria.
7.	Recovery-restart	- capabilities to recover in a timely and planned manner from any disruption of datafile access or processing capability.
8.	Audit	- of all critical system functions and resources to ensure that all the above policies are properly implemented and performing as planned.

These basic elements are only a framework which can be tailored for a particular installation. Security requirements vary in time because new technology becomes available which can have an impact on existing measures and procedures as well as threats. Therefore no single set of measures and procedures can guarantee an installation to be secure. Using the security policy as a starting point, management should anticipate the consequences of introducing new technology by adjusting the security policy. Otherwise security decisions will be made at various management levels within the organization, without fitting in a balanced framework.

To achieve the objectives mentioned under the risk area of system software, a proper change management organization is essential.

8. Computer Security Audit

A computer security audit is an investigation performed by an independent expert to confirm that adequate computer security measures are properly implemented.

A top-down approach is recommended to carry out a computer security audit using the following phases:

1. Preliminary review to obtain knowledge about management's policy related to computer security, organizational structure, applications, system software, hardware, the installation's environment, and the formal procedures.
2. Identification of weak/strong risk areas, using the six risk categories as a framework:
    1. Organization:
        - the security policy;
        - the organizational structure and responsibilities;
        - the division of responsibilities;
        - guidelines and procedures resulting from the security policy, such as:
            . grant of terminal user authorities (on-line processing);
            . production job routing (batch processing);
            . problem management;
            . accounting;
            . change management for applications;
            . change management for system software;
            . change management for system hardware;
            . personnel recruitment (including temporary employees);
            . job rotation;
            . personnel attitude evaluation;
            . leave policy;
            . documentation;
            . contingency planning and testing;
            . insurance.
    2. Corporate data:
        - management of data and DBA procedures.
    3. Applications:
        - the internal control procedures for the main applications.
    4. System software:
        - access control system.
    5. Hardware:
        - maintenance carried out by manufacturers;
        - internal back-up;
        - external fall back.
    6. Environment:
        - identification of threats;
        - physical security and emergency measures;
        - data communication links.
3. Interim report.
4. In-depth review of weak risk areas.

Before an audit of the risk area of systems software can be carried out, it is important that the auditor has a thorough understanding of the security mechanism of, and the user interface to, the systems software. There are different architecture/operating system security mechanisms at the instruction, operand, data, or language level [7].
The MVS operating system is considered one of the most secure commercially available operating systems. IBM has issued a statement of integrity for this operating system, although there are other operating systems of IBM without such a statement (VM and VSE).

9. MVS Security Audit

Depending on the results of the previous phases, an MVS security audit may be needed to be carried out. This audit consists of the following phases:

1. Preliminary review to obtain knowledge about:
   - procedures within the technical support department;
   - system software;
   - hardware:
     . CPU's;
     . channel switching;
     . I/O subsystem;
     . RJE I/O stations;
     . readers and printers;
     . terminal network.
   - environment.

2. Selection of a target installation.

3. The MVS security audit process.
   This paragraph gives an overview of some of the main threats and evidence of controls which are to be evaluated in this phase of an MVS security audit, such as:

   1. System Control program
      Control object: MVS system integrity
      A. Threat - wrong values of the system parameters so that security mechanisms of MVS can be bypassed
         Evidence - parameters of IEASYS00 of the SYS1.PARMLIB
      B. Threat - no control over the Authorized Program Facility
         Evidence - parameters of IEASYS00, the change management procedures for APF programs, and the directory of the APF libraries

C. Threat - user SVC's and User Exit routines
Evidence - SVC table of the I/O sysgen, the parameters of subsystems, the source and load versions of the User Supervisor Routines and Exits and change management procedure

D. Threat - User entries in the Program Property Table
Evidence - Load version of the IEFSDPPT and change management procedure

2. Job Entry System
Control object: Access Control System

A. Threat - unauthorized access via JES using terminals
Evidence - JES2 parameters and change management procedure

B. Threat - unauthorized access via JES card readers
Evidence - procedure for production job routing (batch processing)

3. Transfer of data
Control object: Access Control System

A. Threat - unauthorized system access using dial-in modems
Evidence - inventory of system hardware, sign-on procedures, and change management procedures for system hardware

B. Threat - unauthorized system access using VTAM application
Evidence - start net procedure (S NET), parameters of ATCCOM00 of the SYS1.VTAMLST and change management procedure

C. Threat - availability of RJE lines and VTAM application outside office hours
Evidence - network operator procedures

4. Storage of data
Control object: Access Control System

A. Threat - shared use of external storage by test and operational processing
Evidence - inventory of system hardware, the I/O sysgen and change management procedure

B. Threat - unauthorized system access using dial-in modems and RJE
Evidence - the I/O sysgen and the change management procedure

5. TSO and performance monitors
Control object: Access Control System

A. Threat - unauthorized system and data access
Evidence - TSO-user attributes of the SYS1.UADS, a report of authorized TSO-users and the change management procedure

B. Threat - performance monitors
Evidence - user attributes for the use of the performance monitors and the procedures to use them

6. Access Control Software
Control object: Access Control System
A. Threat - unauthorized system and data access
Evidence - parameters of the access control software, access rules, resource definitions, terminal user attributes, a report of authorized users, and the related procedures for giving terminal user authorizations
B. Threat - security violations by terminal users
Evidence - logging and surveillance procedures

4. Report:
- conclusion;
- findings;
- recommendations.

10. To Conclude

To assist the installation of computer security measures and procedures, a management security policy must be defined, which can be based on the identification of undesired events and the costs of measures and procedures to prevent these events from occuring.

Although the computer security policy must cover all relevant risk areas, special attention must be paid to the risk area of systems software, since it is the heart of a secure computer installation. A change management structure and procedures must be developed within the organization to ensure that a secure computer installation is generated and maintained.

No special technical expertise is required to carry out the first two phases of the computer security audit. However, the auditor needs a thorough understanding of the security mechanism of, and the user interface to, the systems software to carry out an in-depth review of this risk area.

References

[0] Didham, A., "Basic advance reading paper on MVS", Computer audit technical update course (1985).
[1] Summer, R.C., "An overview of computer security", IBM systems journal, vol. 23, no. 4 (1984), pp. 309-325.
[2] Thomas, Drs. R.A.C. en Paans, Ir. R. "Certificering van software: utopie of werkelijkheid", NGI sectie EDP-auditing, Symposium certificering software (1984), pp. 55-68.
[3] Lorin, H. and Deitel, H.M., "Operating systems", pp. 1-31, Addison Wesley, The system programming series.
[4] IBM manual: GA22-7085 Principles of operations.
[5] McPhee, W.S., "Operating system integrity in OS/VS2", IBM systems journal, vol. 13, no. 3 (1974), pp. 230-252.
[6] IBM's statement of MVS system integrity.
This statement includes a list of APF-authorized programs of which the integrity is the responsibility of IBM.
[7] Roos, H., "Security and audit of operating systems", International Symposium (NIvRA) on auditing in an advanced complex computer environment (1984).

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

COMPACT

Winter 1985/1986

SCHRIJVERS REAGEREN

door J.C. Boer

De overdrachtsprocedure is meer dan een gebruikerstest

In de inleiding van mijn artikel "De overdrachtsprocedure is meer dan een gebruikerstest" Compact 85/3 nr. 39,heb ik beoogd de positie van maatregelen van interne controle binnen de automatiseringsorganisatie ten opzichte van de gebruikerscontroles op de werking van applicatiesystemen tot uitdrukking te brengen.
Doel hiervan was tot een uitgangspunt te komen voor het formuleren van door de verschillende "gebruikers" (in ruime zin, namelijk inclusief alle andere bij de gegevensverwerking betrokken bedrijfsonderdelen, in het bijzonder de afdeling produktie binnen automatisering) te stellen eisen aan de automatiseringsorganisatie. Deze eisen dienen tijdens de systeembouw te worden geformuleerd, de genomen maatregelen dienen tijdens de acceptatiefase, door alle betrokkenen, te worden getest en geaccepteerd.

Impliciet bedoelde ik in de inleiding het volgende te concluderen. In de automatiseringsorganisatie kunnen maatregelen van interne controle worden genomen ten aanzien van volledigheid, juistheid, tijdigheid en bevoegdheid van de verwerking.
Deze maatregelen hebben een preventief karakter, terwijl de gebruiker zelf achteraf (repressief) aan de hand van de uitkomsten en signalen de verwerking op deze aspecten kan controleren.

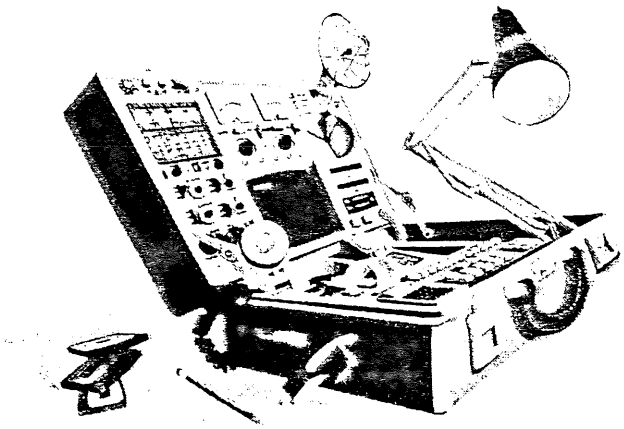
Preventieve maatregelen als gevolg van eisen aan de automatiseringsorganisatie zijn bovendien noodzakelijk ten aanzien van de continuïteit, privacy/geheimhouding en ten behoeve van een adequaat beheer van gegevens en programma's. De naleving van deze vorm van preventieve maatregelen is voor eindgebruikers achteraf erg moeilijk vast te stellen; vaak zullen feilen te dien aanzien door toeval en/of op pijnlijke wijze aan het licht komen. Reden waarom tijdens de overdrachtsprocedure (en ook periodiek) het testen van deze preventieve maatregelen en procedures door alle betrokkenen van bijzonder belang is.

