J. ten Wolde

compact

COMPUTER EN ACCOUNTANT

Klynveld Kraayenhof & co
ACCOUNTANTS

VOORJAAR 1977 3E JAARGANG NR. 3

10

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

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

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

Redactie:
A.W. Neisingh, J. Philippo,
D. Steeman en J.H. Urbanus.

Adres: Pr. Irenestraat 59 Amsterdam

VAN DE REDACTIE

Bestaat de lezerskring van Compact normaliter uit hen, die de automatiseringscursus van de maatschap hebben gevolgd, gezien de inhoud van het voor U liggende nummer wordt Compact deze keer verspreid onder alle accountants en controleleiders.

In dit nummer is de eerste aflevering opgenomen van het artikel "Het gebruik van de computer in de accountantscontrole" door A.W. Neisingh, terwijl H.J.M. van der Wielen zijn visie vastlegde met betrekking tot "Noodzaak tot aanwezigheid van de accountant in het computercentrum".

Het boekje "Data base en accountant" wordt besproken door C.J.E. Lankreijer met een naschrift van H. Roos.

De fraude bij ICI laat ons nog niet los. In A.B.C.-nieuws wordt daarop nog enig commentaar gegeven.

Zoals bekend zijn de leden van de Automatiserings- en Controlegroep onder meer op de hoogte van de mogelijkheden van het gebruik van de computer in de accountantscontrole en de faciliteiten (zoals de eigen computer) die binnen onze maatschap kunnen worden geboden.

Schroomt U niet U door één van de leden van de A.C.-groep op de hoogte te laten stellen van de mogelijkheden in Uw specifieke situatie.

Degenen, die Compact voorheen niet ontvingen, doch in de toekomst toezending op prijs stellen, kunnen daartoe bericht zenden aan de heer J. Philippo (kantoor Amsterdam).

HET GEBRUIK VAN DE COMPUTER IN DE ACCOUNTANTSCONTROLE

door A.W. Neisingh

Inleiding

Wanneer de accountant een opdracht aanvaardt tot controle van de jaarrekening zal hij allereerst een onderzoek moeten instellen naar de kwaliteit van de organisatie van de gecontroleerde en de daarin begrepen maatregelen van interne controle. Op grond van de kennis omtrent de wijze waarop de organisatie is opgezet en de werking daarvan zal de accountant moeten vaststellen welke verificatiewerkzaamheden benodigd zijn. In een controleprogramma, waarin een zo optimaal mogelijk gebruik van de beschikbare controlemiddelen zal worden nagestreefd (controlemix) wordt vervolgens aangegeven welke controlewerkzaamheden dienen te worden verricht.
Zoals bekend beschikt de accountant over een aantal controlemiddelen, te weten:

- cijferbeoordeling
- inventarisatie
- verbandscontroles
- detailwaarnemingen
- externe gegevens
- totaalcontroles.

De toenemende betekenis van de automatisering voor de gegevensverwerking, in het bijzonder op de terreinen die een rechtstreekse invloed hebben op de financiële verslaglegging, leidt ertoe, dat de accountant in het kader van de controle bij het beoordelen van opzet en werking van de organisatie aandacht aan de automatisering dient te besteden.

Een aantal controlemiddelen lenen zich voor "geautomatiseerd" gebruik, terwijl de computer daarbij als hulpmiddel kan fungeren.
Bij het op deze wijze gebruiken van de computer kan worden gedacht aan het selecteren van te controleren posten, waarbij als mogelijkheden kunnen worden genoemd:

- het gebruik van steekproefroutines in programmatuur, waarmee op snelle en vooral juiste wijze te controleren posten ten behoeve van een detailwaarneming op grond van vooraf gedefinieerde criteria uit een massa worden geselecteerd;
- het (geautomatiseerd) confronteren van posten met een norm;
- het vergelijken met behulp van de computer van gegevens (op basis van [on]gelijkheid).

Daarnaast kan de computer in de accountantscontrole ook worden gebruikt voor het testen van de juistheid en de goede werking van operationele programmatuur.

In dit artikel zal allereerst worden ingegaan op het onderzoek van gegevensverzamelingen met behulp van controleprogrammatuur, terwijl daarnaast een enkele opmerking zal worden gewijd aan voor specifieke doeleinden ontwikkelde programmatuur.

In het volgende nummer van Compact zal allereerst worden ingegaan op de problematiek ten aanzien van data base en audit software, terwijl vervolgens aandacht zal worden besteed aan technieken ten behoeve van het testen van programmatuur, zoals:

- het testen van programmatuur met behulp van
  - testgevallen
  - integrated test facility
- parallel simulation
- het gebruik van flowcharting pakketten
- missed branch indicators.

Tot slot zal een overzicht van de nieuwe ontwikkelingen worden gegeven.

Het onderzoek van gegevensverzamelingen met behulp van audit software

Wanneer de accountant heeft besloten in zijn controle de computer te gebruiken voor het onderzoek van gegevensverzamelingen, kan hij gebruik maken van standaard audit packages of van eigen, per geval te ontwikkelen programmatuur.
Het is echter ook mogelijk in toepassingsprogrammatuur van de gecontroleerde zodanige voorzieningen op te nemen, dat op deze wijze in de behoefte(n) van de accountant kan worden voorzien.

Opgemerkt wordt, dat de onafhankelijkheid van de accountant ter zake van de uitvoering van zijn controlewerkzaamheden in gevaar kan komen omdat de "wandel" van de operationele programmatuur, waarin zijn controleroutine is geïntegreerd, zich aan zijn waarneming onttrekt. De accountant zal dus bij iedere wijziging, die in het operationele programma wordt aangebracht, betrokken moeten worden om de invloed van de programmawijziging op het functioneren van de controleroutine vast te stellen.
Daarnaast zal de accountant moeten constateren, dat tijdens de computerverwerking de controleroutine ongewijzigd en correct wordt gebruikt.

In geval de automatiseringsorganisatie in ernstige mate niet voldoet aan de eisen, die daaraan vanuit een oogpunt van interne controle moeten worden gesteld, kan de accountant ten behoeve van zijn controle van de boven omschreven techniek geen gebruik maken.
De ingewikkeldheid van bestaande programmatuur, alsmede de risico's verbonden aan het toevoegen van een of meer controleroutines aan deze programmatuur kan de accountant van deze mogelijkheden doen afzien.

Als voorbeelden kunnen worden genoemd:

- het opnemen van een steekproefroutine in het grootboekmutatieprogramma van de gecontroleerde en het afdrukken van de in de steekproef getrokken posten (inkoopfacturen, kasstukken en dergelijke), alsmede
- het signaleren van posten die in de controle de aandacht verdienen, zoals kortingspercentages > x%, marges tussen verkoopprijs en inkoopprijs en inkoopprijs < y% en dergelijke.
  De signalen kunnen onmiddellijk na de verwerking worden afgedrukt.

Achtereenvolgens zullen de volgende aspecten de revue passeren:

1. Redenen van het gebruik van de computer
2. Bewerkingen
3. Stappen in verband met het opzetten van de toepassing
4. Wie programmeert de toepassing
5. Plaats van verwerking
6. Maatregelen ter verhoging van de betrouwbaarheid van de controle
7. Bewaren van programmatuur.

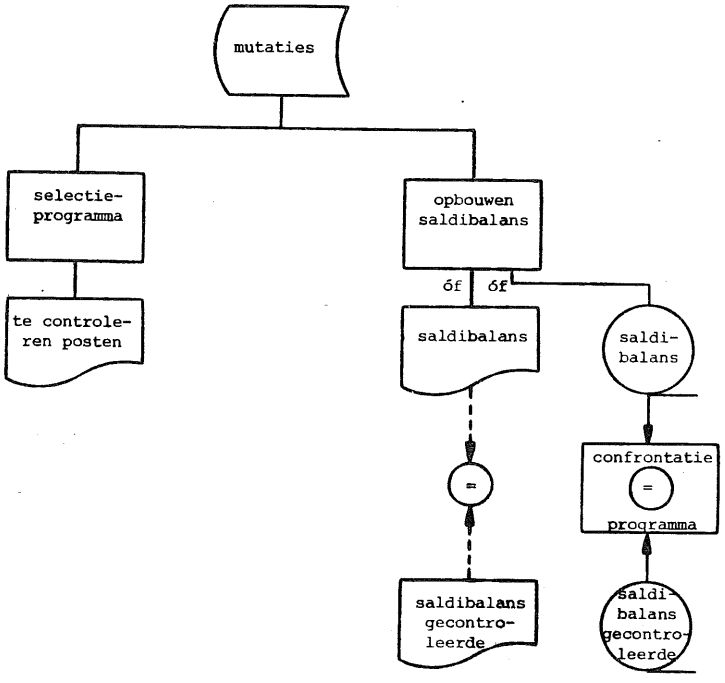
1. Redenen van het gebruik van de computer

Waarom zal de accountant de computer gebruiken in zijn controle? Verschillende redenen kunnen worden genoemd.

- De accountant zal - ondanks dat zijn informatiebehoefte een afgeleide is van die van het management - veelal informatie in een andere vorm nodig hebben.

- De accountant kan de computer gebruiken voor het maken van eigen vastleggingen ter confrontatie met die van de gecontroleerde, waarbij de confrontatie ook kan worden geautomatiseerd. De confrontatie van computerbestanden is noodzakelijk om vast te stellen, dat het bestand van de gecontroleerde, dat in feite de gegevensverzameling vormt, juist en volledig is. Computeroutput van de gecontroleerde kan door de invloed van een systematische programmafout gebreken vertonen.

