# compact

COMPUTER EN ACCOUNTANT

UIT DE INHOUD




Klynveld Kraayenhof & Co.
ACCOUNTANTS

Internationaal KMG Klynveld Main Goerdeler

NUMMER 27 9E JAARGANG LENTE 1982

# COMPUTER EN ACCOUNTANT

INHOUDSOPGAVE




NUMMER 27 9E JAARGANG LENTE 1982

compact

Lente 1982

## VAN DE REDACTIE

*LENTE 1982: een nieuw geluid.*

De aangekondigde samenvatting van de lezing "De invloed van kleinschalige automatisering op de accountantscontrole" geschreven door de heren J.F.C. van Epen en drs. J.E. Huizenga, vormt de prelude. Daarna volgt een compositie met 2 variaties op het thema Privacy van de hand van de heren A.W. Neisingh "2 dagen Oostenrijk" en "De wet op de persoonsregistraties" van J.F.C. van Epen.

De gebruikelijke vingeroefeningen kunt u lezen onder de rubrieken "Boeken", "Tijdschriften" en "ABC-Nieuws".

Toegift vormt de mededeling van de nieuwe cursusbrochure 1982.

Geachte lezer, heeft u commentaar of aanvulling op dit lenteprogramma, laat de redactie het weten. Voor u is daarvoor ruimte beschikbaar in Compact.

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

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

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

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

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

Ontwikkeling op het gebied van de privacywetgeving

OP 26 april jl. vond het symposium 'De privacywetgeving in de Nederlandse samenleving' plaats. Het symposium, dat door ruim 400 personen werd bezocht, is bijzonder geslaagd, niet in het minst door de slotrede, die werd uitgesproken door de Minister van Justitie J. de Ruiter.

Uit zijn voordracht vermelden wij hierna de laatste ontwikkeling op het gebied van de wetgeving met betrekking tot de bescherming van de persoonlijke levenssfeer.

WETSONTWERP REGELT VOORLOPIGE AANMELDING GEAUTOMATISEERDE PERSOONSREGISTRATIES

De Ministerraad heeft op 8 april ingestemd met een ontwerp van tijdelijke wet aanmelding geautomatiseerde persoonsregistraties. Het wetsontwerp zal ter advisering aan de Raad van State worden voorgelegd. Het ontwerp heeft betrekking op een deel van de materie die wordt geregeld in het ontwerp van Wet op de persoonsregistraties en kan worden beschouwd als een aanloop daartoe.
Het is de bedoeling van Minister De Ruiter dat de tijd tot de inwerkingtreding van de grote privacywet zo goed mogelijk wordt benut met voorbereidende werkzaamheden.
Eén daarvan is de bevordering van de zelfregulering door de houders van geautomatiseerde persoonsregistraties.
Daarnaast komen er onderzoeken naar aard en aantal van de bestaande persoonsregistraties, waarvan de resultaten van belang kunnen zijn voor de parlementaire besluitvorming en voor de voorbereiding van de Registratiekamer, die bij de inwerkingtreding van de wet op de persoonsregistraties aan het werk moet gaan.
Als derde voorbereidingsmaatregel dient de nu voorgestelde wettelijke verplichting tot het doen opnemen in een openbaar register van bepaalde categorieën van geautomatiseerde persoonsregistraties. In het bijzonder moet daarbij worden gedacht aan registraties die gevoelige persoonsgegevens bevatten, zowel bij de overheid als in de particuliere sector.

Het nieuwe wetsontwerp voorziet in de instelling van een openbaar register bij het Ministerie van Justitie. Geautomatiseerde persoonsregistraties, die in de termen van de wet vallen, zullen zich daar moeten aanmelden per apart formulier waaruit de gegevens omtrent de inrichting van de registratie kunnen worden afgeleid.
Verwacht wordt dat door deze regeling wordt bevorderd dat de houders van persoonsregistraties, die tot aanmelding worden verplicht zich nog beter bewust zullen worden van de problematiek van de bescherming van de persoonlijke levenssfeer.

Redactie

# DE INVLOED VAN KLEINSCHALIGE AUTOMATISERING OP DE ACCOUNTANTSCONTROLE

Onder bovenstaande titel is door J.F.C. van Epen en drs. J.E. Huizenga in januari jl. een inleiding gehouden voor de landelijke contactvergadering accountants van Klynveld Kraayenhof & Co.
In het eerste deel van de presentatie lag het accent op de problemen die voor de controlerend accountant kunnen ontstaan ten gevolge van het door de cliënt niet of onvoldoende beheersen van de invoering van kleinschalige automatisering (mini-, micro- of small business computers).
In het tweede deel werd de invloed op de uitvoering van de accountantscontrole behandeld.

## Deel 1: Invoering kleinschalige automatisering

door J.F.C. van Epen

### 1. Inleidend kader

De werking van een computer wordt bepaald door de in de computer actief zijnde programmatuur. Daardoor is een computer een zeer flexibel instrument, dat geheel volgens de wensen van zijn gebruiker zou kunnen functioneren. Dat dit niet altijd zo is, wordt in hoofdzaak veroorzaakt door het feit dat de gebruiker meestal niet zelf de computerprogramma's ontwerpt en codeert. Eén of meerdere malen zal overdracht van informatie en kennis plaatsvinden voordat de programmatuur gereed is. In deze keten treffen wij bijvoorbeeld de volgende schakels aan: gebruiker - projectleider - systeemanalist - programmeur. Teneinde de werkzaamheden van deze functionarissen te beheersen is een aantal werkregels opgesteld voor de wijze waarop computerprogramma's tot stand dienen te komen. Deze regels dienen, heel ruim gesteld, door een organisatie te worden uitgevoerd die borg staat voor de ontwikkeling van betrouwbare computerprogrammatuur.

Daartoe dienen in de ontwikkelingsorganisatie een aantal maatregelen van interne controle te zijn opgenomen zoals functiescheiding, goede documentatie en periodieke evaluatie.

Het proces van de ontwikkeling van computerprogrammatuur is daartoe opgedeeld in een aantal stappen. Bij voorbeeld:
1. Formuleren eisen.
2. Systeemontwerp.
3. Systeemanalyse.
4. Programmering.
5. Test.
6. Conversie bestanden.
7. Invoering.

Deze programma-ontwikkelingscyclus wordt vaak aangeduid met de Engelse term "System Development Life Cycle" (meestal afgekort tot SDLC).

Ook al wordt de ontwikkeling nog zo goed bewaakt, de programmatuur nog zo goed getest, volledige zekerheid omtrent de juistheid van de programma's is niet te verkrijgen. Er kan zich in de toekomst altijd wel een onvoorziene situatie voordoen die tot onjuiste verwerking leidt. In de programmatuur zullen daarom controles moeten worden opgenomen, die in een foutsituatie tot signalering leiden. Een andere mogelijkheid is het aanbrengen van tellingenverbanden.
Uiteraard dient de gebruikersorganisatie deze signaleringen en controle-informatie op een juiste manier af te handelen. Aanpassing van deze organisatie is daarom onvermijdelijk.

Het vorenstaande is van toepassing op het gehele gebied van de automatisering. Aangegeven is op welke wijze de met automatisering samenhangende problemen tot een oplossing kunnen worden gebracht: met een adequate organisatie die middels een aantal maatregelen van interne controle zichzelf beschermt tegen foutieve handelingen. Daarvoor zijn mensen nodig.
Wanneer wij ons beperken tot kleinschalige automatisering, zien wij nieuwe problemen ontstaan. Kleinschaligheid impliceert immers minder mensen rondom de computer. En daardoor minder mogelijkheden tot functiescheiding. Zo zal doorgaans de automatiseringsafdeling ook klein zijn, dan wel geheel ontbreken. Het aantal specialismen zal zeker gering zijn. Veelal ontbreekt dan ook de afdeling systeemontwikkeling.

De benodigde specialisten worden dan van buiten de organisatie aangetrokken. Er zijn in de loop der jaren een veelheid van bureaus ontstaan die computer-programma-pakketten ontwikkelen en verkopen: de zgn. software-huizen. Ook wordt programmatuur op bestelling, geheel naar de wensen van de klant gemaakt. Ook tussenvormen komen - veelal om budgettaire redenen - voor, waarbij standaardpakketten worden gemodificeerd op grond van de individuele gebruikersbehoeften.
En juist hier ligt de oorzaak van veel problemen: In het afhankelijk zijn van buitenstaanders. Hun veelal solistisch optreden, dikwijls gepaard met een beperkt inzicht in interne controle en vooral hun gebrek aan specifieke bedrijfskennis van hun cliënten zijn de oorzaken van soms optredende teleurstellende resultaten. Bovendien werken zij onder een zware tijdsdruk, waardoor zij meer aandacht hebben voor het technisch - dan voor het betrouwbaarheidsaspect. Om enige verwachting uit te spreken over het op te leveren eindprodukt, zullen een aantal kritische vragen gesteld moeten worden, zoals:

- Weet de gebruiker (cliënt) precies wat hij wil hebben en is hij in staat dit correct te formuleren?
- Heeft hij daarbij in voldoende mate gedacht aan toekomstige ontwikkelingen?
- Heeft het software-huis begrepen wat de klant wil? (Terugkoppeling!)

- Heeft de klant voldoende greep op de ontwikkeling, zodat zo nodig tijdig kan worden bijgestuurd?
  Wordt gewerkt volgens de methode van de SDLC, is hier eigenlijk de vraag.
- Zijn de systeemanalisten en de programmeurs van het software-huis van voldoende niveau?
- Gelden er bij het software-huis algemeen aanvaarde standaards en normen voor de ontwikkeling van programmatuur?
- Zijn daarin maatregelen van interne controle voorgeschreven?
- Is er een test- en acceptatieprocedure voorzien?
  Testen is een uitermate belangrijke fase in de systeemontwikkeling.
- Is er voldoende controle op de conversie van bestanden?
  Conversie wordt ook nogal eens verwaarloosd. Juist omdat dit aan het eind van de ontwikkelingscyclus plaatsvindt.
- Geeft het software-huis instructies voor de beveiliging van programmatuur en bestanden?

Helaas is de ervaring dat in sommige gevallen, waar het om kleinschalige automatisering gaat, een aantal van de gestelde vragen niet positief beantwoord kan worden. Met, op zijn zachtst gezegd, vervelende gevolgen voor de gebruiker. En soms ook voor de accountant. Door bijvoorbeeld het verzwakken van de interne controle of het niet meer beschikbaar komen van voor hem relevante informatie, ziet hij zijn controle bedreigd.

Een verzwakking in de organisatie kan optreden door het niet in stand houden van functiescheidingen binnen de computer.
Juist de moderne verwerkingstechnieken, waarbij ieder die een terminal binnen bereik heeft de computer kan bedienen, vereisen stringente doorvoering van de bestaande functiescheidingen.

## 2. Praktijksituaties

Na de inleiding werd ter illustratie een aantal praktijksituaties geschetst. Enkele hiervan zullen nu kort worden toegelicht.

### 2.1 Een software-huis dat geen programmerings- en documentatiestandaards heeft voorgeschreven

De toepassing vereiste het op meerdere plaatsen in de verwerking uitvoeren van eenzelfde berekening, namelijk het opbouwen van de verkoopfactuur. Echter steeds met een ander doel:

a. ten behoeve van het "orderblad" (ter controle op de factuuropbouw);
b. voor het vervaardigen van de factuur zelf;
c. voor het journaliseren van de factuur.