Door een technische oorzaak is in bedoelde inleiding een klein gedeelte van de tekst weggevallen, waardoor met name de genoemde impliciete conclusie waarschijnlijk niet door de lezer zal zijn getrokken. Daarom geef ik de bedoelde tweede alinea van de inleiding graag nogmaals, maar nu volledig weer:

"De gebruiker van een informatiesysteem kan, bij een goed opgezet informatiesysteem, zijn verantwoordelijkheid voor een juiste en volledige informatieverwerking dragen door de gebruikerscontroles geïntegreerd in het informatiesysteem. Deze controles zijn repressief van aard.

De functiescheidingen in de automatiseringsorganisatie als maatregel van interne controle zijn preventief van karakter; tevens dragen zij bij tot het bereiken van een organisatie die verantwoordelijkheden kan dragen ten aanzien van de eigendomsrechten van programma's en gegevens, de continuïteit, de privacy en de geheimhouding."

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



DE MICROCOMPUTER IN DE ACCOUNTANTSCONTROLE

door H. Veenman

Dit maal wil ik uw aandacht vestigen op het File Analysis Tool. Het programma dat drie jaar geleden geboren werd als het zeer beperkte KKC Audit Package is uitgegroeid tot een volwaardig produkt, bedoeld om op de microcomputer bestandsonderzoeken uit te voeren.
Om u een idee te geven wat kan en niet kan met dit pakket volgt hieronder een deel van de Introductie zoals deze in de handleiding bij het pakket gevonden wordt.

Introduction

Welcome to the File Analysis Tool by KMG Klynveld Kraayenhof & Co. We think you'll find FAT a well-written and useful piece of audit software.

FAT is a data-oriented audit tool you can use to examine client data files such as a General Ledger or a Sales Journal to verify that the records on which financial reports are based reflect established accounting principles. FAT is accountant-friendly and is designed for direct use by auditors; special programming knowledge is not necessary.

You can use FAT to support compliance as well as substantive and dual purpose testing. And, unlike general-purpose database programs, FAT has the built-in test routines auditors need and FAT produces reports in a form suitable for direct inclusion in your working papers.

By automating this testing process, FAT makes the examination of large volumes of data more economical and reduces sampling risks. Manual follow-up of processing results will remain an essential part of control procedures; however, FAT eliminates tedious and increasingly costly work and focuses attention on important judgment areas. Using FAT will save costs over a number of years and result in more effective verification.

How FAT Works

FAT uses five principal means of manipulating client data to carry out a wide variety of tests. These techniques can be used alone or in combination to analyse a file and include

1. Summation
2. Sorting
3. Statistical Sampling
4. Selection
5. Mathematical Calculation

With these five techniques, FAT gives you the flexibility needed to carry out effective audit testing. There is no single computer assisted audit just as there never was a single "manual" audit.

Here are some examples of the many tests FAT can perform :

1. **Total Controls.** FAT can be used to add all the debit and credit fields in a data file such as an Accounts Receivable file to see if the totals agree with each other and with control counters maintained outside the computer and in the General Ledger.

2. **Aging.** FAT can be used to age the entries in a client file such as in an Accounts Receivable subledger. For example, outstanding purchases older than 60 days can be listed to the printer or disk file for verification and control.

3. **Tolerance Controls.** FAT can be used to examine values which may only deviate from the norm by a fixed percentage. For example, you can test to see if the gross profit for a certain article deviates by more than 15 percent.

4. **Statistical Sampling.** FAT has a sophisticated built-in statistical sampling routine known as the Sieve Method which can be used to build a random sample of transactions or postings for subsequent verification of compliance. The Sieve Method may select any record in a file; however, larger amounts have a greater chance of being selected and you can choose a sample size such that all amounts over a specified value are certain to be selected.

When Should You Use FAT?

Naturally, the first prerequisite for using FAT is that your client has some or all of his financial records in electronic form. A second prerequisite is that the records must be on, or be converted to, standard ASCII files in the MS-DOS format and be available either on diskettes or on a hard disk. KMG Klynveld Kraayenhof & Co. has developed the File Conversion Tool to make conversion to MS-DOS format practicable for as many varieties of computer as possible. You can get more information over FCT from your local support center or from KMG Klynveld Kraayenhof & Co. at the address listed in the Licence Agreement.

Assuming that the first two prerequisites for using FAT have been met, the decision as too when and how to use FAT will depend on the files available for analysis and the nature of the engagement.

How to Use This Manual

This manual is designed to help auditors with different backgrounds and levels of expertise to work with FAT. It is designed to be used in conjunction with the extensive context-sensitive help function built into the program.

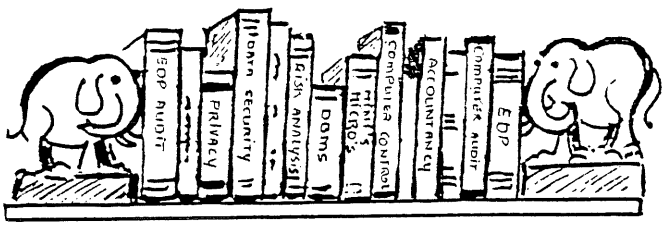
FAT is entirely menu-driven and most of the menus and screens are self-explanatory. You can always request help with the F10 **HELP** function key.

Each section has been written with the beginner as well as the experienced user in mind. Many illustrations and screen displays are provided as visual guides. Before getting started it will be helpful to get familiar with the manual and its sections.

Manual Style

We have tried to make the manual clear and consistent. Steps for procedures you must follow are numbered and notes or examples are provided where additional information is needed.

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



Boeken

door drs. D. Kruif, ing. J.C. van Winkel en J.A.W. Winterink

1. Titel: Systeembeheer en beveiliging in de automatisering
Auteur: ir. H. Völlmar
Uitgever: Het Spectrum "Marka Pocket"
Omvang: 151 pagina's
Boekbespreking door J.A.W. Winterink

Algemeen

In het voorwoord wordt door de schrijver aangegeven, dat dit boek is geschreven voor iedereen die nauw betrokken is bij het gebruik van geautomatiseerde systemen. Hierbij denkt hij zowel aan de gebruikerszijde als aan de zijde van de automatiseringsdeskundigen.

Systeembeheer is vooral een belangrijk aandachtsgebied voor het management. Aangezien de moderne organisatie steeds afhankelijker wordt van geautomatiseerde systemen en daarmee steeds kwestbaarder wordt, moet het beheer van aanwezige systemen goed worden geregeld. Het is de verantwoordelijkheid van het management daartoe de nodige maatregelen te nemen.

Door een goede regeling van het systeembeheer kan ook worden voorkomen dat de organisatie te kwetsbaar wordt voor malafide praktijken. De bezorgdheid voor computerfraude wordt terecht met de dag groter naar aanleiding van het bekend worden van tal van computerschandalen.

Systeembeheer en beveiliging van de informatievoorziening hebben veel met elkaar te maken. Een hoge graad van beveiliging tegen ongewenste gebeurtenissen is niet denkbaar zonder een zorgvuldige regeling van het systeembeheer.

Het boek richt zich dus hoofdzakelijk tot die managers die zich afvragen wat er moet worden geregeld en hoe dat het beste kan gebeuren. Juist voor deze categorie van lezers is door de schrijver getracht de tekst dan ook zoveel mogelijk vrij te houden van automatiseringsjargon en waar mogelijk alleen Nederlandse termen te gebruiken.

De vraag is of het gebruik van deze termen de leesbaarheid van het boekje verhoogt; een term als "dienstprogrammatuur" (programmatuur die nodig is om een computer te laten functioneren) in plaats van systeemprogrammatuur, is voor mij bepaald geen gelukkige keuze. Wil de topleiding vandaag de dag met zijn automatiseringsdeskundigen kunnen communiceren, dan zal enige kennis van "automatiseringsterminologie" geen overbodige luxe zijn.

Bespreking

De tekst van het boek is in vier delen uitgewerkt.

In het eerste hoofdstuk worden de principes van de regeling van het systeembeheer uiteengezet.

De daarop volgende vier hoofdstukken bevatten uitwerkingen van de deelgebieden.

Hoofdstukken 6 en 7 geven nog wat extra materie en in hoofdstuk 8 wordt de actie van het organiseren van het systeembeheer behandeld.

Hoofdstuk 9 tenslotte gaat over het beveiligen van de informatievoorziening.

Hoofdstuk 1

De uitgangspunten bij het organiseren van het systeembeheer zijn zeer eenvoudig. Men moet het organiseren van systeembeheer op dezelfde manier benaderen als het organiseren van alle andere activiteiten in een organisatie. Wat betreft het organiseren van systeembeheer moet men zich steeds afvragen wie wat het beste kan doen. De volgende principes worden vervolgens beschreven:

1. Laat een taak uitvoeren door degene die daartoe het beste in staat is; inhoudelijk-gerichte taken door de gebruiker en technisch-gerichte taken door de automatiseringsdeskundigen.

2. Ga er vanuit dat een geautomatiseerd systeem een gereedschap is van de gebruiker en laat hem datgene bepalen wat hij als consument zelf moet beslissen.