In het hierna volgende blokschema worden de in beide hiervoor genoemde punten aangegeven mogelijkheden weergegeven.



figuur 1. Systeemstroomschema t.b.v. accountantscontrole

Het wordt voor de accountant ook mogelijk zelfstandig berekeningen te laten uitvoeren ter controle van de gegevens.

- Bij de redenen de computer in te schakelen bij de controle mag zeker de mogelijke besparing op controlekosten niet ontbreken, alsmede de verbetering van de kwaliteit en effectiviteit van de controle.

  (Onze ervaring is, dat zelfs ingeval veel tijd moet worden besteed aan het geschikt maken van bestanden van de gecontroleerde voor verwerking op een andere computer [conversie] een besparing op controlekosten mogelijk is.

  De kosten van analyse en programmering kunnen binnen een redelijke termijn worden terugverdiend.)

- Geautomatiseerde gegevensverwerking leidt veelal tot steeds omvangrijkere gegevensverzamelingen, waarbij steeds minder informatie in direct voor de mens leesbare vorm beschikbaar komt en controleerbare vastleggingen in een aantal gevallen gaan ontbreken. Slechts die informatie wordt afgedrukt, die in het bedrijf benodigd is voor planning, besturing en dergelijke. Dit is derhalve meestal geen historische informatie, waarover nu juist de accountant wenst te beschikken, alsmede over de middelen om de volledigheid daarvan vast te stellen.

  Wat dacht U van een microfiche, waarop 207 pagina's computeroutput (van circa 40 regels per pagina) zijn vastgelegd op 14 x 9 cm? De microfiche is niet meer machinaal verwerkbaar.

2. Bewerkingen

Onderstaande bewerkingen kunnen worden uitgevoerd met de meeste audit standaardprogrammatuur.

a. Technische functies

1. Samenvoegen van twee bestanden (met de mogelijkheid matched of unmatched records af te drukken).
2. Invoegen van gegevens uit een bestand in records van een ander bestand.
3. Sorteren.
4. Totaliseren en afdrukken.
5. Afdrukken en ponsen.

b. Audit-functies

1. Vergelijken.
2. Selecteren, zowel enkelvoudige als samengestelde selectie.
3. Trekken van steekproeven.
4. Rekenen (optellen, aftrekken, delen en vermenigvuldigen).

Met deze bewerkingen zal het veelal mogelijk zijn de gewenste toepassingen te realiseren.
In sommige gevallen zal het echter nodig zijn bepaalde bewerkingen op grond van de daarvoor geldende condities uit te voeren; meer geavanceerde standaardprogrammatuur of zelf te schrijven programma's zullen daarvoor nodig zijn.

3. Stappen in verband met het opzetten van de toepassing

De stappen in de totstandkoming van controleprogrammatuur wijken in principe niet af van de fasen in de ontwikkeling van een "normaal" automatiseringssysteem (vooronderzoek, ontwerp, analyse, programmering, testen, invoering).
Er zijn echter een aantal acties en afwegingen die moeten worden verricht voordat met de echte probleemanalyse kan worden begonnen.
Daarnaast bestaat de bemanning uit accountants - gebruiker en accountants gespecialiseerd in de problematiek ter zake van automatisering en controle.

Welke zijn nu die acties en afwegingen.
De behandelend accountant zal, zoals in de inleiding van dit artikel is genoemd, bij het opstellen van een nieuw controleprogramma, respectievelijk bij kritische herbeoordeling van het controleprogramma mogelijkheden zien bepaalde onderdelen "geautomatiseerd" uit te voeren.
Na contact met de administratie en vervolgens in overleg met een op automatisering en controle gespecialiseerde collega-accountant kunnen de gedachten nader worden bepaald en kan worden vastgesteld of door het gebruik van controleprogrammatuur respectievelijk door middel van het toevoegen van controleroutines in de gebruikersprogramma's toepassingen kunnen worden gerealiseerd.

De volgende gang zal zijn naar het hoofd automatisering, die - indien het de bedoeling is de toepassing op de computer van de gecontroleerde te verwerken - informatie zal moeten verstrekken over de computerconfiguratie, de beschikbaarheid van informatiedragers en dergelijke.
Ook zullen met hem afspraken moeten worden gemaakt over de wijze waarop de programmatuur mettertijd zal worden verwerkt.

Indien het verwerken van controleprogrammatuur niet mogelijk is, dan wel niet gewenst wordt geacht de toepassing bij de gecontroleerde te verwerken, zal moeten worden nagegaan of en op welke informatiedrager een bestand ter verwerking op bijvoorbeeld de computer van de accountant beschikbaar kan worden gesteld, respectievelijk of conversie (= technische omzetting) van het bestand mogelijk is.
De problemen bij de conversie van bestanden moeten niet worden onderschat!

Wij vestigen er de aandacht op, dat het gebruik van programmatuur in de accountantscontrole ook mogelijk is in gevallen waarbij de gecontroleerde beschikt over apparatuur met magneetbandcassettes, respectievelijk over kleine computerinstallaties.

Conversie van deze cassettes naar een magneetband is in een aantal gevallen (afhankelijk van de vastleggingscode) mogelijk door inschakeling van servicebureaus of leveranciers die over conversie-apparatuur en -programmatuur beschikken.

Vervolgens zal de systeembeheerder toestemming worden gevraagd, dat - bij voorkeur een kopie van - het benodigde bestand ter beschikking van de accountant zal worden gesteld in verband met verwerking met door de accountant ontwikkelde programmatuur.
De documentatie van het geautomatiseerde systeem waarover de accountant uit hoofde van zijn functie reeds beschikt, zal moeten worden geverifieerd ten aanzien van de bestandsorganisatie, de record- en bestandsindelingen, de omvang van de bestanden en dergelijke. (Op de problematiek ter zake van data bases en audit software wordt later ingegaan.)

Te allen tijde zal een programma moeten worden ontwikkeld waarmee - door het opbouwen van totalen - kan worden vastgesteld, dat het beschikbaar gestelde bestand overeenstemt met het bestand waaruit de gecontroleerde zijn gegevens heeft geput en waarvan de gecontroleerde de totalen ter beschikking heeft.

4. Wie programmeert de toepassing

In gevallen waarin is vastgesteld, dat door het aanbrengen van voorzieningen in programmatuur van de gecontroleerde aan de wensen van de behandelend accountant het beste wordt tegemoet gekomen, moeten deze voorzieningen door programmeurs van de gecontroleerde worden geprogrammeerd.
Probleem hierbij is evenwel, dat beïnvloeding van de controle-arbeid van de accountant hierdoor mogelijk is.
De accountant zal derhalve de programmatuur zeer grondig moeten testen en eventueel zijn toevlucht moeten nemen tot het doorlezen van (bepaalde gedeelten van) het programma.
Ingeval eigen controleprogrammatuur op de computer van de gecontroleerde zal worden verwerkt, kan per toepassing worden beslist of programmeurs van de gecontroleerde de programmering ter hand zullen nemen, of anderen. In ieder geval zullen in beide gevallen een gedetailleerde analyse en functiespecificaties moeten worden gemaakt.

Bij gebruik door de accountant van standaardcontroleprogrammatuur en information and retrieval packages zal de toepassing worden gerealiseerd door programmeurs van de accountant.
De programmering kan worden vereenvoudigd door zoveel mogelijk bewerkingen te standaardiseren en in een programmabibliotheek vast te leggen (steekproefroutines, matchen van bestanden).

5. Plaats van verwerking

De computerverwerking kan op een aantal adressen plaatsvinden, te weten op de computer van de accountant, de gecontroleerde of elders (bijvoorbeeld servicebureau).

Wanneer de verwerking van de controleprogrammatuur op de computer van de accountant plaatsvindt, wordt audit independence bereikt. De accountant heeft in dit geval intern maatregelen genomen, dat integriteit van verwerking en bestanden bereikt wordt.

Daarnaast kan als belangrijk voordeel worden genoemd, dat nu informatie afkomstig van ieder computersysteem kan worden verwerkt (mits de conversie van de benodigde bestanden mogelijk is).

Wanneer de verwerking van controleprogrammatuur op de computer van de gecontroleerde plaatsvindt dient de accountant maatregelen te nemen ter voorkoming , dat de controleprogrammatuur door de gecontroleerde wordt gekopieerd, dat de verwerking van de programmatuur wordt beïnvloed of, dat de betrokken bestanden op enigerlei wijze (opzettelijk) worden veranderd.
De volgende procedures kunnen worden gevolgd:

1. De accountant houdt zich aan de regels zoals die gelden ten aanzien van de geautomatiseerde gegevensverwerking bij de gecontroleerde. Dit heeft voornamelijk betrekking op de aanbieding van programmatuur en besturingsgegevens, alsmede op het bijwonen van de verwerking; de controleprogrammatuur wordt verwerkt als ware het een normale job.
2. De gegevensverwerking vindt plaats onder de verantwoordelijkheid van de accountant. Deze heeft hierdoor greep op de "omgeving" waarin de controleprogrammatuur wordt verwerkt.

Men bedenke, dat de onder 2 genoemde procedure tot grote weerstand bij de gecontroleerde kan leiden.
Deze weerstand zal hoofdzakelijk betrekking hebben op de verlaging van de bezetting van de computer gedurende de tijd, dat de accountant van het systeem gebruik maakt.