Een uit efficiency-overweging correcte oplossing zou zijn geweest om de berekening door een afzonderlijke routine te laten verrichten en deze routine steeds aan te roepen wanneer de berekening gewenst is. Dit geeft de zekerheid dat de uitkomst steeds identiek is als dezelfde grootheden aan de routine worden aangeboden.

De programmeur koos, bij gebrek aan een dergelijk voorschrift, voor de meest omslachtige en minst betrouwbare methode. Overigens zonder hiervan melding te maken in de documentatie.
Hij programmeerde de berekeningroutine driemaal, steeds met gebruikmaking van een andere naamgeving voor de gebruikte variabelen. Hierdoor viel vrijwel niet op dat het driemaal om dezelfde berekening ging.
Daarbij kwam dat hij de berekening niet goed had begrepen, zodat de bewuste routine gewijzigd moest worden.
Vermoedt u wat er gebeurde?
Inderdaad, twee van de drie routines werden gewijzigd; die voor de journaalpostopbouw werd vergeten.
Ogenschijnlijk liep bij de invoering alles goed. Bij de accountantscontrole werd echter ontdekt dat sommige journaalposten onjuist waren. De administrateur had deze nimmer bekeken. Onervarenheid met automatisering deed hem blindelings vertrouwen op de computer.
Het heeft veel (accountants)werk gekost de administratie weer in het reine te krijgen.

## 2.2 Foutieve invoering van een standaard programmapakket

Een veel voorkomende faciliteit in financieel-administratieve pakketten is de mogelijkheid om boekingen op nader op te geven grootboekrekeningen te cumuleren en dan pas af te drukken; het zgn. verdicht boeken.
Uit vrees voor te veel papier, een te dik grootboek, wordt van deze mogelijkheid nogal eens in ruime mate gebruik gemaakt door administrateurs; en dan zonder voorafgaand overleg met hun accountant.
Het gevolg is dat op de grootboekrekeningen allerlei samengestelde bedragen verschijnen, waarvan de opbouw óf met veel moeite, óf in het geheel niet kan worden verkregen.
Er is mij reeds een aantal van deze gevallen bekend. De verkregen papierbesparing kan echter leiden tot een toeneming van accountantskosten, wat ingeval van tijdig overleg voorkomen had kunnen worden.

## 2.3 Te veel vertrouwen in het software-huis

De programmatuur die was vereist, was alleen voor wat betreft de inkoopadministratie specifiek voor het bedrijf. Dit gedeelte moest dan ook "naar maat" gemaakt worden. De boekhouding (grootboek, debiteuren- en crediteurensubadministratie) kon worden gevoerd met behulp van programmatuur die doorgaans tot het standaardaanbod behoort van een software-huis dat actief is op de markt voor administratieve automatisering. Vandaar dat op basis van een vrij beknopt systeemontwerp, slechts omvattende een korte beschrijving van de gewenste functies en uitvoer, de programmeurs aan het werk gingen. De gebruiker bleef lange tijd buiten spel.

Toen het systeem eindelijk werd opgeleverd bleek er nauwelijks mee te werken. Ook de accountantscontrole bleek problemen op te leveren. Redenen voor de accountant om een deskundige van de A.C.-groep te raadplegen. Bij gebrek aan actuele documentatie werd de kennis over het systeem vergaard door middel van interviews met de programmeur. Daarbij bleek dat deze voor het eerst in zijn loopbaan een administratieve toepassing had ontwikkeld.
Enkele van de vele gebreken van het systeem zijn wellicht daardoor te verklaren. Zij spreken voor zich:

- een journaalpost behoefde niet in evenwicht te zijn om geaccepteerd te worden;
- het saldo per crediteur was niet steeds gelijk aan het totaal van de voor die crediteur openstaande posten;
- alle boekingen werden per verwerking samengesteld tot één journaalpost zonder verslag waardoor achteraf niet meer was vast te stellen waaruit een journaalpost bestond;
- daardoor was ook geen specificatie te verkrijgen van te verrekenen BTW;
- kostenfacturen konden niet worden geboekt omdat alleen het inkoopgoederenprogramma de crediteurenadministratie kon bereiken, waaruit dwangmatig de voorraadrekening gedebiteerd werd;
- creditnota's werden als debetnota's verwerkt.

Daarnaast miste het systeem een aantal voor de verwerking noodzakelijke functies.
De vooraf overeengekomen koopsom was reeds lang betaald en voor herstel van de fouten zou per uur bijbetaald moeten worden. Onze cliënt was, na een driedaagse test en een daarop volgend verslag van KKC omtrent de geconstateerde gebreken van het systeem, van mening dat het software-huis wegens wanprestatie in rechte zou zijn aan te spreken.

## 2.4 Verlies van functiescheiding ten gevolge van de invoering van automatisering

Onze cliënt had een software-huis gekozen dat werkte volgens goede interne standaards en normen.
De cliënt zelf was zeer alert en voerde het systeem liever een half jaar later in dan dat hij te weinig aandacht zou besteden aan testen en verbeteren van de programmatuur. Ook zijn accountant werd tijdig ingeschakeld en een medewerker van de A.C.-groep kon de gehele ontwikkeling volgen en zo nodig amenderen.

Het probleem ontstond hier echter pas bij de invoering.
Hoewel dit aanvankelijk niet de bedoeling was, werden bij de verschillende gebruikende afdelingen terminals geplaatst. Er waren echter geen afzonderlijke produktiebibliotheken per gebruiker voorzien. Er was geen controle op de persoon die een bepaald programma startte en daarmee bestanden ging bijwerken. Alle mogelijkheden van de computer stonden aan ieder ter beschikking. Zelfs programmeren.

De functiescheiding die in de onderneming aanwezig was en die voor de accountant één van de pijlers van interne controle was, waarop zijn controle steunde, was hierdoor in één keer buiten werking gesteld.

Ondanks onze betrokkenheid werden wij verrast door deze situatie. De cliënt had het niet belangrijk genoeg geacht ons ervan in kennis te stellen. Het bedrijf had zich in onvoldoende mate gerealiseerd welke de organisatorische consequenties zouden zijn bij het invoeren van automatisering op een dergelijke geavanceerde manier.

2.5 Doorbreken van de vereiste procedures door de gebruiker zelf

Tenslotte een aantal korte praktijkvoorbeelden waar het nalaten van noodzakelijke handelingen hebben geleid tot continuïteitsverstoring of verlies van gegevens.

A. Op een kleine computer werkend met zgn. diskettes was een controle voorzien om vast te stellen dat de juiste diskette in de machine was gebracht. De terminalbediende moest aan de hand van het laatste invoerverslag het laatst ingebrachte boekstuknummer intoetsen. Dit werd door het computerprogramma vergeleken met het nummer in het laatste record op de diskette. Klopte dit, dan was men nagenoeg zeker dat de juiste diskette was geladen. Een eenvoudig maar goed werkend controlemiddel.
Eén der gebruikers vond dit echter nogal lastig. Hij schreef daarom zelf een klein programma dat op de diskette het gevraagde gegeven opzocht en op het beeldscherm toonde.
Het daarna opgestarte verwerkingsprogramma kreeg op zijn vraag het zoëven opgezochte antwoord en ging verder zonder dat lastige gezoek naar het laatste verwerkingsverslag.

B. Een andere mogelijkheid om zeker te zijn met de juiste diskette verder te werken is deze eenvoudig in de computer te laten zitten. Eén onzer cliënten paste deze methode toe. De computer was van het tafelformaat. Inbrekers hadden dan ook weinig moeite met het voor de hobbymarkt best interessante apparaat. Op een morgen was dan ook niet alleen de computer weg, maar ook de boekhouding. Vastgelegd op de diskette in de computer. Men had verzuimd kopieën te maken.

C. Dat dagelijks kopiëren van alle belangrijke bestanden tot de vaste procedures dient te behoren, die nageleefd móeten worden ook als het wat later wordt, ondervond één onzer cliënten waar dit eenmaal werd nagelaten. Toen de volgende morgen degene die normaal de computer bediende ziek was moest een ander zijn taak overnemen en de computer starten. Dit werd verkeerd gedaan. Het gehele bestand waarin de orderverwerking was vastgelegd ging teniet. De inderhaast geroepen administrateur zou het wel even repareren. Hij greep echter mis toen hij de kopie-bestanden van de vorige dag zocht. Wel die van de dag daarvoor. Die toen maar geladen. Maar de produktie van een hele werkdag was wel verloren gegaan.

Deze laatste drie case-studies beschrijven de gevolgen van het doorbreken van procedures en voorschriften door diegenen die verantwoordelijk zijn voor de goede computerverwerking. Hoeveel te erger is het met cliënten waar helemaal geen procedures gelden. Waar ieder voor zich bepaalt wat er moet gebeuren. Wat kan daardoor allemaal mis lopen?

## 3. Samenvatting van het eerste deel

De in het vorige hoofdstuk geschetste praktijkervaringen doen ons realiseren dat er bij het invoeren van automatisering wel het een en ander mis kan lopen. De oorzaken moeten meestal worden gezocht in het onvoldoende rekening houden met de zich wijzigende organisatie. Tijdens de ontwikkeling van de systemen én na de invoering ervan. Zowel onze cliënt als wijzelf als controlerend accountants kunnen daarvan kwalijke gevolgen ondervinden.
Een subtiele vraag hierbij is: Wat kan de accountant er aan doen?

Toch wel het een en ander. En bovendien: hij móet er wat aan doen!

Immers, automatisering beïnvloedt de organisatie en de organisatie heeft weer invloed op de aanpak van de controle. Wij zullen moeten vaststellen dat in de organisatie van de cliënt adequate maatregelen van interne controle en beveiliging zijn opgenomen, ter waarborging van een betrouwbare en een ongestoorde gegevensverwerking.
Ook tijdens de ontwikkeling van geautomatiseerde informatiesystemen zullen er maatregelen getroffen moeten zijn die zijn gericht op het tot stand komen van betrouwbare en veilige systemen.

Een aantal mislukkingen in de praktijk zou voorkomen kunnen worden bij alert reageren van de behandelend accountant. De oorzaak ligt vaak bij de cliënt zelf, die zijn accountant - uit kostenoverwegingen - er maar liever buiten laat.

De investeringsbeslissing wordt nogal eens genomen op grond van de prijs van de computer en de programmeerarbeid. Toch maken deze slechts ongeveer de helft uit van de totale investering. Tot de andere helft behoren allerlei kosten, waaronder die voor het testen de belangrijkste zijn. Ook de kosten van de accountant, als medebelanghebbende bij het systeem, zullen uit doelmatigheidsoverwegingen in een vroegtijdig stadium gemaakt dienen te worden.
Ook al weegt voor de cliënt het economisch motief zwaar, de accountant mag zich in het belang van zijn controle er niet van laten weerhouden zich tijdig op de hoogte te stellen. Hij dient zich ervan te vergewissen dat zijn cliënt aandacht heeft besteed aan de essentiële voorwaarden voor een betrouwbare automatisering, alsmede de doeltreffendheid van de informatieverstrekking.
In de inleiding is een aantal van deze voorwaarden genoemd.

Ter afsluiting laten wij nog enkele attentiepunten volgen:

- Er dient personeel vrijgemaakt te worden ter begeleiding van de systeemontwikkeling (stuurgroep, werkgroep).
- Er dient een doordachte planning te zijn aan de hand waarvan de voortgang kan worden getoetst.
- Er dient een uitwijkprocedure te zijn voor het geval het systeem niet tijdig wordt opgeleverd.
- "Meekijken" door leden van de A.C.-groep is in veel gevallen aan te bevelen.