3. Zorg dat door functiescheiding een zo veilig mogelijke situatie wordt gecreëerd, hetgeen tevens inhoudt dat het beheerde proces zo goed mogelijk moet zijn te controleren.

4. De hoogste lijnmanager in het gebied waarin het geautomatiseerde systeem werkzaam is, draagt de eindverantwoordelijkheid voor de taken die des gebruikers zijn.

Hoofdstukken 2, 3, 4 en 5

Deze hoofdstukken bevatten uitwerkingen van de deelgebieden:

hoofdstuk 2 - Het beheer van de gegevens;

hoofdstuk 3 - Het beheer van de applicatieprogrammatuur;

hoofdstuk 4 - Het beheer van de apparatuur en de dienstprogrammatuur;

hoofdstuk 5 - Het beheer van de documentatie.

De opbouw van deze hoofdstukken is zodanig, dat achtereenvolgens wordt behandeld:
- een analyse van de beheersfunctie;
- een modelfunctiebeschrijving van de beheerder;
- tien raadgevingen voor de beheerder.

Een duidelijke aanpak, die zeker voor het management van ondernemingen verhelderend zal werken.

Hoofdstukken 6, 7 en 8

Deze hoofdstukken gaan vervolgens in op:

hoofdstuk 6 - Systeembeheer bij gespreide verwerking en opslag van gegevens;

hoofdstuk 7 - Speciale overlegorganen;

hoofdstuk 8 - De invoering van verbeteringen van het systeembeheer.

Terwijl in de voorgaande hoofdstukken is uiteengezet hoe men het systeembeheer kan regelen, worden in dit hoofdstuk aanbevelingen gedaan voor de eigenlijke actie van het organiseren. Hierbij wordt ook even kort ingegaan op het systeembeheer als een gebied, waarop een EDP-audit gericht kan zijn: evaluatie van het systeembeheer en het doen van aanbevelingen op welke punten verbeteringen in het systeembeheer en de beveiliging gewenst zijn.

Hoofdstuk 9

Dit hoofdstuk behandelt het gehele gebied van de beveiliging van géautomatiseerde systemen. Als uitgangspunt geldt hier, dat men pas ernst kan maken met het verhogen van de beveiliging van de informatievoorziening, als het systeembeheer goed is geregeld.

Epiloog

De auteur hoopt dat dit boek tevens geschikt zal zijn voor het onderwijs in de informatica en dan met name het hoger beroepsonderwijs. Hier komen immers de automatiseringsmanagers van morgen vandaan. Zij met name zullen moeten weten hoe men samen met de bedrijfsleiding het systeembeheer vorm kan geven.

Ik denk dat dit boek inderdaad hiervoor geschikt zal zijn. Daarnaast zal het aan te bevelen zijn voor accountants, die organisaties tegenkomen, waar het systeembeheer nog in de kinderschoenen staat. Hij weet dan in ieder geval wat er allemaal bij komt kijken, wil men het systeembeheer op een fatsoenlijke en voor hem bevredigende wijze laten functioneren.

2. "Boek": MAB, november/december 1985
Onderwerp: Accountantscontrole en automatisering
Bespreking door D. Kruif

Deze keer geen boekbespreking, maar een gedeeltelijke bespreking van het laatste themanummer van het Maandblad voor Accountancy en Bedrijfshuishoudkunde.
In dit themanummer wordt middels 7 artikelen aandacht besteed aan accountantscontrole en automatisering.

Deze artikelen zijn:
1. J.H. Blokdijk
   Informatiegerichte analytische controle
2. Prof. L.A. van Hulsentop
   De aanpak van de accountantscontrole
3. Prof. drs. K.P.G. Wilschut
   De beoordeling van het systeem van interne controle bij toepassingen van automatisering
4. Prof. L.C. van Zutphen
   EDP-auditing; een poging tot verduidelijking
5. Drs. A. Straatman
   Accountantsoordelen inzake applicatiesoftware
6. Drs. H.M.I. van der Putten
   Accountantscontrole bij kleinschalige automatisering
7. Drs. J.E. Huizenga
   Accountantscontrole en integratie van de gegevensverwerking

De eerste twee artikelen behandelen twee verschillende opvattingen over de aanpak van de accountantscontrole.
Uit oogpunt van automatisering zijn deze artikelen minder interessant, omdat uit de uiteenzettingen blijkt dat het verschil in opvattingen nauwelijks beïnvloed wordt door automatisering.
Het artikel van Wilschut behandelt de invloed van automatisering op beoordeling van het systeem van interne controle. De kern van de problematiek van automatisering en controle is volgens de schrijver het ondanks toepassing van automatisering blijven bestaan van voor de controle noodzakelijke functiescheidingen tussen gebruikers.
De schrijver gaat hierop in, mede aan de hand van Nivra geschrift nr. 13.
Van Zutphen geeft in zijn artikel een globaal overzicht van het fenomeen "EDP-auditing". Hoewel dit artikel weinig nieuws bevat, geeft het een goed en gestructureerd beeld van het vakgebied en de aandachtsgebieden die daarin worden onderkend.
Op de artikelen van Straatman en Van der Putten wordt hierna wat dieper ingegaan.
Tenslotte behandelt Huizenga in zijn artikel enkele aspecten van integratie van gegevensverwerking, waarbij aandacht wordt besteed aan technische hulpmiddelen en (nieuwe) organisatorische functies. Tevens geeft hij aan wat de invloed van de integratie is op de door hem besproken controlemiddelen van de accountant.

Al met al mag worden gesteld, dat het lezen van dit themanummer zeer de moeite waard is.

A. Straatman Accountantsoordelen inzake applicatiesoftware

De oorzaak van de behoefte aan een accountantsoordeel met betrekking tot betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking is tweeërlei:
1. de groeiende afhankelijkheid van organisaties van de automatisering;
2. de sterke opkomst van standaard applicatie-software.

Ad 1

De schrijver legt in dit artikel de nadruk op het thema "kunnen verwachtingen waargemaakt worden".
Hierbij wordt gedoeld op verwachtingen die gebruikers koesteren ten aanzien van de door de accountant/EDP-auditor*) af te geven mededeling (zie NIVRA geschrift no. 26).
Deze verwachtingen zijn vaak te hoog gespannen; men verwacht dat de accountant de organisatie en haar informatiebehoeften zo goed doorgrondt dat hij gemakkelijk tot een pasklaar antwoord kan komen of bepaalde applicatiesoftware "voldoet".
Dat dit niet zo gemakkelijk is, blijkt onder meer uit de voorbehouden die worden gemaakt in de voorbeeldteksten in NIVRA geschrift no. 26 van mededelingen. De gebruiker heeft op zich weinig aan deze voorbehouden; hij is meer gebaat bij de positieve betekenis van de mededeling (wat kan de applicatie wél).

De accountant zal echter in zijn mededeling niet aan voorbehouden kunnen ontkomen, al was het alleen maar om daarmee een fouttolerantie tot uitdrukking te brengen. Dit wordt mede versterkt door het feit, dat het mensen zijn die met de computer moeten werken; zij vormen een wezenlijk onderdeel van het door de accountant beoordeelde informatiesysteem en kunnen als zodanig de werking van het systeeem in belangrijke mate beïnvloeden. Oordeelt de accountant bijvoorbeeld positief over de opzet van applicatie-software, dan betekent dit dat in die opzet zodanige voorzieningen getroffen zijn, dat een doeltreffende interne controle op de werking van het systeem mogelijk is.

Dit betekent dus, dat de gebruiker niet van zijn plicht ontslagen is om zijn taak goed te vervullen, wil het systeem inderdaad goed functioneren.

De accountant kan het best inspelen op de verwachtingen van het management van een organisatie ten aanzien van een af te geven mededeling, door in overleg met het management te komen tot een goede formulering van de opdracht tot het onderzoek naar betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

* Er wordt in het vervolg voor het gemak alleen gesproken van "accountant", in plaats van accountant/EDP-auditor.

Ad 2

Het management van organisaties wenst in toenemende mate zekerheid voor aanschaf van een standaard software-pakket of hetgeen in de verkoopdocumentatie staat aangeprezen ook daadwerkelijk door een pakket wordt uitgevoerd. Voordat tot aanschaf wordt overgegaan is het van belang dat de gebruiker (en niet de accountant) een nauwkeurige specificatie geeft van de informatiebehoeften middels een programma van eisen. Dat dit niet een samenraapsel zal moeten zijn van overgenomen kreten uit commerciële folders lijkt een overbodige opmerking, toch wil dit nogal eens het geval zijn met alle negatieve gevolgen voor de kosten/batenverhouding in het functioneren van een organisatie.
De accountant kan wel behulpzaam zijn bij het expliciet maken van een programma van eisen. De gebruiker denkt veelal dat dit niet nodig is, omdat het aan te schaffen pakket toch "standaard" is. Hierbij wordt vergeten, dat ook standaardpakketten veelal het levenslicht aanschouwen als stukje maatwerk voor een bepaalde klant en dus allerminst "standaard" zijn.
Hiernaast zal de accountant aanvullend onderzoek moeten doen naar pakketten die bij de specifieke eisen van deze organisatie passen. Dit zal zeker nodig zijn, omdat er een groot aanbod van standaard-software is.