Ingeval de computerverwerking van de controleprogrammatuur van de accountant niet bij de gecontroleerde maar elders plaatsvindt, dient de accountant de geheimhouding van de onderhavige gegevens te waarborgen. Dit geldt in het bijzonder bij de conversie van de bestanden en bij de verwerking op de computer van een servicebureau.
Een lid van de staf van de accountant dient in dit geval zowel de conversie als de verwerking bij te wonen.

6. Maatregelen ter verhoging van de betrouwbaarheid van de controle

Het is van het grootste belang maatregelen te nemen, waardoor de betrouwbaarheid van de gegevensverwerking - in het bijzonder bij gebruik van de computer van de gecontroleerde - kan worden verhoogd. Aan een aantal bedreigende factoren is hiervoor reeds aandacht besteed.

Men diene zich te realiseren, dat het bij de huidige geavanceerde computersystemen met de daarbij behorende besturingsprogrammatuur en andere "harde" software niet uitgesloten moet worden geacht, dat:

- in (controle)programmatuur tijdens het inlezen en tijdens de verwerking wijzigingen worden aangebracht, respectievelijk de programmatuur wordt gekopieerd;
- geselecteerde informatie onvolledig, respectievelijk gewijzigd wordt afgedrukt;
- geselecteerde informatie nogmaals wordt afgedrukt;
- opgebouwde bestanden ongeoorloofd worden gelezen of overschreven.

In interdisciplinaire researchgroepen wordt onderzocht op welke wijze het besturingssysteem van de computer, spooling software en dergelijke de (ver)werking van programmatuur kan beïnvloeden en welke informatie door de computer op dit punt beschikbaar wordt gesteld.

De maatregelen die kunnen worden getroffen zijn:

1. Het bijwonen van de verwerking van de controleprogrammatuur door de accountant.
   Doelstelling van het bijwonen van de verwerking is onder meer vast te stellen dat:

   - programmatuur, besturingsinformatie (JCL) en gegevens volgens de daartoe geldende regels aan het computercentrum ter verwerking worden aangeboden;
   - de verwerking geschiedt volgens de voorschriften en aan de hand van bij operating beschikbare documentatie;
   - alle communicatie tussen computer en operator wordt vastgelegd (bijvoorbeeld op het consoleverslag);
   - andere operationele programmatuur, respectievelijk testprogrammatuur de verwerking van de controleprogrammatuur en de integriteit van de gegevensverzamelingen niet beïnvloedt;
   - besturingsinformatie niet tijdens de verwerking van de controleprogrammatuur wordt gewijzigd;
   - geen informatiedragers worden verwijderd van het centrum, waarop tussen- en/of definitieve bestanden zijn geschreven ten behoeve van de accountant in het kader van de verwerking met de controleprogrammatuur.

   Bovenal is van betekenis, dat ingeval de accountant de verwerking van controleprogrammatuur bijwoont, hij waarborgen schept met betrekking tot zijn onafhankelijkheid.

Daarnaast betekent het tevens, dat de accountant zich enerzijds een oordeel kan vormen over de wijze waarop de organisatie van de computerafdeling (de produktiefunctie) is opgezet, waarin begrepen de maatregelen van interne controle en beveiliging.
Anderzijds verschaft het bijwonen van de verwerking de accountant inzicht in de werking van die organisatie. Een oordeel over de opzet en de werking van de organisatie kan voor de accountant van betekenis zijn bij het opstellen van zijn controleplan.

2. Het direct na elkaar afdrukken van het gebruikte programma (met een voor deze run unieke naam) en de met dat programma vervaardigde uitvoer. Ook bij gebruik van spooling-programmatuur biedt dit de zekerheid, dat de uitvoer daadwerkelijk met behulp van het daarvoor afgedrukte programma is vervaardigd.
Indien de accountant de verwerking niet bijwoont, dient de instructie voor de nabewerking van computeruitvoer te luiden: "niet scheuren".

3. Het opbouwen van totalen, waarmee kan worden vastgesteld, dat het totaal van de onderzochte gegevensverzameling identiek is aan dat van het bestand, dat door de gecontroleerde wordt gebruikt.
Door weergave van dit totaal aan het einde van de run via console kan tevens worden vastgesteld, dat de juiste uitvoer is ontvangen.

4. Het onmiddellijk ná de computerverwerking in (laten) nemen van:

   - de programma-afdruk
   - de uitvoer
   - de afdruk van de besturingsinformatie
   - een kopie van het consoleverslag

   ter controle.

   Vervolgens dient zo mogelijk vastgesteld te worden, dat:

   - de programma-afdruk correct is (is het juiste startgetal en interval gebruikt in de steekproefroutine en dergelijke);
   - de juiste versie van het betreffende bestand is gebruikt (afdruk besturingsinformatie);
   - de omgeving waarin de controleprogrammatuur is verwerkt geen invloed op die verwerking heeft gehad.

   Opgemerkt wordt, dat aan de controle van het consoleverslag een beperkte betekenis moet worden toegekend, zolang niet vaststaat welke informatie niet wordt afgedrukt, omdat dit bij systeemgeneratie is bepaald.
   Bovendien moet eerlijkheidshalve worden vermeld, dat een consoleverslag moeilijk leesbaar is. Slechts weinigen zullen in staat zijn voor de controle relevante informatie uit het verslag op te pikken,

   Het is van belang de controle zo snel mogelijk na het beschikbaar komen van de uitvoer aan te vangen.

7. Bewaren van programmatuur

Ingeval de accountant gebruik maakt van portable audit packages heeft hij veelal geen keuze met betrekking tot de bewaring van de programmatuur.
In de desbetreffende contracten is veelal een clausule opgenomen, dat de programmatuur slechts onder berusting van de accountant mag blijven.
Dit betekent, dat de accountant de informatiedrager met programmatuur zelf dient te bewaren en dat hij ná verwerking van de controleprogrammatuur ervoor zorg dient te dragen, dat geen (delen van de) programmatuur in de computer, respectievelijk op externe geheugens achterblijft.
Bij het audit package Auditape wordt daarom een routine gebruikt waarmee de gebruikte programmatuur en de aangemaakte bestanden niet bereikbaar worden gemaakt voor verdere verwerking.

Wanneer de accountant gebruik maakt van standaardpakketten, die in principe zijn ontwikkeld voor information retrieval doeleinden, zal het pakket ter beschikking staan van vele gebruikers en derhalve op het computercentrum beschikbaar moeten zijn.
De door de accountant geschreven toepassingen die met behulp van een dergelijk pakket worden uitgevoerd, kunnen óf in de programmabibliotheek, óf in een bibliotheeksysteem worden opgenomen, respectievelijk door de accountant zelf worden bewaard.

Het bewaren van controleprogrammatuur op de programmabibliotheek is uit controle-overwegingen slechts toegestaan indien op enigerlei wijze kan worden vastgesteld, dat de controleprogrammatuur ongewijzigd is gebleven.

Bij het bewaren van controleprogrammatuur op een bibliotheeksysteem kan gebruik worden gemaakt van de mogelijkheden tot beveiliging die door een dergelijk systeem worden geboden, zoals passwords, een automatische versienummering, een beveiliging tegen het aanbrengen van (ongeautoriseerde) wijzigingen in programma's, de onmogelijkheid operationele programmatuur te kopiëren, respectievelijk programmatuur operationeel te verklaren.

NOODZAAK TOT AANWEZIGHEID VAN DE ACCOUNTANT IN HET COMPUTERCENTRUM

door H.J.M. van der Wielen

Op verzoek van de redactie van Compact heeft Van der Wielen zijn gedachten met betrekking tot de aanwezigheid van de accountant en/of leden van zijn staf in verband met controlewerkzaamheden in het computercentrum in het onderstaande stuk vastgelegd. Deze notitie is als volgt ingedeeld:

1. Omschrijving van enkele begrippen
2. Eigen controleprogramma's van de externe accountant
3. Beoordeling opzet en bestaan van de organisatie, in het bijzonder van het systeem van interne controle en beveiliging (statische waarneming)
4. Beoordeling werkzaamheden van de interne controleurs
5. Periodiek onderzoek naar de goede werking van het systeem van interne controle en beveiliging (dynamische waarneming)
6. Periodiek onderzoek naar de goede werking van het systeem van interne controle en beveiliging bij het verwerken van bepaalde toepassingen
7. Aanbevelingen en conclusie

1. Omschrijving van enkele begrippen

Computercentrum : Met het computercentrum is in dit geval zowel bedoeld het verwerkingscentrum als de groep (systeemontwerpers enz.) die de voorbereiding van de projecten verzorgt, respectievelijk de specialisten, welke de harde software ontwikkelen en onderhouden.

Interne controle :
- Interne controle is alle controle ten behoeve van de leiding van een huishouding (nader uitgewerkt in blz. 64 t/m 68 van de Bedrijfseconomische Encyclopedie).
- De technische interne controle op de informatie, of wel kortweg controle op de vorm, is voor verantwoording van het computercentrum.
- De inhoudelijke interne controle op de informatie, of wel kortweg controle op de inhoud, is voor verantwoording van de verantwoordelijke gebruiker, evenals de presentatie van de output.

Externe controle : Onder externe controle wordt verstaan de controle die wordt uitgeoefend door en ten behoeve van anderen dan de leiding.