# DE INVLOED VAN DE KLEINSCHALIGE AUTOMATISERING OP DE ACCOUNTANTSCONTROLE

## Deel 2: Uitvoering van de accountantscontrole

door drs. J.E. Huizenga

### 1. Inleiding

In de afgelopen decaden heeft zich in de accountantscontrole een verschuiving voorgedaan van een controleaanpak, waarbij het accent lag op de controle van de informatie (de gegevens) naar een aanpak, welke zich meer richt op de beoordeling van (de goede werking van) de organisatie.

Deze accentverschuiving vond plaats onder invloed van ontwikkelingen in:
- de administratieve organisatie;
- de interne controle;
- de administratieve techniek;
- de leer van de accountantscontrole.

Het moge duidelijk zijn dat deze ontwikkelingen wel te onderscheiden, maar door hun onderlinge samenhang, zeker niet te scheiden zijn.

Eén van de ontwikkelingen in de administratieve techniek is de opkomst van mini- en microcomputers, of wel de kleinschalige automatisering.

Hieronder zal worden ingegaan op de invloed van deze moderne technische hulpmiddelen op de accountantscontrole.

### 2. Enige bijzondere aspecten van kleinschalige automatisering welke van belang zijn voor de accountantscontrole

#### 2.1 Administratieve organisatie

Bij de beoordeling van opzet en werking van de administratieve organisatie dient met name aandacht te worden besteed aan de volgende punten.

- Functiescheidingen

  In een kleinschalige automatiseringsorganisatie ontbreekt vaak een effectieve functiescheiding tussen gebruikers en automatiseringsafdeling.
  Indien een afzonderlijke automatiseringsafdeling aanwezig is, laat de functiescheiding tussen ontwikkeling (systeemontwerp, programmering en onderhoud van programmatuur) en bediening vaak te wensen over. Wanneer er telkens slechts ten behoeve van één bedrijfsafdeling door de computer gegevens worden verwerkt en

de gegevens van de overige bedrijfsafdelingen niet door het actieve computerprogramma kunnen worden benaderd, is het ontbreken van bovengeschetste functiescheidingen een minder groot bezwaar dan wanneer er sprake is van gemeenschappelijk gebruik van de computer en de gegevens door meerdere bedrijfsafdelingen.

In het laatste geval is het onder andere van groot belang dat de scheiding tussen de diverse gebruikers wordt geëffectueerd door middel van bijvoorbeeld het wachtwoordensysteem (passwords) en het beheer over bibliotheken met programma's en gegevensbestanden. De meeste mini's en micro's hebben wel enige vorm van password- en bibliotheekbeveiliging. Deze beveiliging is echter vaak zo beperkt (door de technische mogelijkheden en/of de wijze waarop de mogelijkheden worden toegepast) dat van een effectieve scheiding tussen de gebruikers onderling en tussen de gebruikers en de automatiseringsafdeling geen sprake is. Voor de accountant betekent dit een reëel gevaar van doorbreking van voor hem belangrijke functiescheidingen.

- Algemene maatregelen van interne controle met betrekking tot de geautomatiseerde gegevensverwerking, welke maatregelen gelden voor alle computertoepassingen.
Hierbij is met name van belang of gebruik gemaakt wordt van interpretertalen (BASIC) of compilertalen(COBOL) voor de programmering van computertoepassingen.
Een groot aantal kleine computers is uitgerust met interpreters, welke bij de programmaontwikkeling voordelen hebben boven de compilers. Uit gezichtspunt van interne controle hebben interpreters het nadeel dat geteste en geaccepteerde produktieprogramma's eenvoudig gewijzigd kunnen worden en wijzigingen in het bronprogramma ogenblikkelijk effectief worden. Bovendien is het bij veel interpreters mogelijk een lopend programma te onderbreken, de inhoud van werkvelden te inspecteren en eventueel te wijzigen en vervolgens de verwerking te hervatten. Dit alles zonder dat enig spoor van de ingreep achterblijft!
Het moge duidelijk zijn dat interpreters van het hierboven beschreven type een zodanige verzwakking vormen van de interne controle, dat voor de accountant het gebruik van deze interpreters voor produktieprogramma's onaanvaardbaar is.

Een andere factor welke van invloed is op de effectiviteit van de algemene maatregelen van interne controle wordt gevormd door het besturingssysteem. Het besturingssysteem verzorgt onder andere het gegevenstransport tussen programma's, gegevensbestanden en terminals en vormt een belangrijke schakel in de betrouwbaarheidsketen.
Vooral in de sfeer van de microcomputers is het besturingssysteem vaak een zwakke schakel uit het gezichtspunt van betrouwbaarheid. De microcomputers en hun besturingssystemen zijn in

eerste instantie niet ontwikkeld ten behoeve van administratieve toepassingen en bevatten mede daardoor allerlei mogelijkheden tot raadplegen en wijzigen van gegevens en programma's buiten de normale procedures om. De accountant zal moeten onderzoeken of het besturingssysteem functies bevat welke de betrouwbaarheid van de produktieprogramma's en -bestanden kunnen aantasten en of deze functies uit de produktieomgeving verwijderd kunnen worden.

Wat hiervoor gezegd is over besturingssystemen geldt min of meer ook voor de hulpprogrammatuur of utilities. Een verschil is dat het besturingssysteem altijd nodig is om met de computer te kunnen werken, terwijl de hulpprogrammatuur alleen in bijzondere gevallen nodig is. Om het gevaar van onjuist of onrechtmatig gebruik van hulpprogrammatuur te verminderen zou een mogelijke oplossing zijn deze programmatuur alleen in speciale gevallen en op een gecontroleerde wijze in de computer te laden en na gebruik te verwijderen.

## 2.2 Organisatiegerichte controleaanpak

Onder het hoofd Administratieve organisatie is een aantal aandachtspunten behandeld met betrekking tot de opzet en werking van de administratieve organisatie. In veel gevallen zal de conclusie moeten zijn dat de accountant aan het stelsel van interne controlemaatregelen in het geautomatiseerde traject van de informatieverzorging, te weinig zekerheden kan ontlenen om bij zijn controle het accent op de opzet en werking van de organisatie te leggen.
Eén en ander betekent zeker niet dat de accountant bij zijn controle het automatiseringsgebeuren zou kunnen negeren. Integendeel, vaak is de cliënt zich in het geheel niet bewust welke risico's er met betrekking tot de gegevensverwerking worden gelopen en welke oplossingen of compenserende maatregelen mogelijk zijn.
Dit is bij uitstek het deskundigheidsterrein van de accountant en hij zal de cliënt over deze aspecten kunnen (moeten?) adviseren.

## 2.3 Informatiegerichte controleaanpak

Voor het selecteren van de te onderzoeken posten in het kader van een informatiegerichte controleaanpak staan dankzij de automatisering de volgende methoden ter beschikking:

- selectie met behulp van audit packages, zoals wij die reeds kennen voor de grotere computers (CARS, EDP-AUDITOR, CA-EARL). Deze pakketten hebben het voordeel dat ze alle functies bevatten die de accountant bij de selectie van posten nodig heeft (rekenfaciliteiten, steekproefmodules, e.d.). Een nadeel is dat vaak gebruik gemaakt moet worden van een COBOL-compiler, welke niet op alle installaties aanwezig is;

- selectie met behulp van opzoek of retrieval programma's van de leverancier. Deze programma's zijn niet altijd beschikbaar. Ze zijn in het algemeen eenvoudig te gebruiken, doch zijn beperkt in hun mogelijkheden;

- selectie met behulp van hulpprogrammatuur of utilities. Deze programma's zijn vaak wel beschikbaar; ze zijn moeilijk te gebruiken en vaak functioneel nog beperkter dan de retrieval programma's;
- het is altijd mogelijk een speciaal selectieprogramma te (laten) schrijven. Dan zijn alle functies beschikbaar. Ze zijn vaak minder flexibel dan audit packages en relatief duur.
- momenteel wordt in een aantal gevallen cliëntenbestanden van kleinschalige computers geconverteerd zodat ze op de KKC-computer met het EDP-AUDITOR pakket verwerkt kunnen worden. Niet van elke computer kunnen de bestanden geconverteerd worden naar onze computer;
- indien selectie van de posten uit bestanden niet mogelijk is, kan vanaf computerlijsten met behulp van onze eigen microcomputers redelijk efficiënt een steekproef getrokken worden.

Er is een scala aan mogelijkheden om computers in te zetten bij de selectie van te onderzoeken posten; welke in een concreet geval toepasbaar is, kan de accountant met behulp van de A.C.-groep bepalen.

### 2.4 Andere toepassingsmogelijkheden

Niet alleen voor de selectie van te onderzoeken posten kan de accountant gebruik maken van de mogelijkheden van (kleinschalige) automatisering dat is tevens het geval bij cijferbeoordeling en het zelfstandig construeren van totaal- en controleverbanden.
Met name voor cijferbeoordeling en financiële modellen zijn voor kleinschalige computers een aantal interessante pakketten beschikbaar, die de accountant zou kunnen gebruiken en met behulp waarvan hij zijn cliënt van dienst kan zijn bij het opstellen van liquiditeitsprognoses, modellen voor investeringsbeslissingen, e.d.

## 3. Samenvatting

In de inleiding is gesteld dat, de ontwikkeling van de laatste decaden overziend, een accentverschuiving heeft plaatsgevonden in de aanpak van de accountantscontrole te weten van een informatiegerichte naar een organisatiegerichte controleaanpak.
Daarna is een aantal bijzondere aspecten van de kleinschalige automatisering behandeld. De conclusies zijn dat kleinschalige automatisering:

- beperkingen oplegt aan de mogelijkheid tot opzetten en handhaven van adequate maatregelen van interne controle;
- leidt tot een meer informatiegerichte controle-aanpak;
- mogelijkheden biedt om met behulp van de computer door de accountant te onderzoeken posten te signaleren;
- mogelijkheden biedt om ten behoeve van de controle het cijfermateriaal te hergroeperen of rekenkundig te bewerken.

# DE WET OP DE PERSOONSREGISTRATIES, ZIJN STRUCTUUR EN ZIJN INVLOED OP DE ORGANISATIE

door J.F.C. van Epen

## 1. Inleiding

Op 30 november 1981 is aan de Tweede Kamer aangeboden het Ontwerp van Wet houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties, doorgaans Privacywet genoemd. Een beknopte samenvatting van de meest belangrijke aspecten van deze wet, overgenomen uit het computerweekblad Computable, is in onderstaand kader weergegeven.

De noodzaak voor deze wet wordt in de Memorie van Toelichting, hoofdstuk 2, als volgt gemotiveerd: "Technische en maatschappelijke ontwikkelingen hebben de bescherming van de persoonlijke levenssfeer in onze tijd actueel gemaakt. Dit geldt voor het vraagstuk in het algemeen, het geldt in het bijzonder voor de registratie van persoonsgegevens. Om te kunnen voorzien in de groeiende behoefte aan informatie betreffende personen wordt steeds vaker gebruik gemaakt van moderne hulpmiddelen, waaronder computersystemen wel het meest op de voorgrond treden. Deze systemen verschaffen zo grote mogelijkheden tot opslag en verwerking van gegevens, dat reeds daardoor de vraag naar meer en meer specifieke informatie kan worden gewekt. In het oog springende eigenschappen van deze systemen zijn voorts de snelheid waarmede zij werken, hun vermogen tot ordenen, selecteren en het leggen van verbanden, de mogelijkheid om op grote schaal informatie te verkrijgen en een grote kring van gebruikers, zo nodig op afstand, direct en zonder menselijke tussenkomst te bedienen."
Dus vooral de mogelijkheid om snel en op grote schaal gegevens te verwerken, te bewerken en te koppelen maakt regulering gewenst.