Het zou wenselijk zijn een soort van algemeen certificaat af te geven bij een bepaald pakket, waarnaar eenvoudig zou kunnen verwezen (vergelijkbaar met een "consumentenbondachtige waardering van de gebruiks- en controleaspecten"). Dat wil zeggen een positief geformuleerde beschrijving waarop de gebruiker zijn situatie kan projecteren.
Dit is volgens de schrijver onbereikbaar door de diversiteit in de spelregels van de gebruiker.

Tenslotte nog enkele opmerkingen over continuïteit en controleerbaarheid. Het certificaat bij standaard-software kan de continuïteit van de leverancier/maker niet garanderen. Je kunt hoogstens continuïteit aannemen als een bepaald pakket bij veel organisaties is geïnstalleerd. Met betrekking tot de controleerbaarheid hebben accountant en de gebruiker (en de gebruikers onderling) veelal uiteenlopende opvattingen. Zo zal een groep gebruikers bepaalde geprogrammeerde controles niet wensen vanwege de inbreuk op de flexibiliteit, terwijl een andere groep gebruikers deze controles juist efficiënt vindt vanwege het hem uit handen nemen van onnodig werk. Volgens de schrijver dienen de geprogrammeerde controles in de mededeling van de accountant te zijn opgenomen.

Aan volledigheid van de verwerking en aan audit trails is in dit artikel geen aandacht geschonken.

COMPACT

Winter 1985/1986

Drs. H.M.I. van der Putten Accountantscontrole bij kleinschalige automatisering

Inleiding

Het begrip kleinschalige automatisering wordt niet direct gekoppeld aan de omvang van de computercapaciteit, maar meer aan de omvang van de organisatie.
In dit artikel wordt onder kleinschaligheid verstaan een omvang, waarbij een afzonderlijk rekencentrum (met full-time-functies van systeemontwikkeling, programmering, produktie/operating en bestandsbeheer) ontbreekt.
Kleinschaligheid kenmerkt zich verder onder meer door:
- geen functiescheiding tussen EDP en gebruikers;
- geen functiescheiding tussen de functies die we graag binnen een rekencentrum zien;
- de (stand-alone) computer bevindt zich op de gebruikersafdeling;
- de gebruikers hebben relatief weinig automatiseringskennis;
- gebruik van kleinere goedkopere computers met primair op gebruiksgemak en snelheid gerichte besturingssystemen;
- veel standaardprogrammatuur;
- beperkte of geheel ontbrekende systeemdocumentatie;
- uitgebreid gebruik van kwetsbare diskettes als opslagmedium;
- voornamelijk interactieve transactiegewijze verwerking van gegevens;
- informele procedures ter zake van registratie, verslaggeving, analyse, planning en controle.

De schrijver besteedt vervolgens aandacht aan twee onderwerpen:
1. de interne controle bij kleinschalige automatisering;
2. de invloed op de accountantscontrole.

Ad 1

In dit hoofdstuk wordt ingegaan op verschillen met zowel de niet-geautomatiseerde situatie als de situatie van grootschalige automatisering. Verder worden subparagrafen gewijd aan:
- functiescheiding;
- beheersing van de systeemontwikkeling;
- toegangsbeheersing;
- controle op invoer, verwerking en uitvoer;
- waarborgen van continuïteit;
- controleerbaarheid.

Ad 2

De bespreking van de invloed op de accountantscontrole vindt plaats aan de hand van de volgende subparagrafen:
- algemene oriëntatie op de te controleren organisatie;
- beoordelen opzet en werking van de interne organisatie;
- opstellen controleplan.

De schrijver besluit met onder meer de volgende conclusies: Voorkom overmatig controleren. Ga bijvoorbeeld niet met uitgebreide checklists een organisatie analyseren op goede werking van de interne controle, als reeds na de eerste oriëntatie blijkt dat essentiële en voor de controle onvervangbare functiescheidingen ontbreken. Waar sprake is van grote risico's c.q. een groot belang voor de jaarrekening en tevens een zwakke interne controle, zal de accountant zijn controle moeten intensiveren en bijvoorbeeld zijn toevlucht moeten nemen tot cijferbeoordeling, verbandscontroles, totalencontroles buiten de computer om en verificatiewerkzaamheden in detail.
Omgekeerd, als er sprake is van gering belang voor de jaarrekening en een sterke interne controle, kan de accountant zelfs adviseren de interne controle te reduceren ter besparing van de kosten.
Voor alle situaties geldt, dat een evenwicht gevonden dient te worden tussen systeemgericht en gegevensgericht controleren.

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

TIJDSCHRIFTEN

door mw. D. Jansen Heijtmajer, J.L.H. Kooijman en J.C. Boer
met medewerking van mw. W. de Munck-Kraamer

"Nederlandse privacy-wetgeving: licht aan het einde van de tunnel"
Prof. D.W.F. Verkade
Computerrecht, januari 1986

door J.C. Boer

In de zomer van 1985 heeft de regering het wetsontwerp 19.095 voor een "wet persoonsregistraties" aan de Tweede Kamer aangeboden. Het is een hernieuwd voorstel om tot een privacy-wetgeving in Nederland te komen na het intrekken van het in 1981 ingediende wetsvoorstel geënt op het rapport van de staatscommissie Koopmans.

In het artikel van D.W.F. Verkade wordt ingegaan op de hoofdlijnen van het nieuwe ontwerp, dat zich kenmerkt door een gestroomlijnde en vereenvoudigde uitwerking in vergelijking tot het eerste ontwerp. Na een positief globaal commentaar wordt ingegaan op de onderlinge verhoudingen van bijzondere en algemene privaatrechtelijke regels. Aan dit laatste aspect zal in deze samenvatting slechts geringe aandacht besteed worden.

In hoofdlijnen zal ingegaan worden op de belangrijkste aspecten van het nieuwe wetsvoorstel. De consequenties van de regelingen zullen met het commentaar uit het artikel worden toegelicht.

Het wetsvoorstel is primair privaatrechtelijk van opzet.
Dit betekent, dat benadeelden bij een conflict naar de burgerlijke rechter zullen moeten stappen. In plaats van één individuele burger kan een belangenvereniging (of stichting) een procedure aanhangig maken (een zogenaamde groepsactie).
Alvorens naar de rechter te stappen kan een weliswaar niet bindend advies aan de registratiekamer gevraagd worden.
Het gevolg van het gekozen wettelijke systeem is, dat de houders van registraties risico's lopen ter zake van een andere uitleg en toepassing van de wet. Het risico van de vage normen ligt bij de houder van de registratie.

Het wetsontwerp betreft zowel geautomatiseerde als niet-geautomatiseerde registraties.

Branche- c.q. sectororganisaties kunnen sectorgewijze gedragscodes opstellen. De registratiekamer kan met betrekking tot een gedragscode een verklaring met een oordeel over de aanduiding met de wettelijke of anders gestelde eisen verstrekken. Bij een toetsing is de rechter niet aan deze "goedgekeurde" gedragscode gebonden, doch zij zal deze wel zwaar in haar afweging moeten laten wegen.

De concrete reglementering van de registratie moet plaatsvinden middels een "meldingsformulier". De aanmelding van een registratie zal leiden tot een ter inzage legging van het reglement.
Ten aanzien van de aanmeldingsplicht zullen bij algemene maatregel van bestuur uitsluitingen plaats kunnen vinden. In het wetsontwerp ligt reeds vast, dat voor enige bij bijzondere wet ingestelde overheidsregistraties, de desbetreffende speciale overheidsregels van toepassing blijven.

De registratiekamer krijgt een adviserende en (repressief) toezichthoudende taak. De controle door de registratiekamer vooraf, zoals vastgelegd in het oude wetsontwerp, is gedereguleerd tot een onafhankelijke toetsing achteraf.

De "hoeksteen" van de privacy-bescherming in verband met persoonsregistraties is het inzagerecht. Het weigeren van inzage wordt door de wetgever niet als onrechtmatig gezien, alhoewel de inzage verleend moet worden. De juridische betekenis hiervan is in het artikel nader uiteengezet. Praktisch betekent het dat een geregistreerde, soms via lange procedures, altijd inzage in de registratie kan verkrijgen.

In de paragraaf "internationale aspecten" is opgenomen, dat het niet zonder meer toegestaan is gegevens te verstrekken aan, respectievelijk te betrekken van registraties die zich elders bevinden en waarop de wet geen toepassing heeft.
In het commentaar wordt naar voren gebracht dat de mogelijkheden tot civielrechtelijke acties of strafrechtelijke sancties tegen het ontduiken van deze bepaling niet in het wetsontwerp opgenomen zijn.

Het wetsontwerp betreft slechts de regeling van registraties, het gebruik of misbruik van persoonsgegevens valt niet onder de werking van de wet. De auteur pleit ervoor in de wet op te nemen, dat ondanks deze bijzondere wet een onverhinderd beroep gedaan kan worden op het gemeen recht (bijvoorbeeld artikel 1403 BW onrechtmatige daad en 1374 lid 4 BW uitvoering overeenkomsten te goeder trouw).

Nieuw ontwerp Privacy-wet

Welke gevolgen heeft de nieuwe, sterk gewijzigde wettelijke regeling voor het verzamelen, bewaren en gebruik van persoonsgegevens.

Verslag Euroform studiedag 11 september 1985
door mw. Wilma de Munck-Kraamer

Enkele accenten nieuwe wetsvoorstel:

- Verschuiving van een publiekrechtelijke aanpak naar een privaatrechtelijke aanpak.
  Zelfregulering in praktijk (artikel 10 van Grondwet).

- Verzekeren van een behoorlijke en zorgvuldige bescherming door:
  . bevorderen openbaarheid;
  . verbeteren rechtspositie van geregistreerden;
  . regulering.