Intern controleur: Staffunctionaris onder het hoofd van het verwerkingscentrum respectievelijk onder de leiding van de automatisering, met als opdracht controlewerkzaamheden ten behoeve van de leiding te verrichten.

2. Eigen controleprogramma's van de externe accountant

Voorwaarde voor het goed functioneren van de externe controle is, dat de door de accountant nodig geachte controlemaatregelen, resulterend in het "werkprogramma", alleen door hem worden bepaald. Genoemde maatregelen worden als regel niet aan de gecontroleerde bekendgemaakt, om te voorkomen, dat hij zich hierop zou kunnen instellen.
De accountant kan besluiten om - voor een deel van de controlehandelingen - gebruik te maken van de computer. Zijn werkprogramma zal dan gedeeltelijk bestaan uit een computerprogramma.

Gegeven het hiervoor geformuleerde uitgangspunt zal de accountant dan ook:

- het betreffende computerprogramma in eigen beheer (laten) maken en testen, hierbij rekening houdend met de bestaande automatiserings- en acceptatieprocedures en documentatievoorschriften;
- na gereedkomen van het controleprogramma ook dit deel van het werkprogramma niet aan de cliënt in handen geven;
- de uitkomsten van het controleprogramma direct na verwerking door de computer zelf in beslag nemen;
- het verwerkingsverslag bij de uitkomsten betrekken om te constateren, dat een ongestoorde verwerking is geschied.

Deze activiteiten kunnen het meest eenvoudig worden gerealiseerd wanneer de accountant beschikt over eigen programmeurs en een eigen computercentrum. Bij verwerking in het eigen centrum is het "gevaar" van het ter kennis komen van de cliënt van de uitkomsten van deze controle-arbeid het geringst. Binnen het raam van de technische mogelijkheden zal de voorkeur van de accountant derhalve duidelijk uitgaan naar de verwerking in het eigen computercentrum.

Verwerking in het centrum van de cliënt is eveneens een mogelijkheid, zij het dat dan de volgende voorwaarden vervuld moeten zijn:

- De organisatie van het centrum zal aan de daaraan te stellen eisen van interne controle moeten voldoen.
- De accountant moet de mogelijkheid hebben de organisatie van het centrum waar te nemen en te beoordelen.
- De uitkomsten van het controleprogramma, alsmede het consoleverslag dat op de verwerking van het controleprogramma betrekking heeft, dienen onmiddellijk ter beschikking van de accountant te worden gesteld.
- Tijdens de verwerking moet de computer ter beschikking van de accountant staan, die tevens zijn eigen operating system zal gebruiken.
- Het controleprogramma mag niet ter beschikking komen van de cliënt, dit wil zeggen de accountant dient te verhinderen, dat het programma door de cliënt nadat de accountant het centrum heeft verlaten over het programma kan beschikken.

Indien het niet mogelijk is de computer geheel ter beschikking te stellen en/of dit uit kostenoogpunt niet wenselijk is, dient gebruik gemaakt te worden van de harde software van de cliënt. De accountant zal zich hierbij dienen te realiseren, dat de geheimhouding van de verwerking in handen van de cliënt kunnen raken.
Ingrepen kunnen in de programmatuur in een eerder stadium dan de feitelijke verwerking van het controleprogramma plaatsvinden.
Het is niet bekend in hoeverre technische mogelijkheden aanwezig zijn om al deze zogenaamde "vensters" in de door de cliënt vervaardigde software of in de door de leverancier geleverde standaardsoftware zijn aangebracht, te onderkennen.
Vooral bij multiprogrammeringssituaties en online-toepassingen in en buiten het centrum kan een opzettelijke ingreep door een systeemprogrammeur niet geheel worden voorkomen.

Aansluitend zal de accountant, na bestudering van de programmatische beveiligingen in het operating system en andere relevante software hierop inspelen in zijn eigen programmatuur, ten einde de hiervoor genoemde risico's zoveel mogelijk te trachten uit te sluiten.
Een erg belangrijk hulpmiddel hierbij kan de beoordeling van de uitkomsten van een verantwoord accounting systeem zijn, aangevende een chronologische registratie van de verwerking van systemen, de tijdsduur en hun doorbelasting.

Wat betekent het voorgaande nu voor de accountant die staat voor het vraagstuk van een "waterdichte" controle van de jaarrekening.
Het probleem van iedere (individuele) accountant, die een bepaalde jaarrekening onderzoekt, is altijd de afweging tussen:

1. het ontlenen van zekerheid aan de organisatie;
2. zelf verifiëren.

Een administratie, waarbij geautomatiseerde gegevensverwerking plaatsvindt, verandert het probleem voor de accountant niet. Probleem blijft de bedoelde afweging (die uiteraard in zijn uitwerking mogelijk wel beïnvloed zal worden door het computergebruik).

Stel dat het controleprogramma van de accountant door de afdeling systeemontwerp en programmering van de cliënt zou worden ontwikkeld omdat deze procedure minder kosten met zich brengt, alsmede dat effectiever gebruikt gemaakt kan worden van het bestaande standaardbesturingssysteem.
Daarmede is het controleprogramma qua methodiek aan de cliënt bekend, behoudens de keuze van de accountant van de te onderzoeken posten, perioden en cijferreeksen.
Voorwaarde is echter, dat het programma geheel is getest op juistheid en volledigheid (bijvoorbeeld door het gebruik van proefgevallen en Combi). Het tenslotte goedgekeurde programma - vastgelegd op een tape of disk onder beheer van de accountant - mag niet aan de cliënt in handen worden gegeven.

Terugkerend naar de problematiek ter zake van het verwerken van controleprogrammatuur onder besturing van het besturingssysteem van de cliënt zal het gezien het voorgaande duidelijk zijn, dat de accountant de verwerking van zijn programma's moet bijwonen om het risico dat zijn controleprogramma en de uitkomsten hiervan bij de cliënt bekend worden zo klein mogelijk te maken.

In sommige gevallen zal de accountant geen enkel risico mogen aanvaarden; de verwerking van het controleprogramma zal dan niet op de computer van de cliënt mogen plaatsvinden.

3. Beoordeling opzet en bestaan van de organisatie, in het bijzonder van het systeem van interne controle en beveiliging (statische waarneming)

a. De maatregelen ter beoordeling van de automatiseringsorganisatie binnen het computercentrum omvatten de volgende sectoren:

1. De automatiserings- en acceptatieprocedure
2. De functiescheiding en procedures binnen het centrum
3. De gegevensverzamelingen binnen het centrum
4. De gegevensverwerking binnen het centrum.

b. De accountant kan niet volstaan met de beoordeling van achter zijn bureau, maar zal het bestaan in de praktijk, ook in geval er geen sprake is van geautomatiseerde controleprogramma's van de accountant, moeten waarnemen.

c. Om richting te geven aan de werkzaamheden is het van belang een inventarisatie te maken van de elementen van de administratieve organisatie. Hiervoor een schema op te zetten in overleg met de cliënt en diens interne controleur.

4. Beoordeling van de werkzaamheden van de interne controleurs

Het adequaat fungeren van een intern controleur betekent een versterking van de interne controle.
In hoeverre de accountant van diens waarnemingen en bevindingen gebruik kan maken, kan eerst bepaald worden na kennisneming van diens instructies en werkplan.
De accountant zal in een aantal gevallen over de schouder van de intern controleur moeten meekijken.

5. Periodiek onderzoek naar de goede werking van het systeem van interne controle en beveiliging (dynamische waarneming)

Kortheidshalve kan verwezen worden naar het vermelde onder punt 3a en 3b. De frequentie en diepgang van het onderzoek zijn afhankelijk van het computercentrum en de aard (typering) van de geautomatiseerde systemen. In een aantal gevallen zal de goede werking van de organisatie af te lezen zijn uit de controle op de output van de systemen.

6. Periodiek onderzoek naar de goede werking van het systeem van interne controle en beveiliging bij het verwerken van bepaalde toepassingen

Afhankelijk van het belang van de uitkomsten van een systeem voor de jaarrekening van de cliënt respectievelijk om andere redenen is het soms noodzakelijk dat de accountant tijdens het verwerkingsproces vaststelt, dat de output is vervaardigd door het verwerkingscentrum onder de condities zoals in de voorschriften of andere regelen is aangegeven. Bedoeld bijwonen op zich zelf beschouwd geeft geen garantie dat de uitvoer zonder meer aanvaard mag worden; wel kan het betekenen, dat de accountant (respectievelijk de interne controle) een aantal controlehandelingen nu niet meer behoeft te doen.
Dat dit bijwonen alleen in overleg met de gebruiker van de informatie, alsmede met het hoofd van de verwerkingsafdeling mag plaatsvinden, is duidelijk. Ook het verwerkingscentrum moet de interne controle- en beveiligingsaspecten in aanmerking nemen en zich eraan houden. Dat zal onder meer betekenen, dat alleen personen met autorisatie van bevoegde instanties van de cliënt en diens accountant de verwerkingszaal mogen betreden.