**Het wetsontwerp op de persoonlijke levenssfeer heeft in beginsel betrekking op geautomatiseerde bestanden van gegevens die zijn te herleiden tot individuele personen. Anonieme gegevens vallen er dus buiten. Er is een mogelijkheid ook niet-geautomatiseerde bestanden onder de werkingssfeer van de wet te brengen. Er wordt onderscheid gemaakt tussen, in toenemende graad van gevoeligheid, meldingsplichtige, reglementsplichtige en vergunningsplichtige bestanden. De eerste zijn onderworpen aan een van een aantal op verschillende toepassingen gerichte standaardreglementen, de tweede hebben een eigen, door de onafhankelijke Registratiekamer goedgekeurd reglement, en de derde bovendien een vergunning. De wet zal verplichtingen bevatten voor zowel de houder van een persoonsregistratie als de bewerker (bijvoorbeeld een computerdienstverleningsbedrijf). Beide moeten aan de voorwaarden voor inschrijving bij de Registratiekamer voldoen. Sankties voor registreerders komen neer op het intrekken van de inschrijving, maar ook is strafvervolging denkbaar. Bovendien heeft een geregistreerde stevige grond onder de voeten bij een eventuele eis tot schadevergoeding. Kriteria waarop een gegevensbestand wordt beoordeeld zijn onder meer doel, inhoud, herkomst, bewaartermijn, gebruik en de mogelijkheden tot inzage en korrektie die de geregistreerde heeft. Deze zaken moeten worden vastgelegd in het reglement.**

De mogelijkheid tot het koppelen van bestanden en het daardoor verkrijgen van minder gewenste informatie is met name aanwezig in grotere rekencentra waar vaak een groot aantal persoonsregistraties wordt bewerkt. In deze verschillende persoonsregistraties kunnen dezelfde personen meerdere malen voorkomen, uiteraard met steeds andere gegevens. En ook al kennen wij in Nederland geen algemeen gangbaar persoonsnummer, toch zijn er wel sleutelgegevens denkbaar waarmee dergelijke bestanden onderling gekoppeld kunnen worden, bijvoorbeeld door middel van postcode + huisnummer. Hetzelfde hoofdstuk uit de M.v.T. bevat ook de volgende passage:
"De bezorgdheid voor aantasting van de persoonlijke levenssfeer, die in het licht van deze ontwikkeling is ontstaan, achten wij voor een belangrijk deel gerechtvaardigd. Voor degenen over wie gegevens zijn vastgelegd wordt de huidige situatie gekenmerkt door onzekerheid en ondoorzichtigheid. In veel gevallen beschikken zij niet over de mogelijkheid om na te gaan welke gegevens voor welke doeleinden worden gebruikt. Dit is vooral onbevredigend als op basis van die gegevens beslissingen worden genomen waarbij zij individueel betrokken zijn.

Bijzondere problemen doen zich voor indien het gaat om gegevens van vertrouwelijke aard, of gegevens waarvan de bekendheid in ruimere kring gemakkelijk tot discriminatie of ander maatschappelijk nadeel kan leiden. Deze en andere bezwaren kunnen ook aan de werking van niet-geautomatiseerde persoonsregistraties zijn verbonden.
Wat dit betreft moet dan ook worden vastgesteld, dat de bewustwording van vraagstukken die met de bescherming van de persoonlijke levenssfeer samenhangen, de gevoeligheid voor deze bezwaren heeft vergroot."

Hiermee is duidelijk aangegeven waarom er een wetsontwerp is ingediend dat zich richt op het reguleren van registratiesystemen van gegevens die te herleiden zijn tot individuele personen. En de nadruk ligt daarbij op de geautomatiseerde systemen.

De invoering van de Wet zal zeker gevolgen hebben voor de organisatie waar persoonsregistraties in gebruik zijn, ongeacht of de computerverwerking binnen die organisatie plaats vindt of daarbuiten.
De organisatie die eigenaar is van de persoonsregistratie wordt door de Wet "Houder" genoemd, de organisatie die voor derden de computerverwerking verricht, zoals bijvoorbeeld computerservicebureaus, worden aangeduid als "Bewerker".
Aan beide organisaties worden allerlei regels voorgeschreven om de privacy van de individuele personen, die in een bepaalde relatie tot die organisaties staan, te waarborgen.

## 2. Zelfregulering

Wat opvalt bij de bestudering van het Wetsontwerp en ook in de Memorie van Toelichting wordt benadrukt, is dat er grote waarde wordt gehecht aan zelfregulering.

Hiermee wordt bedoeld dat de houders van persoonsregistraties zelf zullen moeten vaststellen welke regels voor een bepaalde registratie zullen gelden.
De algemene regelingen uit de Wet zullen door de organisatie moeten worden vertaald in de specifieke regels voor elke persoonsregistratie.
Dit betekent dat de organisatie de niet-concreet omschreven bepalingen zelf zal moeten invullen en uitwerken.

## 3. Organisatie

Een definitie van het begrip organisatie wordt in de Wet niet gegeven. De Wet richt zich bij het geven van regels op de houder, in de M.v.T. ook Organisatie van de houder genoemd, alsmede op de bewerker van geautomatiseerde persoonsregistraties. Hoe eng of hoe ruim het begrip "Organisatie van de houder" moet worden gezien is niet zonder meer duidelijk. Wanneer men het begrip eng hanteert, zou eronder kunnen worden verstaan: een afdeling binnen een bedrijf, bijvoorbeeld de personeelsafdeling als houder van de personeelsregistratie.

Stelt men het begrip heel ruim dan zou een "concern" als houder van vele registraties aangemerkt kunnen worden.
Of de waarheid, zoals gebruikelijk, in het midden ligt, is nog een open vraag. Toch zullen zij die actief betrokken worden bij de zelfregulering, bij het uitwerken van de wettelijke bepalingen, een standpunt moeten innemen.
In dit artikel zal ervan uitgegaan worden dat met "Houder" wordt gerefereerd aan juridische eenheden zoals N.V.'s, B.V.'s, gemeenten, overheidsdiensten, enz.

## 4. Structuur van de Wet

Het wetsontwerp omvat 105 artikelen, die in 8 afdelingen zijn gegroepeerd. In afdeling 1 is een aantal begrippen omschreven, zoals: gevoelig gegeven, persoonsregistratie, houder en bewerker.
Art. 3 geeft aan voor welke persoonsregistraties de Wet niet van toepassing is. Dit zijn alleen de zeer "onschuldige" registraties zoals adresbestanden, telefoonboek, giroboek, e.d., alsmede niet geautomatiseerde bestanden, mits daarin geen andere persoonsgegevens zijn opgenomen dan nodig voor het gebruik én geen gegevens daaruit aan derden worden verstrekt.
Afdeling 2 (art. 5 t/m 16) handelt over de Registratiekamer en het register: "De Registratiekamer is belast met de zorg voor de uitvoering en het toezicht op de naleving van de wet" (art. 9, lid 1) en: "De Registratiekamer houdt een openbaar register voor de inschrijving van persoonsregistraties die ingevolge de Wet ingeschreven moeten worden" (art. 14, lid 1).

Bovendien is van belang dat dit register voor iedereen kosteloos ter inzage ligt (art. 14, lid 2).
Afdeling 3 (art. 17 t/m 84) is verreweg het belangrijkste deel van de Wet en geeft regels met betrekking tot de geautomatiseerde persoonsregistraties, terwijl afdeling 4 nader omschrijft in welke gevallen niet-geautomatiseerde registraties met geautomatiseerde gelijk worden gesteld.
Volgens art. 18 kunnen de geautomatiseerde persoonsregistraties, voor zover zij volgens art. 3 onder de Wet vallen, worden ingedeeld in drie categorieën:
a. Meldingsplichtige registraties; zie art. 19;
b. Reglementsplichtige registraties; zie art. 20 en
c. Vergunningsplichtige registraties; zie art. 21.

Tot de laatste categorie behoren alle registraties die de in de Wet genoemde gevoelige gegevens bevatten (art. 1).
In de artikelen 26, 27 en 28 wordt vervolgens bepaald wat van iedere categorie in het register moet worden ingeschreven.
De artikelen 40 t/m 43 geven aan wat tenminste in het reglement moet worden opgenomen. In het volgende hoofdstuk wordt hierop teruggekomen.

Afdeling 5 (art. 87) behandelt de schadevergoeding, afdeling 6 (art. 88 t/m 90) de internationale aspecten, afdeling 7 (art. 91 t/m 93) de strafbepalingen en afdeling 8 omvat de overgangs- en slotbepalingen.

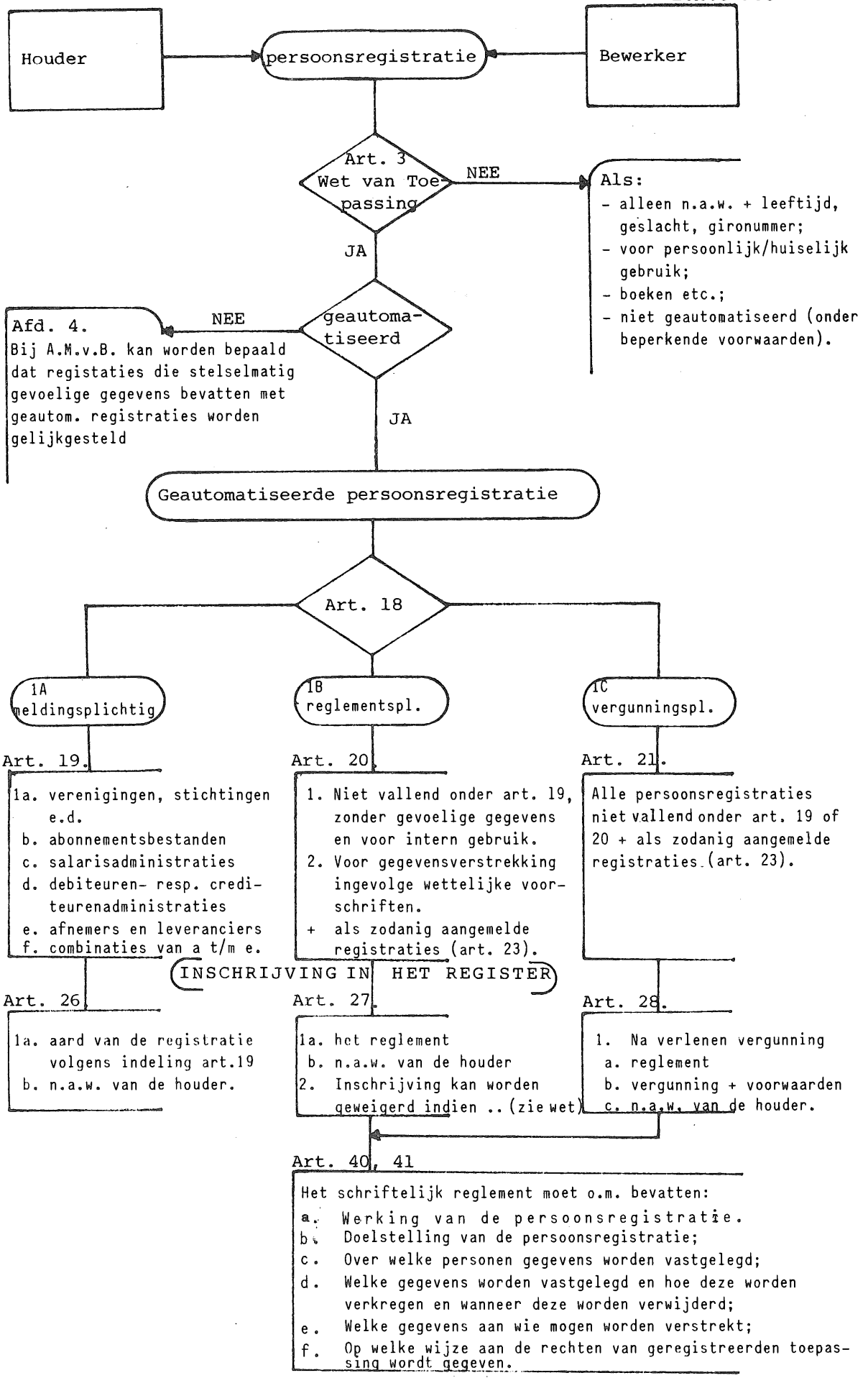
Het accent van de regeling ligt op afdeling 3. In bijgaand schema is de samenhang van de afdelingen 1 en 4 met het eerste deel van afdeling 3 weergegeven.