- Ten aanzien van de regulering
  . in oude wetsontwerp had de regulering een sterk preventief karakter; denk aan registratieplicht, aanmeldingsplicht of toestemmingsplicht voor de verschillende registraties;
  . in het nieuwe wetsontwerp wordt de nadruk gelegd op materiële normen in de wet zelf door middel van repressief toezicht. Verder wordt het onderscheid tussen geautomatiseerd en niet-geautomatiseerd opgeheven.

- Registraties betreffen individuele gegevens die samenhang vertonen door:
  . hun aard;
  . hun doel;
  . hun gemeenschappelijk gebruik.
  Het beschikbaar stellen van gegevensbanken valt hier ook onder.

- Een registratie moet een bepaald doel hebben, aanvaardbaar zijn en van redelijk nut voor de houder.

- Gegevens moeten rechtmatig zijn verkregen en in overeenstemming met het doel zijn.
  Juistheid en volledigheid moeten zijn nagestreefd.

- Overheidsregistraties moeten ook nog noodzakelijk zijn.

- Verstrekking aan derden is alleen toegestaan als het gebruik van derden voortvloeit uit het oorspronkelijke doel.
  Dus meer dan "in overeenstemming met". Anders is toestemming van geregistreerden noodzakelijk.

- Voor beveiligingseisen zie artikel 8.

- Gedragscodes ter zake van de zelfregulering moeten worden gedefinieerd op sectorniveau (denk aan beroep, branche) en per registratie.

- Rechten van geregistreerden:
  . recht van kennisneming;
  . recht op inzage;
  . recht op inlichtingen over herkomst;
  . recht op inzage in gebruik;
  . recht op verbetering (correctie).

- Handhaving van wet door de registratiekamer (afdeling per sector). Dit is overigens een langduriger weg dan het huidige kort geding.

- Registraties in de publieke sector hebben reglementplicht, in de private sector slechts aanmeldingsplicht via een speciaal formulier.

- Klachten bij de registratiekamer kunnen ambtshalve worden ingediend, alsook door betrokkene(n) en belangenverenigingen of stichtingen.

- Internationaal dataverkeer: artikel 49/50.

- Het koppelen van 2 of meer registraties zal veelal niet "voortvloeien" uit het oorspronkelijke doel en derhalve aanvechtbaar zijn.

- De verantwoordelijkheid voor de beveiliging van de registratie ligt bij de houder.

Das Software-Testat"
Bernd Koch
Die Wirtschaftsprüfung nr. 24, Dezember 1985.

door J.L.H. Kooijman

Het artikel richt zich op het probleem van de software-certificering: de onderzoekmethode, de toetsingscriteria en de aard en strekking van de mededeling.

De schrijver stelt bij de aanvang, dat "tüchtiger" gebruikers met behulp van slechte software heel goed in staat zijn, betrouwbare informatie te verstrekken en dat slordige gebruikers de resultaten van goede software zeer wel negatief kunnen beïnvloeden.
Rond dit thema is het artikel opgebouwd en uitgewerkt.
De vragen zijn: wat is nu eigenlijk het onderzoeksobject, hoe diepgaand moet het onderzoek zijn en voor wie zijn de resultaten van belang.

Hierna volgt een interessant betoog over de te hanteren Soll-positie bij de controle van software ("Ook software-controle is als alle controles een Soll-Ist vergelijking").
Bij software waarmee een administratie gevoerd kan worden is de Soll-positie, dat de software een ordelijke administratie mogelijk moet maken. Dit uitgangspunt is een te ruim en moeilijk operationeel te maken begrip. Zelfs indien "ordelijke administratie" (ordnungsmässiger Buchführung) afdoende zou kunnen worden gecodificeerd, is daarmee nog niet de Soll voor de administratieve software gedefinieerd.
Die software immers is het middel waarmee wordt geadministreerd, terwijl ordelijke administratie een samenspel is tussen middelen, voorschriften en menselijke handelingen.
Of zoals de schrijver stelt:

"Bekanntlich kann man aber mit ein und demselber Hammer je nach Geschick den Nagel krumm oder gerade in die Wand schlagen."

De speurtocht naar een geschikte Soll-positie eindigt enigszins teleurstellend: het oude (handmatige) systeem of vergelijkbare administratieve systemen moet als Soll worden gekozen.
De toetsingsnorm luidt dan dat de software het voeren van een ordelijke administratie ten opzichte van de oude situatie moet vergemakkelijken, of in elk geval niet verzwaren.
In de visie van de schrijver is dit overigens een logische gevolgtrekking; de schrijver gaat er vanuit dat (toekomstige) gebruikers - en de lezers van het software-certificaat - erop uit zijn het administreren met behulp van automatisering te rationaliseren.

De mate van rationalisatie moet dus worden vastgesteld.
De betrouwbaarheid van de administratie kunnen de gebruikers immers heel goed zelf beïnvloeden.

Behalve in situaties waarin de software als zodanig wordt gecontroleerd (in grote lijnen: kwaliteitscontrole, efficiency, prestatiekenmerken, etc.), komt het erop neer, dat de certificering van software, die wordt toegepast binnen een stelsel van interne controlemaatregelen, uiteindelijk voert tot een certificering van dat IC-stelsel.

Het artikel bevat een overzicht waarin een onderscheid aangebracht is tussen hardware-controles en organisatiecontroles. Onder de noemer organisatiecontroles blijken procedures, totaal-afstemmingen en geprogrammeerde controles te zijn begrepen.
De schrijver geeft voorts een overzicht van de stappen die bij een software-controle achtereenvolgens worden gezet.

Met betrekking tot de af te geven mededeling volgt een opsomming van de in de mededeling op te nemen aspecten. Hierbij wordt gebruik gemaakt van de tekst van mededelingen in het kader van de jaarrekeningcontrole.
Daarbij de waarschuwing dat, indien de software geïsoleerd van de administratieve organisatie en interne controle bij de gebruiker is onderzocht, de mededeling geen uitspraak kan bevatten over de met behulp van de software te bereiken "ordelijke administratie".
Dat hangt immers van het gebruik af.

Voorgesteld wordt, in de mededeling op te nemen welke eisen te stellen zijn aan de maatregelen van interne controle in de administratieve organisatie van de (toekomstige) gebruiker.
Daarnaast zou de mededeling nog voorwaarden kunnen bevatten zoals bijvoorbeeld de voorwaarde dat:
- de maker de handhaving en het onderhoud van de gecontroleerde software moet kunnen garanderen;
- de maker zorgt voor voldoende scholing van de toekomstige gebruiker, etc.

Het artikel besluit met een overzicht van de inhoud van de opdrachtbevestiging, waarin ook wordt opgenomen op welke wijze de software-producenten bekendheid mogen geven aan het onderzoek en de resultaten ervan, alsmede een voorstel (aan de opdrachtgever) over de tekst van de af te geven mededeling.

Het probleem van de verkoopreclame "over de rug van de onderzoeker heen" valt volgens de schrijver op te lossen door bij de opdracht minimaal te bedingen dat die reclame onopvallend moet geschieden en dat de naam van de onderzoeker daarbij niet mag worden genoemd.

Daarenboven wordt nog geadviseerd een "Letter of Representation" (L.O.R.) te vragen, waarin de opdrachtgever moet verklaren dat er geen andere bestanden en programma's nodig zijn dan die, welke in de documentatie zijn beschreven, dat het te verkopen pakket identiek is aan het onderzochte en dat eventuele wijzigingen worden toegelicht wanneer het certificaat aan geinteresseerden wordt verstrekt.

Met name de suggesties voor de L.O.R. getuigen van weinig vertrouwen in de mogelijkheden van de onderzoeker en van wat al te veel optimisme met betrekking tot de waarde van de onderhoudsclausule.

In Nederland heeft het NIvRA zich destijds bezig gehouden met de problematiek van de controle van software inclusief de daarbij noodzakelijke maatregelen van interne controle.
(NIvRA-geschrift nr. 26, 1982.)
Uit een commentaar op dit geschrift door H.A. Kampert RA citeren wij:
"De mededeling maakt gewag van een stelsel van maatregelen en procedures voor zover gericht op de betrouwbaarheid en continuïteit. Daarover wordt meegedeeld, dat het stelsel voldoet aan redelijkerwijs te stellen eisen. Deze wijze van formuleren maakt terecht onderscheid tussen betrouwbaarheidsbevorderende maatregelen en de betrouwbare gegevensverwerking zelf. Langzamerhand ontstaat in het beroep de neiging om kortheidshalve zich van een te suggestief woordgebruik te bedienen door van een betrouwbaar systeem en betrouwbaarheidsonderzoek te spreken en dus om maatregelen en betrouwbaar systeem te vereenzelvigen."

Ook hier wordt het gevaar gesignaleerd van het al te ijverig doortrekken van conclusies over het middel naar conclusies over het produkt dat onder andere met behulp van dit middel tot stand komt.
De normen voor de certificering van een met behulp van automatisering gevoerde administratie - met een ander doel dan jaarrekeningcontrole - zijn nog niet beschikbaar.
In het vakgebied van de automatisering is de certificering van software inmiddels uitgebreid in discussie. In accountantskring is met de publicatie van NIvRA het laatste woord zeker niet gezegd en verdere studie op het gebied van de controletechniek is gaande.
Het ligt in de bedoeling om in een van de volgende nummers van COMPACT nader in te gaan op de software-certificering met een overzicht van publicaties en visies.