7. Aanbevelingen en conclusies

a. Naar mijn mening kan op den duur aan de vraag naar steeds vroegtijdiger oplevering van de jaarstukken en de daarbij behorende accountantsverklaring slechts worden voldaan door dynamisering en automatisering van zoveel mogelijke controlehandelingen, zelfs als dat duurder zou zijn dan handwerk.
De voordelen van eerder beschikbaar gekomen informatie ter bijsturing door de leiding zullen groter dienen te zijn dan de extra computerkosten.

b. Ter beperking van het aantal uren, dat de accountant in de computerzaal aanwezig zou dienen te zijn, is het raadzaam te overwegen aan het controleprogramma van de accountant de hoogste prioriteit te geven; als voorwaarde hiertoe zou uiteraard gesteld dienen te worden, dat het accountantsprogramma zodanig is opgesteld, getest en goedgekeurd, dat een minimum aan oponthoud respectievelijk capaciteitsbeslag wordt veroorzaakt.

c. Centraal staat de uitspraak, dat de leiding de eerste verantwoordelijke is die bepaalt hoe het stelsel van interne controle zal worden opgebouwd, respectievelijk welke maatregelen van beveiliging dienen te worden genomen.
De accountant moet alleen als eis stellen, dat de gekozen oplossing tot controleerbare resultaten zal leiden en indien dit - onverhoopt - niet optimaal het geval zou zijn, dat de accountant van de aangetroffen leemten het effect kan kwantificeren en de zwakke plekken door aanvullende controlewerkzaamheden kan overbruggen.

"DATA BASE EN ACCOUNTANT"

een bespreking door C.J.E. Lankreijer

Algemeen

Begin 1977 is bij Samsom het boekje "Data base en accountant" verschenen. Dit boekje is het rapport van een werkgroep, welke op initiatief van vier accountantskantoren en de Erasmus Universiteit gevormd was.
De opdracht van de werkgroep was: "het onderzoeken van de toepassing van data bases, voor zover van belang in het kader van de accountantscontrole".

Van de werkgroep hebben deel uitgemaakt:

- J.H. Balvert (Pelser, Hamelberg, Van Til & Co)
- K. Gerritse en Th.B. Strasser (ged.) (Moret & Limperg)
- H. Roos en K. van Tilburg (Klynveld Kraayenhof & Co; Erasmus Universiteit)
- J. de Vos (Van Dien + Co)
- P.J.C. Warners (ged.) (Interne Accountantsdienst Rijksuniversiteit Leiden).

Het rapport is geschreven voor accountants met enige kennis op automatiseringsgebied en werkzaam in de algemene controlerende functie.
Door publikatie van het rapport is gebruik voor opleidingsdoeleinden mogelijk gemaakt.

Een van de voornaamste conclusies uit het rapport is, dat de materie dermate complex is, dat in de nabije toekomst beveiliging van data bases en beoordeling van de interne controle in data base systemen specialistenwerk zal zijn. Dit is een conclusie waarmee men zich na lezing van het rapport ongetwijfeld zal kunnen verenigen.
Maar laat dit geen reden zijn om het rapport ongelezen te laten. Met name de hoofdstukken 1 (Introductie tot de data base) en 2 (Organisatorische aspecten van de data base) zijn ook voor de niet-specialist duidelijk; zij lijken mij een goed inzicht te geven in de principes van de data base en de organisatorische consequenties hiervan, gezien in het licht van de interne controle.
(Ik moet mij op dit punt wat voorzichtig uitdrukken, omdat het mij door het ontbreken van elke ervaring met data bases niet mogelijk is het rapport aan de werkelijkheid te toetsen.)
Met hoofdstuk 3 (Beveiliging van gegevens in een data base toepassing) had ik wat meer moeite, vooral met het gedeelte over "autorisatie". Maar hier bevinden wij ons dan ook op een terrein waar de algemene accountant niet zonder de hulp van zijn gespecialiseerde collega zal kunnen.
In hoofdstuk 4 (Data base en standaard-controleprogrammatuur) wordt kort een aantal mogelijke oplossingen geschetst voor problemen die samenhangen met data base en standaard-controleprogramma's. Aan de geschetste oplossingen blijken echter ook nog grote bezwaren te kleven. En wel zodanig, dat ik geneigd ben te concluderen, dat (nog) geen van de oplossingen praktisch uitvoerbaar is.
Als ik het goed begrepen heb, lijkt het mij thans voor een externe accountant bij een voor de jaarrekening van belang zijnde data base toepassing alleen mogelijk tot een goedkeurende verklaring en een betaalbare declaratie te komen, als er effectief kan worden samengewerkt met een interne

accountant. Deze interne accountant zal dan veel specifieke kennis omtrent de betreffende data base toepassing moeten hebben. Of deze conclusie juist is blijkt niet uit het rapport, maar mogelijk kan iemand die wel praktijkervaring met data bases heeft zijn visie eens geven.
De vraag die mij bij het lezen van het rapport steeds meer ging intrigeren is: Hoe bij een belangrijke data base toepassing, in de praktijk, de accountantscontrole is opgezet en uitgevoerd, zodat aan de eis van een "deugdelijke grondslag voor de verklaring" is voldaan.
In dit verband is het jammer, dat blijkens het voorwoord één van de oorspronkelijke deelopdrachten van de werkgroep onder meer wegens tijdgebrek moest vervallen; namelijk het toetsen van de uitwerking van de consequenties van de data base op de interne controle en beveiliging aan de feitelijke situatie in Nederland.

Graag wil ik dit rapport ter lezing aanbevelen aan een ieder die te maken heeft met accountantscontrole en/of interne controle bij geavanceerde geautomatiseerde systemen. Dit is een mogelijkheid om met weinig moeite (er is geen specialistische kennis nodig) en weinig tijd (het rapport is vlot leesbaar en bevat slechts 94 pagina's) een indruk te krijgen van het verschijnsel "data base" en de consequenties hiervan voor de controle.
In de A.C.-bibliotheek is een aantal exemplaren van dit boekje opgenomen, terwijl tevens aan alle kantoren een exemplaar is toegezonden. Het boekje is ook in de handel verkrijgbaar (Samsom).

Overzicht van de inhoud van het rapport

Hier wil ik de onderwerpen die in de hoofdstukken aan de orde komen wat nader aanduiden.

1. Introductie tot de data base

   In dit hoofdstuk wordt getracht de accountant met enige automatiseringskennis, vertrouwd te maken met het verschijnsel "data base" en de daarmee samenhangende terminologie.
   Uitgaande van een aantal problemen, die met behulp van conventionele bestandsvormen niet kunnen worden opgelost, beschrijven de samenstellers van het rapport de wezenlijke kenmerken van een data base.
   Hierbij komen aan de orde:

   - De logische en fysieke gegevensstructuur binnen een data base.
   - Verschillende soorten gegevensstructuren (sequentiële structuur, boomstructuur, netwerkstructuur).
   - Een techniek om de gegevensstructuur vast te leggen (data structuur diagram).
   - Het op voor de computer bruikbare wijze beschrijven van gegevensstructuren in schema's en subschema's.
   - De werkwijze van een data base met behulp van het data base management systeem (DBMS).

In bijlage 1 wordt een eenvoudig voorbeeld van een data base uitgewerkt.
In bijlage 2 wordt enige informatie gegeven over de Data Base Task Group van de CODASYL.

2. Organisatorische aspecten van de data base

Hier wordt ingegaan op de consequenties van de komst van de data base voor de organisatie op korte termijn.
Hierbij wordt onder andere aandacht besteed aan:

- de aanpak van een data base project
- de data dictionary (centrale bibliotheek van gegevensdefinities)
- de taak van de accountant bij het realiseren van een data base
- de data base administration functie
- de netwerkbesturingsfunctie, welke veelal door de master terminal operator wordt uitgeoefend.

3. Beveiliging van gegevens in een data base toepassing

Hier worden achtereenvolgens de volgende interne controledoelstellingen behandeld in het kader van een data base:

- beperking van het beschikken over informatie tot diegenen die daartoe bevoegd zijn (autorisatie, inclusief audit trail)
- waarborgen van tijdige, juiste en volledige verwerking van informatie
- waarborgen van de juistheid, volledigheid en van het permanent beschikbaar blijven van informatie in bestanden en van de beschikbaarheid van het informatieverwerkingssysteem gedurende de tijd dat dit noodzakelijk is (beveiliging, inclusief recovery).

4. Data base en standaard-controleprogrammatuur

In dit hoofdstuk wordt geprobeerd de invloed vast te stellen van de data base op de bestaande standaard-controleprogrammatuur en wordt aandacht besteed aan de mogelijke oplossingen voor de door de data base op dit vlak veroorzaakte problemen.

Tenslotte zijn een Literatuuroverzicht en een Index van trefwoorden aan het rapport toegevoegd.

NASCHRIFT op de bespreking door H. Roos

Op enkele punten (genoemd op blz.17 en blz.18) uit de bespreking van het rapport door Lankreijer wil ik nader ingaan.

Ten eerste zijn conclusie: "dat onder bepaalde omstandigheden effectieve samenwerking met een interne accountant nodig is". Hij denkt daarbij aan een situatie waarin de onderneming, waarop de te certificeren financiële verantwoording betrekking heeft, gebruik maakt van een data base

toepassing. Die data base toepassing is voorts van zodanig grote importantie binnen het gehele administratieve systeem, dat de controlerend accountant er niet omheen kan. Lankreijer stelt dan, dat het in een dergelijke situatie uit kostenoverwegingen noodzakelijk is om tot een effectieve samenwerking te komen met de binnen die onderneming fungerende interne accountant.
Hij noemt het woord kostenoverwegingen niet, doch spreekt over een betaalbare declaratie. Ik meen echter, dat dit geen reële benadering is.