## 5. Taken voor de organisatie

Welke werkzaamheden komen er nu vanuit de Wet op de organisatie van de houder, resp. de bewerker af?
Uit de afdelingen en paragrafen van het wetsontwerp, die zich specifiek richten op de houder of de bewerker, zijn de belangrijkste taakgebieden geselecteerd.

### 5.1 Voorlopige inschrijving (art. 94, 95)

Een van de eerste zaken waarmee de houder te maken krijgt is de verplichting tot voorlopige inschrijving van de persoonsregistratiesystemen behorende tot zijn organisatie, die onder de Wet vallen. Deze voorlopige inschrijving betekent het aanmelden van deze registraties bij de Registratiekamer.
Dit moet geschieden binnen één jaar nadat die Registratiekamer is geïnstalleerd.
In concreto betekent dit dat er binnen de organisatie een inventarisatie zal dienen plaats te vinden van alle registratiesystemen die persoonsgegevens bevatten.


Houder
persoonsregistratie
Bewerker
Art. 3 Wet van Toepassing
NEE
Als:
- alleen n.a.w. + leeftijd, geslacht, gironummer;
- voor persoonlijk/huiselijk gebruik;
- boeken etc.;
- niet geautomatiseerd (onder beperkende voorwaarden).
JA
geautomatiseerd
NEE
Afd. 4.
Bij A.M.v.B. kan worden bepaald dat registaties die stelselmatig gevoelige gegevens bevatten met geautom. registraties worden gelijkgesteld
JA
Geautomatiseerde persoonsregistratie
Art. 18
1A meldingsplichtig
1B reglementspl.
1C vergunningspl.
Art. 19.
1a. verenigingen, stichtingen e.d.
b. abonnementsbestanden
c. salarisadministraties
d. debiteuren- resp. crediteurenadministraties
e. afnemers en leveranciers
f. combinaties van a t/m e.
Art. 20.
1. Niet vallend onder art. 19, zonder gevoelige gegevens en voor intern gebruik.
2. Voor gegevensverstrekking ingevolge wettelijke voorschriften.
+ als zodanig aangemelde registraties (art. 23).
Art. 21.
Alle persoonsregistraties niet vallend onder art. 19 of 20 + als zodanig aangemelde registraties (art. 23).
INSCHRIJVING IN HET REGISTER
Art. 26.
1a. aard van de registratie volgens indeling art.19
b. n.a.w. van de houder.
Art. 27.
1a. het reglement
b. n.a.w. van de houder
2. Inschrijving kan worden geweigerd indien .. (zie wet)
Art. 28.
1. Na verlenen vergunning
a. reglement
b. vergunning + voorwaarden
c. n.a.w. van de houder.
Art. 40, 41
Het schriftelijk reglement moet o.m. bevatten:
a. Werking van de persoonsregistratie.
b. Doelstelling van de persoonsregistratie;
c. Over welke personen gegevens worden vastgelegd;
d. Welke gegevens worden vastgelegd en hoe deze worden verkregen en wanneer deze worden verwijderd;
e. Welke gegevens aan wie mogen worden verstrekt;
f. Op welke wijze aan de rechten van geregistreerden toepassing wordt gegeven.

Vervolgens zullen deze registratiesystemen in categorieën moeten worden ingedeeld, overeenkomstig de indeling van de Wet. Met betrekking tot de meldingsplichtige persoonsregistraties is de moeilijkheid dat er nog een Algemene Maatregel van Bestuur moet komen, waarin wordt bepaald welke persoonsgegevens in de verschillende groepen meldingsplichtige persoonsregistraties mogen voorkomen.
Voor de reglementsplichtige én vergunningsplichtige persoonsregistraties zal reeds bij de voorlopige inschrijving een reglement moeten worden overgelegd.

## 5.2 Opstellen reglementen (art. 41 t/m 43)

Een reglement moet worden opgesteld door de houder.
De Wet geeft een vrij uitgebreide opsomming van onderwerpen die in het reglement moeten worden geregeld.
Indien van het betreffende registratiesysteem een goede documentatie beschikbaar is, zal dit het opstellen van het reglement zeer kunnen vereenvoudigen.
De belangrijkste punten die in het reglement moeten voorkomen zijn:
- Werking van de persoonsregistratie;
- Doelstelling van de persoonsregistratie;
- Over welke personen gegevens worden vastgelegd;
- Welke gegevens worden vastgelegd en hoe deze worden verkregen en wanneer deze worden verwijderd;
- Welke gegevens aan wie mogen worden verstrekt;
- Op welke wijze aan de rechten van geregistreerden toepassingen wordt gegeven.

Voorts is bepaald dat het reglement in de Nederlandse taal moet zijn gesteld.

Bij Algemene Maatregel van Bestuur kunnen nadere regels over de vorm en inhoud van het reglement worden gesteld.

## 5.3 Rechten van de geregistreerden (art. 69 t/m 82)

De rechten van de geregistreerden betreffen:
- kennisgeving van opname in de persoonsregistratie;
- het recht op inzage en verbetering;
- het recht op informatie uit het protocol, dat verplicht is bij vergunningsplichtige persoonsregistraties.

De houder zal voorzieningen moeten treffen om er voor te zorgen dat de geregistreerde hiervan gebruik kan maken.

## 5.4 Optreden als bewerker (art. 55 t/m 66)

Organisaties die voor hun persoonsregistraties gebruik maken van een computerservicebureau kunnen dit na de invoering van de Wet alleen continueren als aan dat servicebureau een vergunning als bewerker is afgegeven door de Registratiekamer.

In art. 57 lid 2 wordt bepaald dat de aanvragende bewerker onder meer moet aangeven welke technische en organisatorische maatregelen zijn genomen ter bescherming van de persoonlijke levenssfeer.
Hieruit kan worden afgeleid dat deze organisatie aan zekere minimumeisen zal moeten voldoen. Welke criteria de Registratiekamer bij zijn beoordeling aanlegt is nog niet bekend.
Vooruitlopend daarop zullen de betreffende organisaties reeds de nodige maatregelen dienen te treffen.
Het kan ook voorkomen dat in geval van calamiteiten moet worden uitgeweken naar een computercentrum van een derde. Deze laatste moet dit binnen een week aan de Registratiekamer mededelen.
De Registratiekamer kan in het belang van de bescherming van de persoonlijke levenssfeer bepaalde voorwaarden aan de vergunning verbinden.

### 5.5 Beveiliging (art. 83 en 84)

De Wet geeft de mogelijkheid om bij AMvB regels te stellen in het belang van een goede beveiliging van persoonsregistraties. Ook de Registratiekamer kan nog aparte voorschriften geven op het moment van inschrijving van een registratiesysteem. De Memorie van Toelichting geeft nog weinig aanknopingspunten in welke richting deze AMvB en/of voorschriften zullen gaan.

## 6. Werkwijze in de organisatie

Om de hiervoor genoemde taken in de organisatie zo goed en efficiënt mogelijk uit te voeren verdient het o.i. aanbeveling dit op een gestructureerde wijze aan te pakken.
Aan het uitvoeren van genoemde taken zijn o.a. de volgende aspecten te onderscheiden: voorbereiding, coördinatie, overleg, voorlichting, beheer en controle.
De verantwoordelijkheid voor het nakomen van de wettelijke bepalingen ligt primair bij de houder. Hij is immers diegene die de zeggenschap heeft over de persoonsregistratie.
Naarmate de organisatie van de houder gecompliceerder is en het aantal registraties groter, zal de noodzaak om in de organisatiestructuur een aantal voorzieningen te treffen zich duidelijker doen gevoelen.
Bij de hierna volgende behandeling van de verschillende aspecten die geregeld moeten worden bij de voorbereiding en uitvoering van de door de Wet vereiste taken is uitgegaan van een organisatie met een aantal min of meer zelfstandige onderdelen.

### 6.1 Voorbereiding/Coördinatie

In een meer complexe organisatie is het bijna een "must" om te komen tot een bepaalde coördinerende functie.
Deze functie zal in eerste instantie tot taak moeten krijgen om voor alle organisatiedelen geldende richtlijnen op te stellen.

Deze richtlijnen zijn in feite een vertaling van de wettelijke bepalingen voor de organisatie.
Zij zullen o.a. aanwijzingen moeten bevatten voor de inventarisatie van de reeds aanwezige persoonsregistraties ten behoeve van de voorlopige inschrijving en aanmelding bij de Registratiekamer.
Ook de procedures welke gevolgd moeten worden voor eventueel nieuw te bouwen registratiesystemen en het wijzigen van bestaande systemen zullen hierin opgenomen moeten worden.
Voorts horen in deze richtlijnen de algemene beveiligingsmaatregelen, welke binnen de organisatie voor persoonsregistraties gelden, thuis.
Aangezien het opstellen van deze richtlijnen geen activiteit voor één persoon lijkt te zijn zou hiervoor een overlegcommissie in het leven geroepen kunnen worden. Deze zou kunnen bestaan uit vertegenwoordigers van de volgende disciplines binnen de organisatie: personeelszaken, organisatie, administratie, automatisering, juridische zaken.
In sommige gevallen kan het nuttig zijn een EDP-auditor of een automatiserings- en controledeskundige van de fungerende externe accountant of van de eigen interne accountantsdienst erbij te betrekken.

## 6.2 Overleg/Voorlichting

Een belangrijk aspect is te zorgen voor een goed overleg met en voorlichting aan de geregistreerde personen, zoals de eigen werknemers.
De houder zal bij het geven van richtlijnen duidelijk moeten maken waarom bepaalde regels nodig zijn. Te denken valt hierbij aan geheimhoudings- en beveiligingsmaatregelen.
Daarnaast zal ook aandacht besteed moeten worden aan de rechten van de geregistreerden.
Een belangrijk orgaan binnen de organisatie is de Ondernemingsraad.
Het is aan te bevelen deze raad te betrekken bij het overleg over en het opstellen van de noodzakelijke richtlijnen.
De Wet schenkt aan dit aspect geen aandacht, maar in de praktijk is de ervaring opgedaan dat overleg met Ondernemingsraden een goede zaak is. Het is gewenst dat dit in een zo vroeg mogelijk stadium op gang gebracht wordt.
Tevens zij in dit verband opgemerkt dat de Ondernemingsraad ten behoeve van de geregistreerden een "ombudsman"-functie zou kunnen vervullen.