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

COMPACT

Winter 1985/1986

Automatisering
Beveiliging
Controle
NIEUWS

door M.C. Duym, J.F.C. van Epen en drs. J. Kuipers

Automatisering

Twee wijzen van fouttolerantie

Kort geleden heeft Stratus Computers, leverancier van fouttolerante systemen, in het World Trade Center Amsterdam haar Nederlandse vestiging geopend.

Hieronder wordt kort ingegaan op de verschillen tussen twee merken fouttolerante computers, Tandem Non Stop computers en Stratus.

Fouttolerante computers zijn computers die een geringe kans hebben buiten bedrijf te raken doordat ze gebruik maken van parallelle processoren. Het verschil is gebaseerd op het bereiken van fouttolerantie via software (Tandem, begonnen in 1974) of via hardware (Stratus, begonnen in 1980).

Software-matige benadering

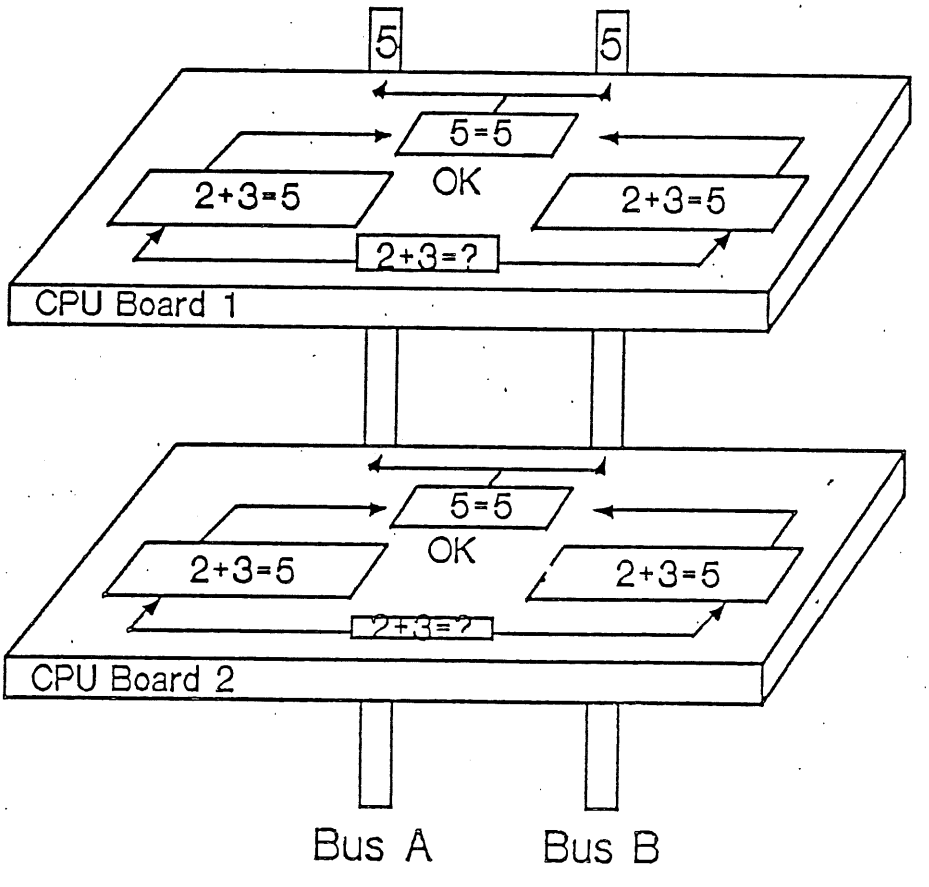
In Tandem computers is de centrale verwerkingseenheid met twee processoren uitgevoerd.
Beide processoren voeren een eigen taak uit en staan permanent klaar om als back-up voor de ander te dienen.
Hiervoor is het nodig dat beide processoren continu op de hoogte worden gehouden van wat de ander doet.
Door deze onderlinge, zeer intensieve communicatie wordt een deel van de verwerkingscapaciteit in beslag genomen.
Om elkaar op de hoogte te kunnen houden dient checkpoint-informatie opgeleverd te worden.
Deze informatie kan alleen verstrekt worden als het programma daarvoor geschikt gemaakt wordt.
Een checkpoint is een punt in een programma waarop de in- en uitvoerbuffers worden geleegd en het werkgebied en enkele besturingsgegevens op journalfile worden opgeslagen om een herstart vanaf dit punt mogelijk te maken.
Dit betekent dat een programma dat zonder meer wordt overgezet op een Tandem computer daarmee nog niet fouttolerant werkt.

Valt een van de twee processoren door een fout uit dan wordt de werklast nog maar door de ene overgebleven processor uitgevoerd.
Dit betekent verlies aan snelheid, capaciteit.

Hardware-matige benadering

Stratus heeft gekozen voor een dubbele uitvoering van de processoren waarbij elke processor dezelfde taak uitvoert.
Onderling zal geen statusinformatie worden uitgewisseld omdat beide processoren precies hetzelfde doen.
Gevolg is tevens dat programmatuur niet fouttolerant gemaakt hoeft te worden. Dit heeft weer consequenties voor de software onderhoudskosten.
Bij een storing werkt het systeem met dezelfde capaciteit door.
Deze hardware-matige benadering is mogelijk geworden door de dalende hardwareprijzen.

De werking van de hardware-matige benadering is in onderstaande figuur nader uiteengezet.



Bronnen: De Automatisering Gids en Computable.

Beveiliging

Les uit de aardbevingsramp in Mexico

Edpacs van januari 1986 bevat een verslag over de ervaringen met de back-up-voorzieningen van de computercentra die door de ramp werden getroffen. De schrijver (George Folch) betoogt dat ondanks de "sad experiences" ook een aantal lessen te leren zijn. Alhoewel wij in Nederland weinig kans op een aardbeving hebben, is het toch denkbaar, dat zich een ramp met soortgelijke karakteristieken voordoet. Deze karakteristieken waren:

1. zeer veel centra worden tegelijkertijd onbruikbaar;
2. een deel van het personeel komt om;
3. toeleveranciers van computers, randapparatuur, papier e.d. zijn ook niet meer operationeel;
4. niet alleen door puin, maar ook door de dagenlange afzetting van het rampgebied door troepen kan personeel niet bij het centrum komen;
5. overheidsdiensten voor gas, water, elektriciteit en telecommunicatie vallen uit.

Enkele dingen waaraan in veel gevallen niet was gedacht:

- het niet in werking stellen van de noodstop;
- uitvallen noodstroom door omvallen batterijen en/of beschadiging daarvan door vallend puin;
- draagbare lampen voor zoeken naar personeel, nog bruikbare apparatuur etc.;
- medicijnen;
- gegevens personeelsleden. Is iedereen er? Wie is in welk ziekenhuis opgenomen? Wie is beschikbaar? Wat zijn de naaste familieleden?
- voedsel en water;
- communicatiemogelijkheden ten behoeve van contacten met leveranciers en andere vestigingen. Door de vernietiging van het ene centrale telefoongebouw van de locale PTT was ook geen communicatie meer mogelijk.

Conclusie:

- Concentratie van computercentra en leveranciers in geografisch klein gebied is riskant (denk aan Amsterdam).
- Alleen een back-up-site op grotere afstand gaf redding.
- Bedrijven met centra buiten het rampgebied maar met minder compatible apparatuur en software waren nauwelijks in staat binnen een redelijke termijn weer operationeel te zijn.

Beveiliging van on-line-systemen

Er is een toenemende aandacht te constateren rond de beveiliging van on-line-systemen.
Het probleem van de beveiliging van on-line-systemen is niet nieuw.
Opvallend is de toegenomen aandacht in de media voor ongeautoriseerde toegang tot systemen, denk bijvoorbeeld aan het "kraken" van het 008-systeem van de PTT en de discussie over de te treffen juridische maatregelen.
In dit kader past dan ook het in de boekhandels verschijnen van een handboek voor computerkrakers waarin de principes van het kraken aan de hobbyist worden uitgelegd (Handboek voor Computer Kraken & Beveiligen, Hugo Cornwall & Wouter Hendrikse, De Achterkant, Leiden 1985, besproken in Compact Zomer/Herfst 1985).
Een en ander kan een goede aanleiding zijn om de interne controlemaatregelen voor on-line-systemen (weer) eens kritisch na te gaan.

Mede op basis van de artikelen Audit of Security over Online Transaction Systems: Environmental Concerns van J.B. Mullen (The Internal Auditor August 1985), Den Hackern ein Schnippchen Schlagen van Michael Sigesmund (Die Computer Zeitung 30 april 1985) en de concept-lijst Attentiepunten Computerbeveiliging van het N.G.I. worden een aantal punten genoemd die van belang zijn bij het beheersen van on-line-systemen.

Toegang tot terminals

De toegang tot terminals dient gecontroleerd plaats te vinden.
Er dient toezicht gehouden te worden op het gebruik van de terminals. Het moet niet zo zijn dat willekeurige personen zo maar kunnen gaan experimenteren met terminals.
Door voor het beheer van terminals bepaalde personeelsleden verantwoordelijk te stellen neemt de beveiligingsbewustheid toe.
Deze verantwoordelijkheid dient dan vastgelegd te worden in de taakbeschrijving van de functionaris. Buiten de normale werkuren dienen de terminals afgesloten te kunnen worden.
Voor het aansluiten van nieuwe terminals of het verplaatsen, afsluiten van bestaande terminals dient door de verantwoordelijke functionaris toestemming gegeven te worden.