Het gaat in wezen om de totale controlekosten en niet alleen om de declaratie van de externe accountant. Wel is het natuurlijk zo, en daar doelt Lankreijer waarschijnlijk op, dat een verhoging van de declaratie niet altijd in dank wordt afgenomen. Een effectieve samenwerking met de interne accountant is natuurlijk altijd wenselijk. Daar doet het al dan niet in het spel zijn van een data base niet aan af.
Wat dan wel? Wanneer er bij de uitvoering van het controleplan doorgedrongen moet worden in de data base, is het een kwestie van doelmatigheid wie van beiden de betreffende actie neemt. Een belangrijke factor daarbij is wie de noodzakelijke specialistische en technische kennis ter beschikking heeft.

Zowel de interne als de externe accountant zullen het systeem, waar de data base deel van uitmaakt, zodanig moeten kennen, dat zij in staat zijn om zich een oordeel te vormen over de kwaliteit van de interne controle in en rond het systeem. Tenminste één van beiden moet in staat zijn om de werking van die interne controle te toetsen. De ander moet in staat zijn om de effectiviteit en de uitkomst, alsmede de omstandigheden waaronder die test is uitgevoerd, te beoordelen.

Vervolgens moet op basis van de evaluatie van systeem en uitgevoerde tests worden besloten, of het noodzakelijk is zelfstandig gegevens uit de data base te lezen en - na selectie - voor verdere controle af te drukken. Uit hoofdstuk 4 is af te leiden, dat bij de huidige stand van zaken de enig realiseerbare oplossing is het zelf schrijven van een programma; in de meeste gevallen zal normaal van COBOL gebruik gemaakt kunnen worden. Dat is niets nieuws. Ook thans werken wij (binnen de A.C.) in vele gevallen met "maat"-COBOL-programma's in plaats van een audit package zoals Auditape of CA-EARL (IS08).

Kenmerkend voor audit-programma's is, dat het bestand vrijwel altijd volledig moet worden doorgelopen om zeker te zijn, dat de inhoud van de relevante financiële velden in totaal overeenstemt met een van tevoren bekend totaal. Dit doorlopen zal steeds geschieden in fysieke sequentiële volgorde. De data base "calls", die hiervoor nodig zijn, en vooral de volgorde van die calls zijn bij sequentiële verwerking betrekkelijk eenvoudig.

Uit hoofdstuk 1 blijkt, dat de verbinding tussen programma en DBMS wordt gevormd door een subschema (althans bij CODASYL-georiënteerde DBMS; bij IMS wordt die functie bijvoorbeeld vervuld door het Program Specification Block).

Dit subschema moet beschikbaar worden gesteld door de Data Base Administrator en zal in samenwerking met de DBA worden ontworpen. In dat subschema zal worden aangegeven, dat het controleprogramma alleen mag lezen. Gevaar voor verminking van de data base is daardoor nauwelijks aanwezig.

Er kan zich evenwel een complicatie voordoen wanneer de betreffende data base een onderdeel vormt van een real time toepassing. Het zal dan om verschillende redenen zoals concurrency en responsetijden niet aanvaardbaar zijn om het controleprogramma uit te voeren naast het real time systeem op dezelfde versie van de data base.

Het voert te ver om in dit naschrift alle mogelijkheden systematisch uit te werken. De bedoeling was om duidelijk te maken dat er in elk geval zowel bij de intern als bij de extern accountant een behoorlijke kennis aanwezig moet zijn. De taakverdeling ten aanzien van de uitvoering van tests en van het maken en uitvoeren van een controleprogramma is afhankelijk van de concrete mogelijkheden.
In elk geval is samenwerking met de DBA noodzakelijk.

A. B. C. - N I E U W S

door A.W. Neisingh

Case ICI

Zoals U ongetwijfeld in de dagbladen heeft gelezen, heeft een personeelslid van ICI geprobeerd het bedrijf ruim 1¼ miljoen gulden af te persen door diefstal van magneetbanden en computerschijven met voor het bedrijf belangrijke gegevens.

Wat leert deze computer abuse ons?

Zoals bekend, dient ernaar te worden gestreefd binnen de automatiseringsorganisatie afzonderlijke functionarissen van voldoende niveau te belasten met:

a. systeemontwikkeling en toepassingsprogrammering
b. systeemprogrammering
c. computerverwerking.

In de afdeling computerverwerking dienen zo mogelijk de volgende functies te bestaan:

1. werkvoorbereiding
2. gegevensvastlegging
3. bediening van de computer
4. in- en uitvoerbehandeling
5. bewaring van informatiedragers.

Bij ICI heeft blijkens de krantenberichten onvoldoende functiescheiding bestaan tussen werkvoorbereiding, bediening van de computer (shift leading) en de bewaring van informatiedragers.
De betrokken functionaris heeft daarbij "geprofiteerd" van de omstandigheid, dat - in het kader van een beveiligingsplan - geen extra maatregelen van beveiliging waren getroffen met betrekking tot de toegang tot de kopieën van belangrijke informatiedragers, voorgaande generaties en dergelijke. (Inmiddels heeft ICI de procedure aangepast door voor te schrijven, dat twee handtekeningen nodig zijn om toegang te krijgen tot de opslagruimte van informatiedragers.)

In het op de volgende pagina opgenomen schema is aangegeven welke mogelijke risico's bij geautomatiseerde gegevensverwerking worden gelopen ter zake van:

- oneigenlijk gebruik van de computer,
- manipulatie met gegevens, alsmede
- moedwillige vernieling, diefstal en dergelijke.

Getracht is de mogelijke schade voor het bedrijf aan te geven met daarbij de preventieve maatregelen, waardoor de risico's kunnen worden beperkt of teniet gedaan. Bij de controlemiddelen wordt slechts puntsgewijze genoemd welke middelen bruikbaar zijn.

In het kader van een opdracht wordt een controleprogramma ten behoeve van de in de automatiseringsorganisatie opgenomen Intern Controleur opgesteld. Het spreekt vanzelf, dat hierin - rekening houdende met de specifieke situatie - een zo optimaal mogelijk gebruik van de controlemiddelen wordt uitgewerkt.

Computermisbruik	Schade voor het bedrijf	Preventieve maatregelen	Controlemiddelen
1. Gebruik computer door personeel voor eigen, c.q. malafide doeleinden			
a. verwerken eigen programma's	. daaraan verbonden kosten . toegenomen kansen op storingen in apparatuur ("spelen")	. procedures m.b.t. planning en werkvoorbereiding, voortgangscontrole . catalogued jobstreams . twee operators per shift . speciale beveiliging van geheime en gevoelige data . research en ontwikkeling op vastgestelde tijden . procedures m.b.t. uitgifte van bestanden . afhaalsysteem voor output . datacommunicatiesystemen beveiligen met toegangscontrole . functiescheiding óók buiten normale werktijden . antecedentenonderzoek	. job accounting . console log . listen programmabibliotheek . outputcontrole, ook op testwerk . beoordelen console en accounting . beoordelen herstarts door inleveren van foutieve output
b. gebruik aanwezige programmatuur voor eigen doeleinden	. daaraan verbonden kosten . afdrukken van (eventueel geheime) bedrijfsgegevens		
c. verwerken eigen programma's om bedrijfsgegevens t.b.v. derden af te drukken (bedrijfsspionage)	. daaraan verbonden kosten . aantasting privacy . concurrentie-vervalsing . andere vormen van schade door bekend worden van niet voor derden bestemde gegevens		
2. Manipulaties met gegevens, O.S. en programma's	. fraude . niet meer juist functioneren van de programmatuur . verstrekken van onjuiste gegevens . werken met verminkte bestanden (bijv. data base)	. antecedentenonderzoek . altijd twee operators in computercentrum . geen systeem- en programmadocumentatie onder bereik van operating . bewaring gescheiden van operating . kopieën aanhouden	. scheduling . file-controlemethodieken . periodieke programmatests; eventueel cross reference
3. Moedwillige vernieling, diefstal			
a. apparatuur	. materiële schade . stilstand informatieverwerking	. reconstructiemogelijkheden . bewaarder informatiedragers als aparte functie . uitwijkmogelijkheid . opberging bestanden . administratie . tijdens ontslagperiode niet meer op C.C. . betrouwbaarheid operators . toegangsbeveiliging . closed shop . alarm . beveiligen energietoevoer	. oogcontrole door leiding
b. informatiedragers	. materiële schade . verlies bestanden . verlies programmatuur		

Schending van de privacy-wetgeving (V.S.)

Three insurance firms named for illegally procuring records

The Northwestern Nationals Insurance Group of Milwaukee, the Home Insurance Group of New York and the Reliance Insurance Co., also of New York, are among the 56 insurance companies indicted in district court here for illegally obtaining individuals' personal records.

Charges included conspiracy to commit theft, criminal solicitation and receipt of stolen property, according to a spokesman for a district attorney.
The three firms are among those that hired Factual Service Bureau Inc., to obtain sensitive personal information from government, medical and credit card company data banks for use in settling insurance claims.
Factual was charged with conspiracy, impersonation and theft of trade secrets for illegally obtaining the records using only a telephone and a well-documented system of subterfuge, according to evidence presented to the grand jury.
In addition to facing criminal action, the three are among 110 insurance companies being investigated by the Colorado State Insurance Commissioner to see whether they also demonstrate "a pattern of unfair claims practices", according to Insurance Commissioner J. Richard Barnes.
If so, the firms could be fined a maximum of $ 50,000 or $ 10,000 per offense, as well as having their licenses revoked or suspended, Barnes said.
Criminal hearings are set in the state court here for February and a hearing before Barnes will follow, he said.
Rep. Barry Goldwater Jr. (R-Calif.) has met with representatives of the Federal Bureau of Investigation, the Justice Department and the Internal Revenue Service in an effort to initiate an investigation within those departments.
In addition to sidestepping security safeguards in federal data banks, hospital record rooms and physicians' offices, Factual also obtained secret credit card company telephone code numbers to obtain individuals' credit records for the insurance companies, according to a Goldwater aide.
As a result of his involvement in the investigation of the privacy violations allegedly committed by the insurance vendors and Factual Service Bureau, Goldwater has received numerous telephone and written reports of other similar violations from former employees of other insurance companies and investigative agencies, the aide said.