## 6.3 Beheer

Zodra binnen de organisatie de voorbereidende werkzaamheden zijn afgerond, zal er voor gezorgd moeten worden dat de door de Wet opgelegde regels blijvend worden uitgevoerd.
Het verdient aanbeveling binnen de organisatie een functionaris aan te wijzen die namens de houder belast wordt met de zorg voor het naleven van de opgestelde richtlijnen.

Als één van de ondersteunende maatregelen voor deze functionaris kan binnen de organisatie een register worden ingesteld, waarin alle persoonsregistraties worden opgenomen.
Alle nieuwe systemen en wijzigingen in bestaande systemen zullen aan hem gemeld moeten worden. Hij zal ook de op te stellen reglementen moeten toetsen aan de richtlijnen.
Teneinde de organisatie op een efficiënte wijze te laten communiceren met de Registratiekamer zou deze beheersfunctionaris als contactpersoon aangewezen dienen te worden.
In het geval dat de bewerker van de registratiesystemen een derde is, lijkt deze functionaris ook de aangewezen persoon voor de contacten met de bewerker.

## 6.4 Controle

In deze beschouwing mag het aspect controle niet ontbreken.
Volgens art. 9 is de Registratiekamer belast met het toezicht op de naleving van de Wet.
Binnen de organisatie is de houder verantwoordelijk voor de uitvoering van de Wet.
In een meer complexe organisatie zal de houder naast een coördinerende en beherende functie behoefte hebben aan een instantie die namens hem nagaat of de uitvoering van de verschillende taken geschiedt overeenkomstig de gegeven richtlijnen; er is dus behoefte aan controle.
Evenals bij de financiële administratie is het aan te bevelen deze controle te laten verrichten door een extern deskundige, dan wel intern een afzonderlijke functie hiermede te belasten.
Vooral daar door de Wet grote waarde wordt toegekend aan zelfregulering lijkt het vanzelfsprekend dat binnen de organisatie wordt gecontroleerd of de intern opgestelde richtlijnen ook worden nageleefd.
Een interne controle- of interne accountantsafdeling zou in samenwerking met de externe accountant deze taak op zich kunnen nemen.

Het NIvRA-bestuur heeft over de onderhavige materie een studierapport vastgesteld, getiteld "Privacy-bescherming en accountant".

# SAMENVATTING VAN DE 2e OESTERREICHISCHER DATENSCHUTZTAG GEHOUDEN VAN 24-26 MAART 1982 TE LINZ (OOSTENRIJK)

door A.W. Neisingh

Het programma van de conferentie zag er als volgt uit:

1. Woensdag 24 maart een drietal inleidingen te weten
   - Aktuelle Fragen des Datenschutzes door de Staatssekretaer im Bundeskanzleramt Prof. Dr. A. Nussbaumer;
   - Europaeische Datenschutzerfahrungen door H. Burkert (Gesellschaft für Mathematik und Datenverarbeitung te Bonn);
   - Forderungen an eine umfassende Novellierung des Datenschutzgesetzes door Dr. K. Bednar (Informations-berater te Wenen).

2. Donderdag 25 maart een zestal workshops (parallel) over de volgende onderwerpen:
   a. Forschung und Datenschutz;
   b. Datensicherung;
   c. Oeffentliche Verwaltung und Datenschutz;
   d. Internationaler Datenfluss;
   e. Personalinformationssysteme en
   f. Medien und Datenschutz.

   Een korte beschrijving van de in deze workshops behandelde problematiek en een literatuurverwijzing is in AC-documentatie opgenomen.

3. Op vrijdag 26 maart volgde een rapportering uit de verschillende workshops, alsmede een samenvatting van de resultaten.

De conferentie was bijzonder geslaagd. Deelnemers (in totaal 71) kwamen vrijwel alle uit Oostenrijk en de Bondsrepubliek Duitsland.

## Aktuelle Fragen des Datenschutzes

Prof. Nussbaumer benadrukte in een bijzonder goede voordracht de problematiek van de bescherming van (persoons)gegevens ten gevolge van de in omvang en ingewikkeldheid toenemende automatisering (zoals integratie van voorheen zelfstandige processen/bestanden, het gebruik van de huiscomputer, de mogelijkheden van tekstverwerking met directe toegang tot operationele gegevensverzamelingen).

Als aandachtsgebieden voor een (betere) bescherming van (persoons)-gegevens noemde hij

- het bijbrengen van bewustzijn bij de mens met betrekking tot de bescherming van gegevens;
- het treffen van preventieve maatregelen in organisatie en systemen;
- het zoeken naar nieuwe mogelijkheden om tot adequate bescherming van gegevens ook in de toekomst te komen;
- controle.

Verder stond hij stil bij noodzakelijke verbeteringen in de huidige Wet en bij grensoverschrijdend gegevensverkeer.
Over dit laatste onderwerp werd opgemerkt, dat er een spanningsveld bestaat met andere landen in verband met afwijkende regelingen ten aanzien van grensoverschrijdend gegevensverkeer.
En dit ondanks dat andere landen ook reeds regelingen op dit punt hebben getroffen. Hij benadrukte dat bilaterale overeenkomsten wellicht noodzakelijk blijken te zijn.
Overigens stond hij wel stil bij het onderscheid of gegevens over de grens worden uitgewisseld

- binnen éénzelfde onderneming (bijvoorbeeld een multinational) of
- tussen verschillende ondernemingen (bijvoorbeeld een Oostenrijkse onderneming die zijn geautomatiseerde gegevensverwerking in het buitenland - bijvoorbeeld bij een servicebureau - laat uitvoeren).

N.B.: Spreker bleek ook op de hoogte te zijn van het Nederlandse ontwerp van Wet op persoonsregistraties. Hij refereerde namelijk aan de toelichting op art. 3 lid b, waarin wordt gesteld dat "persoonsregistraties die naar hun aard voor persoonlijk of huiselijk gebruik zijn bestemd", zoals dagboeken en verjaardagskalenders die veelal in toiletten zijn opgehangen, niet onder de werking van de Wet vallen.

## Europaeische Datenschutzerfahrungen

Herbert Burkert startte zijn inleiding met het geven van een overzicht van

- landen binnen Europa waar een privacywetgeving van kracht is; alsmede van
- landen waar dat nog niet het geval is.

(In het tijdschrift Transnational Datareport wordt regelmatig een bijgewerkt overzicht opgenomen.)
Ook de door de Raad van Europa en de OECD gesanctioneerde documenten werden vermeld.

Burkert signaleerde vervolgens een aantal praktische problemen, zoals:

- het volledig kunnen voldoen aan inzage- en correctierecht, alsmede de voorgeschreven protokolplicht;
- de (bureaucratische) opstelling van Overheden, wanneer vergunningen dienen te worden afgegeven en dergelijke;
- de "ongrijpbaarheid" van de ontwikkelingen in de automatiseringstechnologie en
- de moeilijkheid tot een vertaling te komen van de wet in praktische maatregelen (wat is de invloed van de Wet op de organisatie, op systemen en dergelijke).

Al met al een goede schets van de problemen waarmee bedrijfsleven en overheid worden geconfronteerd bij de implementatie van de Bundesdatenschutzgesetz (BDSG).

Forderungen an eine umfassende Novellierung des Datenschutzgesetzes

Herr Dr. Bednar sprak zijn teleurstelling uit over het feit dat de Wet in Oostenrijk niet erg aanspreekt; er zijn nauwelijks discussies, publicaties en dergelijke. (N.B.: Aan de zogenaamde "Bürgerversammlung namen slechts ca. 20 personen deel, waarvan 15 congresgangers.)
Spreker ging naast enige praktijkgevallen/-problemen in op de noodzakelijk geachte Novellierung.
(Praktijkproblemen: te vernietigen bestanden worden niet vernietigd; het inzagerecht ten behoeve van Kirchensteuer wordt nu een kopierecht; enz.)

Met betrekking tot de noodzakelijk geachte verbeteringen van de wet noemde Bednar onder meer:

- definiëring van begrippen, omdat vele misverstanden ontstaan;
- beperking van (bureaucratische) handelingen, zoals de zeer uitgebreide registratie in een Datenverarbeitungsregister;
- het verwijderen van verwijzingsfouten en inconsequenties uit de Wet;
- het vastleggen van rechten van de geregistreerden onder de term freedom of information (de vergelijking met de Nederlandse wet Openbaarheid van Bestuur kan worden getrokken);
- het opleggen van beperkingen aan de opslag van gegevens in personeelsinformatiesystemen;
- het verbeteren van de procedure met betrekking tot de verplichting gegevens te verwijderen.

Een overigens interessante discussie ontspon zich over de prijs die de geregistreerde moet betalen, indien hij van zijn inzagerecht gebruik wil maken.

Onder het motto "het zijn toch mijn eigen persoonsgegevens" werd iedere vergoeding van de hand gewezen.

Indien toch een vergoeding wordt gevraagd, rijst de vraag of de geregistreerde afhankelijk van verwerkingswijze of opslagmethodiek van de gegevens, een lage danwel hoge prijs moet betalen!

Workshop 4: Internationaler Datenfluss

Een gehele dag hebben de 11 deelnemers aan deze werkgroep de problematiek van het grensoverschrijdend gegevensverkeer besproken. De aanwezigen hadden verschillende achtergronden, te weten Datenschutzbeauftragter (bij Hoechst en Lufthansa), juristen (chemische industrie en auteursrechten), IBM (2x), waarvan één contactpersoon met het Oostblok, Bureau van de Bundesbeauftragter für den Datenschutz, management automatisering, adviseurs.

In de Oostenrijkse DSG worden in Abschnitt 4 de artikelen 32, 33 en 34 de internationale aspecten geregeld.
De exacte tekst is hierna opgenomen.

4. Abschnitt

INTERNATIONALER DATENVERKEHR

Voraussetzungen für Ueberlassungen von Daten in das Ausland

§ 32 1. Die Ueberlassung von automationsunterstützt verarbeiteten Daten aus Oesterreich durch die in den §§ 4, 5 und 17 genannten Rechtsträger in das Ausland ist unter den in § 7 oder § 18 genannten Voraussetzungen zulässig. Sie bedarf der Genehmigung der Datenschutzkommission.

2. In folgenden Fällen bedarf jedoch die Ueberlassung durch unter den 3. Abschnitt fallende Rechtsträger keiner Genehmigung der Datenschutzkommission:
   1. wenn es sich um Ueberlassungen von Daten des Auftraggebers als Betroffenen handelt, oder
   2. wenn die Ueberlassung in einen Staat, in dem auf die Daten ein diesem Bundesgesetz vergleichbarer Datenschutz Anwendung findet, erfolgt, oder
   3. wenn dies in völkerrechtlichen Vereinbarungen vorgesehen ist.