Communicatielijnen

Evenals terminals dienen de communicatielijnen, bijvoorbeeld de bekabeling, voorwerp van beveiliging te zijn.

Het is voor een professional geen probleem meer illegaal aan te sluiten op interne netwerken. Dit probleem speelt vooral als een bedrijfsgebouw met verschillende huurders wordt gedeeld.
Het technisch beheer van het netwerk kan toegewezen worden aan een aparte functionaris die de zorg draagt voor de kwaliteit en de beschikbaarheid van het netwerk. Deze functionaris dient echter geen bemoeienis te hebben met het uitgeven en beheren van passwords.
Indien toegang verkregen kan worden via het telefoonnet verdient het aanbeveling gebruik te maken van een automatische terugbelprocedure.

Software-matige beveiligingen

De toegang tot en het gebruik van het systeem kan middels TP-monitor, DBMS, library-pakket of speciale toegangsbeveiligingspakketten gecontroleerd worden.
Deze software dient zorg te dragen voor:
- toegang tot het systeem middels een sign-on-procedure, te denken valt onder meer aan het weigeren van toegang tot het systeem indien een aantal malen achter elkaar foutief is aangelogd;
- autorisatie over het gebruik van transacties, bestanden en gegevens, te denken valt bijvoorbeeld aan beveiliging middels een dwingend menu;
- registratie van terminal-activiteiten (ook van niet geslaagde sign-on pogingen), zodat controle achteraf mogelijk is;
- automatische sign-off nadat de terminal enige tijd niet meer gebruikt is;
- het niet kunnen benaderen van de password-tabel.

Wanneer het wijzigen van passwords niet door de eindgebruikers zelf geschiedt, dient het password beheer te worden uitgevoerd door een functionaris die geen inhoudelijke bemoeienis heeft met de geautomatiseerde gegevensverwerking.

Beveiliging van gegevens tegen ongeautoriseerde kennisneming of manipulatie geeft aanleiding tot:
- het scheiden van de (on-line) test- en produktie-omgeving om te voorkomen dat getest wordt met het live produktiesysteem. Het gevaar bestaat dat het produktiesysteem down gebracht wordt en gegevens onjuist gewijzigd worden.
- beveiliging van calls, subroutines en jobcontrol-statements;
- encryptie van passwords en gevoelige gegevens.

Remote support

Indien gebruik wordt gemaakt van remote maintenance (ook wel remote support) dienen maatregelen getroffen te worden die de geautoriseerde toegang tot het systeem en de juiste afwikkeling van het onderhoud controleren.
- Het initiatief voor het tot stand komen van de verbinding kan uitsluitend bij het computercentrum gelegd worden;
- Per sessie kan door het management een éénmalig password worden uitgegeven;

- Vooraf kunnen gevoelige bestanden ontkoppeld worden.

Herstelmogelijkheden

Maatregelen om de juistheid en volledigheid van de transactieverwerking en de blijvende juistheid daarvan te beheersen omvatten:
- een adequate logging van transacties zodat herstel mogelijk is;
- het bewaren van kopieën van documentatie, systeemsoftware en applicatie programmatuur;
- het opleveren door de systeemsoftware van voldoende diagnostische informatie ingeval van fouten;
- de aanwezigheid van procedures met betrekking tot het herstarten en herstellen van de verwerking vanaf het moment van storing;
- zoveel mogelijk het dagelijks afstemmen van de juiste verwerking van de invoer, te denken valt onder andere aan het vastleggen van de dagelijkse transactie-omvang;

Algemeen geldt dat de getroffen maatregelen voldoende gedocumenteerd en begrepen moeten zijn, zodat een actief beveiligingsbewustzijn kan ontstaan. Bij het beveiligen van on-line-systemen moet niet uit het oog verloren worden dat met een goed beveiligd on-line-systeem, maar een zwak beveiligd batch-systeem (bijvoorbeeld de mogelijkheid om ongeautoriseerde ponsconcepten tussen te voegen) de beheersing van het totale systeem nog niet voldoende behoeft te zijn.

Risico verbonden aan beveiligingsmaatregel

Dat elke beveiligingsmaatregel op zich ook een zeker risico in zich draagt, zal voor ieder duidelijk zijn. Zo kwamen ons de afgelopen tijd twee voorvallen met halon brandblusinstallaties ter ore. In beide gevallen werd de brand op een voortreffelijke wijze geblust. Achteraf trad als gevolg hiervan toch nog schade op. Deze werd voor zover ons bekend, overigens wel door de verzekering gedekt.

In het eerste geval werd ijzervijlsel mee de zaal ingespoten als gevolg van verroeste leidingen. Dit leidde later tot kortsluiting in de CVE.

In het andere geval reageerde het halon met de metaallegering van enkele contacten in de computerapparatuur waardoor deze computer niet meer goed functioneerde. Daar dit type legeringen echter niet in alle merken voorkomt en het aantal mechanische contacten snel afneemt wordt het risico op deze schade steeds kleiner.

Controle

Onderzoek van back-up-procedures

Inleiding

Naar aanleiding van een artikel in Edpacs van november 1985 en het bericht over de aardbeving in Mexico in de rubriek Beveiliging, willen wij het onderzoeken van de back-up-procedures in de schijnwerpers zetten.

Aanpak van het onderzoek

Gezien de gemiddelde graad van automatisering, is het voor de interne en externe accountant doorgaans niet goed mogelijk om een integrale controle van de back-up-procedures uit te voeren. Om een optimale effectiviteit te verkrijgen moeten keuzen worden gemaakt. Het is in dit verband aan te bevelen, de volgende richtlijnen in acht te nemen:

1. ga uit van de voor de bedrijfsuitoefening meest kritische systemen. Neem echter ook een of meer van de minder belangrijke systemen. In bijna alle gevallen zullen de kosten van back-up opwegen tegen die van het werken zonder dit systeem of van nieuwbouw (als daar dan capaciteit voor is!) en het nadelige effect op de bedrijfsvoering. Meer over de classificatie van gegevens en toepassingen is te vinden in het Edpacs nummer van december 1985. In dit artikel wordt een classificatiesysteem beschreven waarin onder meer de volgende parameters een rol spelen:
   a. kosten gemaakt bij het creëren van gegevens, documentatie en programmatuur;
   b. kosten of moeilijkheidsgraad van reconstructie;
   c. effect op de managementbeslissingen bij ontbreken gegevens;
   d. maximaal acceptabele vertragingstijd in het beschikbaar komen van gegevens;
   e. eisen die door overheidsorganen, beroepsorganisaties, de markt en het management worden gesteld aan de bewaartermijn van gegevens;
   f. eisen die aan de tijdsduur van de verwerking worden gesteld door andere toepassingen;
2. leg - tijdens het onderzoek rekencentrum en van systemen - dossiers aan ten behoeve van het onderzoek back-up.

Uitvoering onderzoek

Stappen:

1. Doornemen handboek rekencentrum op de volgende onderdelen:
   - naamgevingsnormen;
   - bestandsbeheer standaarden;
   - bewaar- en verversingstermijnen;
   - gebruik library software.

2. Doornemen van de produktieplanningen (dag-, week-, maand- en jaarplanning) en catalogs om vast te stellen welke systeemsoftware, utilities, applicaties en bestanden operationeel zijn;

3. De volledigheid beoordelen van de lijst met kritische systemen of laat deze vaststellen door het management. Zorg dat deze lijst naast het belang voor de bedrijfsuitvoering ook de volgorde aangeeft waarin de betreffende systemen in de recovery-procedure weer operationeel moeten worden.

4. De systemen selecteren die in het verdere onderzoek zullen meelopen.

5. Doornemen applicatiedocumentatie met betrekking tot:
   - benodigde programma's;
   - gebruikte utilities;
   - gebruikte bestanden;
   - relaties met andere systemen;
   - bewaartermijnen;
   - gehanteerde back-up en recovery-procedure;
   - restart-instructies.

6. Doornemen inventarislijst back-up site(s). Hierop moeten de volgende voorraden zijn geregistreerd:
   - tapes met inhoud.
     Van de programma's moet aanwezig zijn:
     . source code
     . load libraries
     . cataloged procedures
     . JCL
     . batch streams
   - gebruikersbestanden;
   - systeembestanden:
     . system files
     . tape management
     . access control
   - documentatie van
     . programma's
     . programma uitvoeringsinstructies
     . werkinstructies
     . noodprocedures
   - hulpmaterialen;
   - voorgedrukte formulieren;
   - lege tapes en lege packs om direct kopieën te kunnen maken;
   - papier en linten;
   - masters van formulieren indien deze niet door de leverancier worden bewaard;
   - gegevens over leveranciers van hardware, software en hulpmaterialen
   - voedsel, munten voor publieke telefooncellen, communicatie-apparatuur, medicijnen, draagbare lampen;
   - personeelsgegevens en gegevens naaste familieleden.

7. Steekproefsgewijze inhoudelijke controle van:
   - tapes door het afdrukken van labels en een aantal blocks. Let naast inhoud ook op record-indeling en bloklengte;
   - formulieren op laatste versie, of versie die nog acceptabel is (bijvoorbeeld oud logo).

8. Vaststellen, dat door het rekencentrum regelmatig een 100% controle plaatsvindt.

9. Controle toegangsbevoegdheden actueel en back-up-sites en de registratie daarvan en het actueel gebruik.

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

ONDERWIJS

Cursus Aanpak Systeembeoordeling en Accountantscontrole (CASA)

5- respectievelijk 8-daagse open cursus.
De laatste 3 dagen van de 8-daagse versie (blok C) zijn uitsluitend bestemd voor accountants in de functie van "controleur" van de jaarrekening.