(Computer World, 8 november 1976)

Overheid erg slordig met kentekengegevens

Bij mijn bezoek aan het computercentrum van de Rijksdienst voor het Wegverkeer heb ik me gaandeweg steeds meer lopen te verbazen over het vrijwel ontbreken van een adequate beveiliging van apparatuur en informatie. Alhoewel er toch min of meer privacy-gevoelige gegevens (bijvoorbeeld betalingsgegevens) worden verwerkt, is de computerruimte voor iedereen, die kwaad wil, eenvoudig te bereiken. Gewoon door de hoofdingang, langs de uiterst vriendelijke portiers (die een paar stevige jongens echt niet tegen zullen kunnen houden) en dan door twee geopende deuren. Ook de computerruimte zelf: gewone ramen, die zeker niet tegen een steen bestand zijn. Den Haag heeft hier weinig geld voor over en weinig oog voor de beveiliging. Eigenlijk een totaal onbegrijpelijke zaak, te meer als men nog bedenkt, dat met behulp van het systeem in Veendam 24 uur per dag de politie van informatie moet worden voorzien. Er is in wezen een paradijs voor saboteurs gecreëerd. Een slordigheid, die vooral een overheid zich nooit mag permitteren. Zelfs niet om budgettaire redenen.

(Computable, hoofdredacteur A.A. van Eek)

Gebruik van de computer in de (accountants)controle

Vermeldden wij in de vorige uitgave van Compact een voorbeeld van het gebruik van de computer waarmee een fraude op het gebied van de sociale verzekering in de V.S. werd opgehelderd, deze keer iets geheel anders.

Using EDP to appraise EDP = $ 200,000 savings

In a company with annual sales of US $ 650,000,000, the auditor was faced with a difference of many millions of dollars between proceeds that would have been obtained if products had been sold at full-book prices and wat was actually reported in computer-produced financial and marketing reports. The only acceptable cause of the difference was quantity rebates. A total of 11 different but integrated systems linked to produce the final reports and effective evaluation involved appraisal of controls in each of the 11 systems.
With 400,000 sales transactions each month which were supported by a number of complex master files (the biggest holding extensive details of 380,000 customers sites and another 160,000 country freight differential items) sheer volume would have restricted activities in a non-EDP environment to the extent that any opinion finally given would have been highly subjective.
Because the systems were computerized, a very high level of appraisal was possible. By extensive use of Mark IV, every sales transaction for all major products for one month was looked at very objectively along with the data extracted by each from the master files. By progressive outsorting and structured reporting of nonstandard items, the source of erosion of every dollar was found along with the frequency and incidence and total cost of each erosion factor.
In achieving this, the integrity and reliability of key data processed and held in each system were effectively appraised. Recommendations were made for control changes which would eliminate proceeds' erosion of US $ 135,000 per annum with little increase in costs. In addition, retrospective calims were made on customs authorities for overpayments and underclaims in excess of US $ 65,000.
All auditors involved were highly enthusiastic about the different approach and stated that the techniques used fave them treatly enhanced job satisfactrion.

(The Internal Auditor)

Pansophic koppelt Easytrieve aan IBM's DL/1 data base bestanden

Pansophic heeft voor het pakket Easytrieve, waarmee door middel van parameters op eenvoudige wijze toegang kan worden verkregen tot opgeslagen gegevens, een koppeling ontwikkeld voor met behulp van DL/1 gecreëerde data base bestanden. Een gebruiker kan nu door middel van het opgeven van het DL/1 segment, sleutelvelden en het hiërarchienummer van de data base toegang krijgen tot de gegevens. Daarbij kan een selectiecriterium worden meegegeven, zodat alleen de gewenste records worden benaderd.

De nu ontwikkelde programmatuur bevat tevens routines voor het op alom toegankelijke wijze (random access) benaderen van bepaalde data base segmenten.

(Computable, 21 januari 1977)

Zoals bekend, is de benadering van data bases met behulp van audit software niet zonder meer mogelijk.
Pansophic heeft nu zodanige voorzieningen in het pakket Easytrieve aangebracht, dat DL/1 data base bestanden kunnen worden benaderd.

Cullinane ontwikkelt beheersysteem voor in data base en conventioneel vastgelegde gegevens

Cullinane Benelux heeft onlangs de zogenaamde Integrated Data Dictionary (afgekort IDD) aangekondigd. Dit pakket is bedoeld als hulpmiddel voor gebruikers van het eveneens door Cullilane geleverde data base systeem IDMS. Met behulp van de IDD-programmatuur kan alle met het computersysteem verwerkte en opgeslagen bedrijfsinformatie worden beheerd. Het systeem biedt onder meer mogelijkheden tot het verkrijgen van een overzicht van alle gegevens tijdens de overgangsfase van conventionele bestanden naar een centrale data base.
Met IDD kan worden gewerkt met behulp van de zogeheten Data Dictionary Definition Language. Het systeem heeft uiteraard een koppeling met IDMS en verder met vertaalprogrammatuur voor Cobol en PL/1. Tijdens de compilatie van in deze talen geschreven programma's worden automatisch de programma-effecten op de bestanden opgezocht, waardoor bijvoorbeeld kan worden nagegaan hoeveel programma's gebruik maken van bepaalde bestanden en records.
Met IDD krijgt een gebruiker de beschikking over 21 standaardrapporten, terwijl het aantal gebruikersrapporten ongelimiteerd is.

(Computable, 4 maart 1977).

ICL's software voor Swift goedgekeurd

De computerapparatuur en de daarmee samenhangende programmatuur, ontwikkeld door ICL om banken te verbinden met het internationale communicatienetwerk is goedgekeurd, nadat uitgebreide testen zijn uitgevoerd voor het direct verwerken van financiële transacties en berichten. De goedkeuring werd in begin december 1976 verleend. De goedkeuring is gegeven door de Society for World Interbank Financial Telecommunications (Swift). Dit is de niet op winst gerichte, onderlinge organisatie van banken over de hele wereld. Swift heeft tot taak een wereldomspannend, op computers gebaseerd netwerk te bouwen en te onderhouden, dat het financiële berichtenverkeer tussen banken verzorgt.
ICL is door Swift aangewezen als een van de voornaamste leveranciers van terminalsystemen, die door de aangesloten banken over de hele wereld zullen worden gebruikt. Het Swift Interface Device (SID) van ICL is ontwikkeld uit de krachtige 1500-serie transactieterminals, waarvan zo'n 5.000 systemen reeds zijn afgezet. Het eerste resultaat van de beslissing die Swift heeft genomen is, dat de vijftien banken, in België, Duitsland, Zwitserland en Engeland, die deze SID-terminals van ICL al hebben geïnstalleerd, nu kunnen gaan werken met het netwerk, zodra dit operationeel is. Berichten en bevestigingen over financiële transacties zullen met een grotere snelheid worden verzonden dan nu mogelijk is met de telexverbindingen die door vele banken worden onderhouden. De informatie zal bovendien veel beter beveiligd zijn en de transmissiekosten worden lager.
Gemakkelijke bediening is een voornaam uitgangspunt geweest bij de samenstelling van de programmatuur. Er is een serie programma's geschreven, waarmee de indeling van vele berichten gestandaardiseerd en duidelijk omschreven zijn. Hetzelfde geldt door de bewerking van de gegevens. De indeling van de financiële berichten wordt geprojecteerd op het beeldscherm, ten einde de operatrice te begeleiden bij de vastleggingswerkzaamheden. Door de hoge graad van standaardisatie is een betrouwbaar, accuraat en kostenverlagende methode voor het verzorgen van het berichtenverkeer verkregen. Het houdt tevens in, dat operators en operatrices binnen enkele uren kunnen leren hoe zij het systeem moeten bedienen. Zij hoeven over geen enkele computerkennis te beschikken. De programmatuur zorgt voor de controle op juistheid en legaliseert de berichten die op de terminal worden ingetoetst. Evenzo controleert het de berichten die worden ontvangen en dirigeert ze naar de gewenste uitvoereenheid. Het zorgt daarnaast voor de handhaving van de procedures die voor het systeem gelden en voegt berichten samen voor de directe verzending of het opslaan tot transmissie op een later tijdstip.

(De Automatiseringsgids, 24 maart 1977)

LITERATUUROVERZICHT

door R. Bron

In de A.C.-bibliotheek opgenomen boeken

AC 112 Informatie- en communicatiesystemen - IBM (126 blz.)

Een richting waarin het computergebruik zich ontwikkelt is, dat de gegevensverwerking op een dusdanige manier wordt geïntegreerd in de dagelijkse bedrijfsvoering, dat de systemen die daarvoor worden gebruikt tegelijkertijd een communicatietaak vervullen. Dit boekje beoogt een overzicht te geven van de diverse apparatuur en programmatuur die IBM daarvoor beschikbaar heeft. Daarnaast worden de samenhangende aspecten behandeld van door de IBM ontwikkelde procedures onder de naam "Systems Network Architecture".