3. Eine nach Abs. 1 notwendige Genehmigung ist zu erteilen, wenn
   1. nicht öffentliche Interessen einschliesslich völkerrechtlicher Verpflichtungen entgegenstehen, und
   2. die Uberlassung den Erfordernissen des § 7 oder § 18 entspricht, und
   3. glaubhaft gemacht wird, dass durch die Ueberlassung in das Ausland schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden, und

4. soweit eine Ueberlassung in das Ausland zum Zwecke der Verarbeitung als Dienstleistung (§ 19) erfolgt, durch entsprechende Vereinbarungen sichergestellt wird, dass den Bestimmungen des § 19 entsprochen wird.

4. Soweit gemäss §§ 8 oder 23 eine Registrierungspflicht besteht, bedürfen auch Ueberlassungen in das Ausland einer Registrierung (§ 47 Abs. 4 und 5).

5. Durch Verordnung des Bundeskanzlers ist nach Anhörung der Datenschutzkommission festzustellen, inwieweit eine Gleichwertigkeit ausländischer Datenschutzbestimmungen (Abs. 1 Z. 2) gegeben ist. Dabei ist insbesondere auf die Wahrung der schutzwürdigen Interessen der Betroffenen Bedacht zu nehmen.

Verarbeitung in Oesterreich für das Ausland

§ 33 Die Verarbeitung von Daten in Oesterreich für ausländische Rechtsträger ist dem Datenverarbeitungsregister zu melden (§ 47 Abs. 4 und 5). Sie unterliegt einer Genehmigung der Datenschutzkommission, soweit dies in völkerrechtlichen Vereinbarungen vorgesehen ist.

Direkter zugriff zu Daten

§ 34

1. § 32 findet auch Anwendung, wenn nur ein Arbeitsgang der Verarbeitung im Ausland oder für das Ausland stattfindet oder ein direkter Zugriff auf im Bundesgebiet gelegene Anlagen der automationsunterstützten Datenverarbeitung aus dem Ausland möglich ist.

2. Wenn vom Bundesgebiet aus ein direkter Zugriff auf in Anlagen der automationsunterstützten Verarbeitung im Ausland gespeicherte Daten möglich ist, findet § 33 Anwendung.

De in de artikelen besproken aspecten kunnen als volgt worden weergegeven:

1. Ueberlassung verarbeiteter Daten ans Ausland.
2. Ein Verarbeitungsschritt im Ausland.

§ 32

3. Verarbeitungsschritt für das Ausland.
4. Direct Zugriff vom Ausland auf Oesterreichische EDV.

5. Verarbeitung fürs Ausland in Oesterreich.

§ 33

6. Direct Zugriff von Oesterreich auf EDV im Ausland.

Uit de artikelen 32, 33 en 34 blijkt dat Keine Genehmigungspflicht noodzakelijk is, ingeval:

- Auftraggeber = Betroffene.

Oder - Gleichwertigkeit ausländischer Datenschutzbestimmungen (inmiddels in Oesterreich geregeld in Bundesgesetzblatt vom 30.12.1980).

Oder - Völkerrechtliche Vereinbarungen vorgesehen.

Van Genehmigungsanspruch is sprake ingeval:

- Gesetzliche Pflicht.

Oder - Ausdrückliche schriftliche Zustimmung der Betroffene (d.h. Notlösung).

Oder - Berechtigter Zweck.

Oder - Ueberwiegende berechtigde Interessen e.Dr.

Oder - Anonymisierung.

Und - öffentliche Interessen Volkerrecht.

Und - Betroffene oder Beeintragter.

Door IBM werd stilgestaan bij het probleem van de Wartungsdaten (onderhoudsgegevens), die via RETAIN/RSF naar een IBM-computer in het buitenland worden gezonden.
IBM heeft voor dit doel een vergunning aangevraagd en gekregen van de Datenschutzkommission.
Overeenkomstig 32, lid 3 punt 4 moeten individuele ondernemingen met IBM-centra waar deze gegevens worden verwerkt, regelingen treffen.

Overigens werd opgemerkt dat IBM via RSF in staat is, bijvoorbeeld bij leesproblemen met vaste schijven, de gehele inhoud van de schijf af te halen!
In dit kader werd opgemerkt dat zoveel mogelijk Anonymisierung van gegevens doelmatig is.

Eén van de aanwezigen wees ook bij de bespreking van dit onderwerp weer op onduidelijkheden in de wettekst, zoals ten aanzien van de term Uebermittlung.

Door mij werd weergegeven wat in het Nederlandse wetsontwerp op de persoonsregistraties is opgenomen met betrekking tot grensoverschrijdend gegevensverkeer.
Hierover handelt afdeling 6, welke hierna integraal is opgenomen.

Afdeling 6: Internationale aspecten

Artikel 88

1. Deze wet is mede van toepassing op zich in het buitenland bevindende persoonsregistraties van een in Nederland gevestigde houder.

2. Artikel 25, tweede lid, en paragraaf 6 van afdeling 3 zijn ten aanzien van de in het vorige lid bedoelde persoonsregistraties niet van toepassing.
De Registratiekamer kan in verband met in het buitenland geldende wetgeving ontheffing verlenen van andere bepalingen van deze wet.

Artikel 89

1. Bij algemene maatregel van bestuur kunnen afwijkende regels worden gesteld omtrent de inschrijving in het register van persoonsregistraties waarvan de houder in het buitenland is gevestigd.

2. De Registratiekamer kan ontheffing van bepalingen van deze wet verlenen indien de bescherming van de persoonlijke levenssfeer bij een in het vorige lid bedoelde persoonsregistratie voldoende is gewaarborgd.

Artikel 90

1. Artikel 83, eerste lid, is van overeenkomstige toepassing ten aanzien van de toegang vanuit Nederland tot persoonsregistraties waarop deze wet niet van toepassing is.

2. Het is een ieder verboden om vanuit Nederland gegevens te verstrekken aan of te betrekken van een persoonsregistratie waarop deze wet niet van toepassing is, voor zover bij algemene maatregel van bestuur is verklaard dat die verstrekking of dat betrekken ten aanzien van die persoonsregistratie of de groep van persoonsregistraties waartoe die registratie behoort niet is toegestaan omdat daardoor de persoonlijke levenssfeer van geregistreerde of te registreren personen ernstig kan worden benadeeld.

(N.B.: Onderstreping van schrijver dezes.)

Overigens passeerden de revue

- Guidelines van de OECD. Gesuggereerd werd deze guidelines als uitgangspunt te gebruiken bij bedrijfsregelingen (zou in VS reeds geschieden).

- Document van de Raad van Europa, dat echter nog in geen enkel land geratificeerd blijkt te zijn.

- Te verwachten EEG-regelingen, waarvan de inhoud niet bekend was.

- SITA-netwerk, waarvan luchtvaartmaatschappijen gebruik maken. Als uitkomst van een conferentie van SITA-gebruikers zou het ondergeschikt maken aan nationale wetgevingen zijn bekrachtigd.

Tot slot werd het probleem van Datenoasen aangetipt.

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

BOEKEN

AC-Documentatie AS026

door J. Philippo

Pitfalls in Distributed Processing.
James Martin extracted from the book
"Design and strategy for Distributed Data Processing".

This chapter, extracted from the book, summarises some of the pitfalls in DDP, those pitfalls can be avoided if the move to DDP is managed appropriately.

If top management is not involved in data processing, it is likely that the full advantages will not be achieved because of corporate politics and lack of corporation wide perspective among the groups who install local systems.

Management strategy

Minicomputers and other small machines will proliferate, playing a vital role in data processing.
Some measure of centralized design and control is needed.
Determining these measures is part of the strategic planning needed for DDP.

At the top of the list of pitfalls is the absence of management control. In some corporations it is too easy for many user departments to obtain incompatible machines.
The entire distributed configuration needs to be planned.

Data design

A major danger in distributed development is that the data in different locations are designed by the different unco-ordinated teams. The same data are represented in many different ways. At a later time, when it is necessary to use the data in a control system extremely expensive conversions are needed.

Low-level software

In practice many minicomputer installations with low-level software have achieved results much faster then large installations with sophisticated expensive software, because of the simpler overall operation, avoidance of complex systems programming and the dedication of the user-groupstaff. Peripheral application development can be made easier if the peripheral machines are linked to a central data base and the developers are given powerfull languages for generating applications which use or update the data.

Unprofessional implementation

Often minicomputer development is unprofessional, standards are not followed, structured programming is not used.
Reorganization, new products and general business changes bring the need to revise the programs, restructure the data or change the hardware or software.

Maintenance

This term is used to refer to the adjustment of existing computer programs and facilities.
Systems can be designed to minimize the maintenance costs. This requires complex software, including database management systems which derive multiple different user views of data from a given database, and data-communications software which derives virtual circuits.

Escalating complexity

While the first applications on a minicomputer may be easy to install, the addition of further applications leads to greater complexity and rising costs.
Computer security is a complex subject, but where appropriate techniques are applied computer installations can be made appropriately secure. However, it is rare to find good security in peripheral end-user installations; tight securing requires the professional security management that is found in some centralized installations. This security management can be extended to the periphery of a distributed system.
Auditors claim that some distributed systems are unauditable, there is no audit trail with which an auditor can reconstruct the history of who entered what transactions into a terminal or changed what records.
Audit trails or archival information can be stored more economically on a central system because of economics of scale in storage.
It is necessary to ensure that the auditors' requirements are met in the initial overall design of a distributed system.

Network incompatibility

In a large corporation it is desirable to have a corporate network. Independently and randomly selected user machines will not all plug into a common network without substantial conversion expense. Often the spread of distributed computer occurs before the network is planned. The two should be planned in an integrated fashion.

Planned evolution

The growth of networks is one form of evolution of distributed facilities.
Unplanned evolution necessitates conversion operations. Spontaneity and flexibility are needed in information systems, and they are the promise held out by terminals, networks, distributed intelligence, and databases. However, DDP with conversion problems is not going to achieve that promise.
A corporation may become filled with incompatible systems using incompatible data - a mess too expensive to straighten out.

Cheap minis, desk-top machines etc. give user groups the ability to break away from the domination of central DP organisations. At the same time, data networking gives the ability to move to a head office some computing functions previously done in subsidiaries or divisions.

## Conclusion

Processing modes at end-users' locations give a suitable degree of autonomy to the end users. These modes fit into an overall system designed to give centralized control of those factors where this is benefical.
The interactions between the modes are kept simple, thus lowering the overall system complexity, but the modes conform to requirements necessary for networking, database operations and interchange of data.
The maximum use is made of software which gives spontaneous access to data, report generation and higher application development productivity.
The system is designed to be auditable and suitable secure.

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

# Tijdschriften

Gedurende enkele jaren heeft J.C.P.M. Vermeeren een waardevolle bijdrage aangeleverd voor deze rubriek. Van harte dank daarvoor. Inmiddels heeft de Redactie van Compact twee medewerkers bereid gevonden hem op te volgen.

De samenstelling van het nieuwe redacteurenteam van de rubriek "Tijdschriften" zal zijn mw. D. Jansen Heytmajer, J.L.H. Kooijman en drs. B.M. de Vries.

## A PENETRATION ANALYSIS OF A BURROUGHS LARGE SYSTEM

UNIVERSITY OF CANTERBURY, NEW ZEALAND,
OPERATING SYSTEMS REVIEW vol. 15 nr. 1 january 1981

AC-Documentatie S803
Trefwoorden B43 B31

door mw. D. Jansen Heytmajer

### Introduction

A penetration analysis attempts to assess how secure a system is against deliberate attempts to use it in an illegitimate manner.