Doel

De cursus heeft als doel de cursist kennis bij te brengen om:
- de kwaliteit van de interne controle van een in belangrijke mate geautomatiseerd systeem van gegevensverwerking te kunnen beoordelen;
- een doelmatige aanpak van accountantscontrole, al dan niet met behulp van de computer, op basis van het verrichte systeemonderzoek te kunnen bepalen;
- op doelmatige wijze de mogelijkheden tot systeemonderzoek in de controle van de jaarrekening te gebruiken.

Inhoud

De cursus bestaat uit drie blokken. In de eerste twee blokken wordt een methode gepresenteerd ten behoeve van het beoordelen van een informatiesysteem op betrouwbaarheidsaspecten. De methode demonstreert, doordat meer de nadruk wordt gelegd op een functionele benadering van de geautomatiseerde gegevensverwerking dan op de technische aspecten daarvan, dat deze activiteit in belangrijke mate kan worden uitgevoerd door functionarissen met algemene kennis op het gebied van automatisering en interne controle. Tevens wordt duidelijk waar deskundigheidsgrenzen moeten leiden tot inschakeling van op automatisering en controle gespecialiseerde EDP-auditors.
In het derde blok wordt ingegaan op de aanpak van de accountantscontrole en het onderkennen van mogelijkheden tot gebruik van de computer daarbij, alsmede op de vraag met welke diepgang systeembeoordeling in het kader van de jaarrekeningcontrole moet plaatsvinden.

Blok A Doorgronden van de bedrijfsfuncties en het informatiesysteem (3 dagen)

De voornaamste moeilijkheid voor de beoordelaar is om op snelle en doeltreffende wijze het systeem in hanteerbare vorm in kaart te brengen. De functionele benadering bewijst hierbij haar nut, vooral doordat de beoordelaar slechts minimale hinder ondervindt van de techniek. De functionele benadering maakt bovendien een variabele diepgang per systeemonderdeel mogelijk. Als eindresultaat komt tot stand een door de cursisten opgestelde globale, maar doelgerichte beschrijving van het informatiesysteem, waarin de te beheersen systeemfuncties duidelijk tot uiting komen.

Blok B Inventarisatie en evaluatie betrouwbaarheidsmaatregelen (2 dagen)

De door de onderzoeker per systeemfunctie opgestelde betrouwbaarheidseisen worden geconfronteerd met de in realiteit aangetroffen maatregelen, hetgeen leidt tot een oordeel over het systeem.

Blok C Systeemonderzoek en de relatie met de controle van de jaarrekening (3 dagen)

Dit blok is uitsluitend bestemd voor accountants in de functie van "controleur" van de jaarrekening.
Goede methoden van systeemonderzoek bieden nog geen garantie dat het onderzoek naar systemen in het kader van de jaarrekeningcontrole steeds op doelmatige wijze wordt verricht.
Veelal wordt op grond van bepaalde criteria een keuze gemaakt van te onderzoeken systemen. Bovendien dreigt het gevaar dat voor onderzoek geselecteerde systemen veel diepgaander worden onderzocht dan in het kader van de jaarrekeningcontrole noodzakelijk is.
Tenslotte wordt vaak niet systematisch gekeken naar de mogelijkheden tot gebruik van de uitkomsten van de systeembeoordeling, alsmede de computer bij de uitvoering van de accountantscontrole. Een goed uitgevoerd systeemonderzoek biedt daarvoor goede uitgangspunten. Onderdeel C van de cursus gaat op de genoemde gebieden in.

De laatste dag van dit blok is een praktijkdag. De cursisten gaan zelfstandig aan het werk met audit-programmatuur op een microcomputer en worden ter plekke geconfronteerd met de resultaten van hun werk.

Wijze van kennisoverdracht

Aan de hand van de casus Rippkoff (waar gebruik wordt gemaakt van diverse geautomatiseerde systemen met on-line gegevensvastlegging en batch-gewijze verwerking) moeten de cursisten in werkgroepen een aantal opdrachten uitwerken. Daarbij wordt stapsgewijs de methode Aanpak Systeembeoordeling gevolgd. Naast ter beschikking gestelde documentatie van het systeem wordt veelvuldig gebruik gemaakt van interviews (rollenspel).
De uit te voeren opdrachten worden ondersteund door inleidingen eventueel in combinatie met "vingeroefeningen".

De achtste dag van de cursus is een praktijkdag.
De cursisten gaan zelfstandig aan het werk met een audit-pakket op een microcomputer.

De cursus heeft in belangrijke mate het karakter van een workshop.

Bestemd voor

De cursus is bestemd voor hen die werkzaam zijn in de interne of accountantscontrole alsook voor systeembeheerders aan gebruikerszijde. Basiskennis op het gebied van automatisering en interne controle vereist. Zie onze Basiscursus Automatisering en Interne Controle.

Voor blok C is uitgebreide kennis en ervaring op het gebied van de accountantscontrole noodzakelijk.

Voorstudie

Vooraf ontvangen de cursisten ter bestudering:
- algemene gegevens van Rippkoff (het casusbedrijf);
- syllabus PRISMA (ten behoeve van het onderdeel Doorgronden van de bedrijfsfuncties);
- syllabus Aanpak Systeembeoordeling.

Benodigde tijd: ca. 4 uur.

Maximum aantal deelnemers

20.

Voor de algemene voorwaarden van inschrijving wordt verwezen naar de cursus-brochure.

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

Overzicht hoofdartikelen 1983/1985

nummer		
30	9e Jaargang (83/1), winter 1982/3	
	- Automatisering voor de rechter hersenhelft	drs. A. Kranendonk
	- Beoordeling betrouwbaarheid van een geautomatiseerd systeem; een aanpak	A.H.C. Koedijk en H. Weerd
	- De microcomputer in de accountantscontrole	H. Veenman
	- A science fiction trip into auditing	R.H. Healey (TR)
31	10e Jaargang (83/2), lente 1983	
	- Gebruik en controle van on-line applicaties	J.L.H. Kooijman
	- Beheersing, beveiliging en controle van het IBM systeem/38	A.H.C. Koedijk
	- Current developments for future thinking	R.H. Healey (TR)
32	10e Jaargang (83/3), zomer 1983	
	- Continuïteit van de gegevensverwerking, een inleiding	H. Roos
	- Back up, restart en recovery (deel 1, back up)	R. Bron
	- Onderzoek naar werking interne controle mogelijk?	drs. J.E. Huizenga
	- Data entry en interactief programmeren via de terminal: het pakket ICCF nader bekeken	R.P. Bosman
	- Down to earth again, KMG potential	R.H. Healey (TR)
33	10e Jaargang (83/4), herfst 1983	
	- Backup, restart en recovery (deel 2, recovery en restart)	R. Bron
	- Password-protectie	A. van der Drift
	- Gebruikersparticipatie op verschillende wijzen beschouwd	H. Frijters
	- How cheap computers are affecting external audit	W. List (TMcL)
34	10e Jaargang (84/1), winter 1983/ lente 1984	
	- Accountant en elektronische informatieverwerking	prof. D. Steeman
	- 100 + 50 - 20 = 80 ??????? De betekenis van concurrency control	A. van der Drift
	- De micro en de controlerende accountant	L. Straathof
	- Opleiding risk manager	F.H. Horbeek (RB) H.A. Huyskens (RB)

Noot afkortingen

TR = Thorne Riddell Canada
TMcL = KMG Thomson McLintock & Co UK
RB = Rabobank, leden werkgroep NGI en VBB

COMPACT

Winter 1985/1986

35	11e Jaargang (84/2) zomer 1984	
	- Controls in systems using modern technology	W. List CA MBCS, (TMcL)
	- Het beoordelen van database-systemen	A. van der Drift
	- Data dictionary systemen in relatie tot het gebruik van data base en data communicatie-technieken	H. Weerd
	- Interactieve consolidatie op de microcomputer met behulp van het pakket Multiplan	drs. P.A.M. Diekman
36	11e Jaargang (84/3) herfst 1984	
	- Security management: from the past to the future	drs. H.C. Kocks
	- De organisatie rond een Systeem/38	H.J. Lijnes
	- Beveiligingsaspecten in netwerken: Theorie en Praktijk	ing. C.J.M. Gielen en H. Weerd
37	11e Jaargang (85/1) winter 1984/1985	
	- Hoe betrouwbaar zijn onze computers?	A.W. Neisingh
	- Beveiliging in lokale netwerken	ing. H.A.J.M. Spape
	- Basic groeit	J.E. de Bue
38	12e Jaargang (85/2) lente 1985	
	- "Capabilities, het wenkend perspectief", theorie, praktijk en toekomst van op capabilities gebaseerde computersystemen	H. Roos
	- Knowledge based systems: een stap vooruit in de beheersbaarheid van administratieve processen	A. van der Drift
	- Vierde generatietalen	drs. J.E. Huizenga
	- Informatie over (elektronische) informatie "Werken met een database"	D. Boom
39	12e Jaargang (85/3) zomer/herfst 1985	
	- De overdrachtsprocedure is meer dan een gebruikerstest	J.C. Boer
	- New technology and new risks in security and control beveiligingsproblematiek in POS en ATM systemen bij banken	A.W. Neisingh en H. Weerd
	- Documentatie van geautomatiseerde informatiesystemen en systeemonderzoeken; vragenlijsten	J.M. Verheul

Noot afkortingen
TMcL = KMG Thomson McLintock & Co UK

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