AC 113 Programmatuurfacetten - IBM (ca. 100 blz.)

Dit boekje geeft een overzicht van de door IBM aangeboden programmaprodukten, alsmede een overzicht van het dienstenpakket van het IBM-servicebureau.

AC 115 HIPO, A design Aid and Documentation Technique - IBM

The purpose of this manual is to describe a design aid and documentation technique called Hierarchy plus Input-Process-Output (HIPO). Intended for systems analysts and programmers, the manual describes how to use HIPO as a design aid and documentation technique throughout the development cycle.

AC 117 Fysieke beveiliging rekencentra - NOVI

De stuurgroep "Beheer van rekencentra" van Studiecentrum NOVI, onder voorzitterschap van prof. R.W. Starreveld, heeft enkele jaren geleden een werkgroep ingesteld welke tot doel had een rapport op te stellen over de fysieke veiligheidsaspecten van rekencentra. Met het groter worden van de rekencentra en het duurder worden van apparatuur, programmatuur en mankracht werden de te nemen maatregelen tegen calamiteiten als brand, diefstal, sabotage, enz. steeds omvangrijker, onoverzichtelijker en dus kostbaarder.

De werkgroep "Fysieke beveiliging" geeft hierbij haar bevindingen over deze materie.
Altijd weer worden nieuwe pogingen gedaan, soms met succes, om het informatieverzorgende werk binnen de rekencentra te verstoren of de informatie ten eigen nutte te gebruiken. Beveiligingsmaatregelen - en dus ook dit rapport - zijn daarom nooit af. De werkgroep is zich daarvan bewust. Maar zij meent tevens, dat desondanks voor een ieder die met beveiliging van informatie, apparatuur, programmatuur en gebouwen heeft te maken, in dit rapport op systematische wijze een groot aantal wenken en aanwijzingen (onder andere door middel van vragenlijsten) te vinden zijn die hem bij zijn werkzaamheden kunnen helpen.

AC 118 Brandbeveiliging van gebouwen
NPR 3900 - Nederlands Normalisatie-instituut

Aangezien een groot aantal activiteiten in toenemende mate afhankelijk is van computers en van de daarmee verkregen gegevens, vraagt beveiliging daarvan tegen calamiteiten, met name brand, bijzondere aandacht.
In tegenstelling tot de tot op heden door het NNI uitgegeven normen inzake de brandbeveiliging van gebouwen, die vooral zijn opgesteld met het oog op de veiligheid van de in het gebouw aanwezige personen, en met het oog op het beperken van schade aan de belendingen en omringende bebouwing, is deze NPR uitsluitend opgesteld ter voorkoming en beperking van schade aan het gebouw en in het bijzonder aan zijn inhoud. In het bijzonder de betekenis die een computerinstallatie kan hebben voor de maatschappelijke orde rechtvaardigt het geven van desbetreffende richtlijnen. Het gaat immers niet alleen om de schade die door brand aan de computerinstallatie kan worden aangebracht, maar vooral om de bedrijfsschade die dientengevolge kan worden toegebracht aan de computergebruikers.

AC 119 The auditor's preliminary review of EDP accounting controls - The California Society of Certified Public Accountants (107 blz.)

Statement on Auditing Standards No. 3, entitled "The Auditor's Preliminary Review of EDP Accounting Controls", requires that, if a client uses EDP in a significant accounting application (whether simple or complex), the auditor should understand the application and assess its essential accounting control features. The purpose of this Computer Impact Series Report is to provide information that can assist auditors in interpreting the application of SAS-3 and in planning for and implementing a preliminary review of EDP accounting controls as part of an audit examination. The report is designed to be a state-of-the-art, "how-to" document, rather than one of a conceptual or standard setting nature. Readers are cautioned that merely reading this Computer Impact Series Report will not qualify them to perform a preliminary review.

AC 121 Guide for reliability assessment of controls in computerized systems (financial statment audits) - U.S. General Accounting Office 1976

This guide was prepared for use on GAO audits made for the preliminary purpose of expressing an opinion on financial statements. It is designed to guide the auditor through a survey of computerized accounting systems to help him understand the system operation, evaluate controls and assess the reliability of computer produced data. With this knowledge, the auditor should be able to make a more informed judgement about the extent of detailed audit tests needed to support an opinion on the statements.

AC 130 Internal audit of inventory control and management - Research Committee report nr. 16 - I.I.A.

The purpose of this study is to describe inventory management processes, emphasizing those areas where the internal auditor can be most constructive. Hopefully, the study will provide the auditor with perspective and serve as a pointer toward an in-depth study of inventory control and management. In keeping with this purpose, the study concludes with a broadly conceived audit program which is offered as a guide in preparing programs for specific needs.

AC 132 Computer data security - H. Katzan Jr.

This book convers the full spectrum of computer data security in modern computer and information systems, including both theoretical and practical aspects of the subject. It is designed to benefit everyone concerned with data security, from the manager to the computer expert.
The book includes an introduction to computer data security, a review of computer systems, computer software, data management and data communication, data security considerations in a computer environment, methodology for data security, applications of data security and a discussion of cryptographic techniques used in data security.
Among the many topics of special interest are: modern computer hardware; storage protection; virtual storage; input and output organization; computer languages; language processors; operating systems technology; terminal-oriented systems; data and storage structurs; data base technology; data security threat potential; data security countermeasures; theory of protection; access management; data file protection; processing limitations; applications of data security; and privacy transformations.
An up to date, authoritative, and comprehensive introduction to effective data security techniques, here is "must" reading for everyone concerned with the collection, storage, and use of information. Here, in fact, is a book whose theme cuts across all industries.

AC 134 Guidelines for automatic data processing, physical security and risk management - Nat. Bureau of Standards - FIPS PUB 31

This publication provides guidelines to be used by Federal organizations in structuring physical security programs for their ADP facilities. It treats security analysis, natural disasters, supporting utilities, system reliability, procedural measures and controls, off-site facilities, contingency plans, security avareness and security audit.
It contains statistics and information relevant to physical security of computer data and facilities and references many applicable publications for a more exhaustive treatment of specific subjects.

AC 135 Principles of data base management - Martin, J. (ca. 350 blz.)

Probably the most important subject in corporate data processing for the next ten years will be the development of data bases. Few persons will escape its impact. Some organizations have been spectacularly successful in building the data bases they need, while others have met with expensive failure.
The most successful ones claim that their organization could not operate the way it does today without their data bases.
It is vitally important that corporate management, as well as data processing personnel, should appreciate the role of data bases in running an organization. They should be able to distinguish the myth from reality, and understand the reasons for failures as well as the roads to success.

Hitherto data base principles have been difficult to learn. Now this volume presents a lucid introduction which is both comprehensive and enjoyable to read. It explains data base management software, data base evolution and growth, and the uses of data bases in managament information systems.

Among its outstanding features, the book:

- Provides the easiest possible way to learn data base principles.
- Presents the subject matter in a simple easy-to-read way, yet all vital aspects of the subjects are covered.
- Explains the reasons for using data base technology rather than the simpler files of earlier data processing.
- Strips away the complexity of current data base software layer by layer.
- Will act as an invaluable guide to management and students in understanding this vital new type of corporate resource.
- Discusses the myth and the reality of "Management Information Systems" and how computer data can be developed to be of maximum value in an organization.
- Summarizes the reasons for success and failure in data base development.
- Gives checklists which will quide management's interrogation of their own data processing staff.

AC 137 Programmeertalen voor gegevensbanken
R. van Dooren / Th.G. Streng - NOVI (205 blz.)

Geschreven in opdracht van de Stichting Het Nederlands Opleidings Instituut voor Informatica (Studiecentrum NOVI), bevat dit boek een toelichting op het CODASYL Data Base Task Group rapport van april 1971.
Hoewel het boek in de eerste plaats is bedoeld als hulpmiddel bij de studie voor de module B.2 van het modulaire informatica-onderwijs, is het eveneens een zeer bruikbare inleiding voor allen die zich willen oriënteren in gegevensbanksystemen die zijn gebaseerd op het CODASYL-model.

Het boek geeft een uitgebreide toelichting op alle taalelementen uit het CODASYL-rapport. Deze toelichting is aangevuld met een groot aantal voorbeelden, zodat een helder inzicht kan worden verkregen in deze materie.

AC 138 Crime by computer - D.B. Parker (330 blz.)

Business, governments, and other institutions that use computers are more vulnerable to large losses and major failures today than ever before. Computerized bank embezzlements average almost $ 500,000 each (about 25 times the average embezzlement). A computer-dependent company faced by even a few days of computer unavailability can face financial ruin.
Hardly any computer crime is uncovered through normal security precautions of accounting controls. Much of what is detected is never reported.
Based on hundreds of cases Donn Parker has investigated, this is the first authoritave book on crime involving computers. Parker, who knows more than anyone about the perpetrators of such crimes, tells who they are, why they do it, how they succeed, and how they can be stopped. He covers, as well, important issues arising out of the new computer technology: legal entanglements, violations of personal privacy, computer intimidation, the future of white-collar crime.
This is must reading for executives, managers, and consultants-and for everyone who owns a credit card or uses a checking account and is concerned about the safety of his financial assets.