This paper describes a penetration analysis of the Burroughs B6700 computersystem at the University of Canterbury.
The software system was Burroughs' 3.0 P.R. # 1 release.

The aspects chosen for investigation were:
a. File Security.
b. Resource Limits.
c. Accounting Methods.
d. Disruption.

### a. File Security

The B6700 file security relies on distinctions between ordinary users and privileged users, privileged programs and operating system tasks.
Ordinary users are subject to strict security controls, but the last three categories have unrestricted access to file data.
The hardware restricts memory access within bounds set by the compilers. The filesystem allows only valid compilers to create or alter machine-code files.
It also controls the creation of new compilers.

Possible Flaws.
No flaws were found in the control exercised by system software over user attempts to manipulate the disk file system directly.
There are powerful protection mechanisms for controlling access to disk- and tapefiles; there is a high probability of detecting attempts at unauthorized access.
As with many systems, password stealing represents a serious threat.
The standard software gives the central site operators privileged status for file access. Where this is considered to be inappropriate it could be readily withdrawn.

Successful Penetration.
An ordinary unprivileged user with sufficient knowledge of the system needs only the ability to be able to modify machinecode in order to penetrate the system completely.

This ability is provided because the system allows code files to be loaded from storage on magnetic tape.
Although the Burroughs software, which transfers files between tape and disk storage does use complex protective structures, there is nothing to prevent a knowledgeable user from initiating these structures and creating arbitrary code files which the Burroughs system will load and execute.

Remedies.
The only complete remedy is to deny unprivileged users the ability to load code files from demountable tape or disk pack.

b. Resource Limits

Code execution is based on the concept of a task. A task may initiate further tasks. If so appropriate limits are transferred to the new tasks. The standard compilers restrict access to the structures from user programs.

Possible Flaws.
If a task can execure uncontrolled machinecode, the system can no longer enforce control over it. Protection of the run-time system is completely dependent on control over the code which is executed.
In case of batchwork, the independent job is assigned to limits, taken from the initiating job (which runs as the highest level task). However in case of CANDE work (work initiated through the terminal system) there is no individual job task for each user sharing the system and appropriate limits are not applied.
The resources remaining for the initiating task or job are transferred to the new task when it is initiated, but the resources used by each task are debited to the job when the task terminates. By initiating new tasks and holding nearly completed tasks in a wait state to prevent them terminating, it is possible for the total resources used by all the tasks to exceed the intended limits.

c. Accounting Methods

An accounting package is used which utilizes the standard Burroughs intrinsics and userdata file structures to maintain its database. The database is updated automatically at job completion and by account entry and reporting packages.
All these programs are protected by the normal file security system against unauthorized use.

Passwordsecurity.
Passwords are held in the userdata file in a hashed form. Only privileged users can read records other than their own, ordinary users may not even alter their own records by direct access to the file.

The terminal system logs unsuccessful attempts to find passwords and deactivates the terminal if several occur in succession.
The run-time system terminates any task which tests an invalid password.

Task Resource Accounting.
The accounting system relies on resource usage as logged by the operating system when each task is completed. The system successfully resists attempts to change these usage variables directly.

Total Penetration.
Any privileged user has complete access to the file system, including the accounting system.
Once code is adequately protected there is a need to bring the privileged users and tasks within the same kind of structure security system as currently controls non-privileged users.

d. Disruption

Files and accounts could be compromised or destroyed and the run-time system sabotaged.
This section considers other disruptive mechanisms.
Physical disruption could be caused by external factors or by internal factors.
Software disruption may occur in any of the following situations, a system crash, pre-emption of resources or a deadlock situation.
Psychological disruption may be caused to either users or operators of the system by activities other than disrupting the system itself.
Generally the system was well-protected against disruption. The major risk was that a password could be stolen and used to disguise the real author of anti-social activities.

Conclusion

Non-total forms of penetration met with very limited success. The security of the controls on code validation and privileged users are interdependent. A breach of either gives total penetration.
The system is theoretically wide open to complete penetration through the insecurity of code files on magnetic-tape.

Lente 1982

LES RISQUES DU TRAITEMENT INFORMATIQUE;
EVALUATION ET CHOISE DES CONTROLES

André Pérès
L.Sc.Comm.,
L.Sc.Compt., C.A.

CA Magazine/août 1981

AC-Documentatie S793
Trefwoord B48 (enkele tableaus zijn in de tekst afgedrukt)

door J.C.P.M. Vermeeren

Welke risico's worden acceptabel gevonden en hoe wordt een aanvaardbaar compromis gevonden tussen de aanwezige risico's en de kosten om zich er tegen te beveiligen.

Het antwoord op deze vraag is doorgaans tweeledig:
1. een analyse van de risico's;
2. een kosten/baten-analyse, die leidt tot de meest efficiënte beveiligingsaanpak.

In het artikel wordt een aantal technieken besproken, die voor de gestelde uitgangspunten nuttig kunnen zijn.

Het artikel is ingedeeld in de volgende paragrafen:
- de aard van het risico;
- de kwantitatieve benadering;
- de kwalitatieve evaluatie van de risico's;
- keuzemodel voor beveiligingsmaatregelen;
- conclusie.

## De aard van het risico

De aard van het risico wordt besproken aan de hand van onderstaand Tableau I.

**Tableau I**
**Composantes des risques du traitement informatique**

| *Agents de risques* | *Événements* | *Dommages/Valeurs* | | | *Conséquences* |
|---|---|---|---|---|---|
| | | *Données* | *Logiciel* | *Matériel* | |
| Personnel | Erreurs humaines | Altération | Altération | | Utilisation d'informations inexactes |
| | Défaillances des appareils | | | | Perte d'éléments d'actif |
| | Actes illicites (fraudes, vol, vandalisme, etc.) | Perte ou destruction | Perte ou destruction | Perte ou destruction | |
| Matériel | Sinistres (incendie, inondation tremblement de terre, etc.) | Divulgation | Divulgation | | Retard dans la production des informations |
| Agents externes | Autres | | | | Utilisation illicite d'éléments confidentiels |

Bij het schatten van de schade die uit een gebeurtenis voortvloeit moeten alle kosten, materieel en immaterieel worden betrokken. Onder de immateriële kosten valt bijvoorbeeld ook de schade, ontstaan door misbruik van uit concurrentie-oogpunt belangrijke gegevens door concurrenten.

Bij de taxatie kan men werken met een verschillende mate van detail. Wij onderscheiden:
- uitgaan van alle mogelijke combinaties van veroorzakers/gebeurtenissen;
- uitgaan van meer gestandaardiseerde gebeurtenissen die verder individueel worden bezien;
- of direct uitgaan van de gevolgen. Naarmate de analyse complexer wordt zal het resultaat in nauwkeurigheid toenemen.

Bedacht moet worden dat de preventieve maatregelen vaak gericht zijn op de veroorzaker en in mindere mate op de gebeurtenissen zelve.

De methoden van risico-analyse kunnen worden onderscheiden in kwantitatieve en kwalitatieve methoden.
In beide benaderingen spelen de volgende grootheden een rol:
- de absolute frequentie (hoe vaak zal een gebeurtenis zich in een gegeven periode voordoen);
- het verlies per gebeurtenis;
- het verlies per periode.

De kwantitatieve benadering

Hieronder worden twee methoden beschreven:
a. De empirisch statistische.
b. De "IBM"-methode.

Ad a.

Een voorbeeld van de empirisch statistische benadering is samengevat in Tableau III.

Deze methode schat de toekomstige verliezen per specifieke mogelijke gebeurtenis op basis van historische gegevens. Deze moeten bekend zijn danwel worden getaxeerd. De schatting geschiedt met behulp van kansrekening. Voordeel is dat naast de gemiddelde verliezen per jaar, ook de deviatie van dat gemiddelde in termen van kansrekening gedefinieerd worden.
De berekening van het totaal maximale verlies kan in termen van waarschijnlijkheid worden uitgedrukt. Dit is met name interessant bij de bepaling van het door middel van assurantie te dekken risico.

Hiertegenover staat als nadeel dat historische gegevens lang niet altijd beschikbaar zijn of voor de toekomstverwachting niet als uitgangspunt aanvaardbaar zijn.

**Tableau III**
**Calcul de la distribution des pertes totales annuelles dues à des destructions accidentelles d'un fichier maître**

***1. Distribution de la fréquence absolue des destructions accidentelles***

| Nombre de destructions par année | Probabilités |
|---|---|
| 0 | 0,2 |
| 1 | 0,4 |
| 2 | 0,4 |

Espérance mathématique = 1,2

***Distribution des pertes unitaires dues aux destructions accidentelles***

| Montant en $ | Probabilités |
|---|---|
| 5 000 | 0,5 |
| 10 000 | 0,5 |

Espérance mathématique = 7 500 $

***2. Distribution des pertes totales annuelles dues aux destructions accidentelles***

| Montant en $ | Probabilités* | Probabilités cumulatives |
|---|---|---|
| 0 | 0,2(a) | 0,2 |
| 5 000 | 0,2(b) | 0,4 |
| 10 000 | 0,3(c) | 0,7 |
| 15 000 | 0,2(d) | 0,9 |
| 20 000 | 0,1(e) | 1 |

Espérance mathématique = 9 000 $ — Écart type = 6 583 $

* Calcul des probabilités de pertes totales annuelles dans l'hypothèse de l'indépendance des événements

Soit T = la perte totale annuelle
F = la fréquence absolue
et PU = la perte unitaire ($PU_1$ et $PU_2$ respectivement pour la 1re et la 2e destruction, le cas échéant)

(a) $P(T = 0) = P(F = 0)$ = 0,2

(b) $P(T = 5\,000) = P(F = 1) \times P(PU = 5\,000) = 0,4 \times 0,5$(**) = 0,2

(c) $P(T = 10\,000) = [P(F = 1) \times P(PU) = 10\,000] + [P(F = 2) \times P(PU_1 = 5\,000) \times P(PU_2 = 5\,000)] = (0,4 \times 0,5) + (0,4 \times 0,5 \times 0,5)$(**) = 0,3

(d) $P(T = 15\,000) = [P(F = 2) \times P(PU_1 = 5\,000) \times P(PU_2 = 10\,000)] + [P(F = 2) \times P(PU_1 = 10\,000) \times P(PU_2 = 5\,000)] = (0,4 \times 0,5 \times 0,5) + (0,4 \times 0,5 \times 0,5)$ = 0,2

(e) $P(T = 20\,000) = P(F = 2) \times P(PU_1 = 10\,000) \times P(PU_2 = 10\,000) = (0,4 \times 0,5 \times 0,5)$ = 0,1

** Explication de certaines équations

(b) Pour que la perte totale annuelle soit de 5 000 $, il faut n'avoir dans l'année qu'une seule destruction et que cette dernière entraîne des dommages évalués à 5 000 $.
(c) Pour que la perte totale annuelle soit de 10 000 $, on peut avoir dans l'année ou bien une seule destruction qui entraîne des dommages de 10 000 $ ou bien deux destructions qui occasionnent, chacune, des dommages de 5 000 $.

Ad b.

De IBM-methode streeft naar een globaler bepaling van de risico's, dan de empirisch statistische methode. Het zoeken naar een grote mate van juistheid vergt te veel tijd bij de analyse en voegt niets wezenlijks toe aan de uitkomsten.

**Tableau IV**
**Tables d'évaluation proposées par Courtney**

| | ***Valeur de v pour la perte unitaire moyenne*** | ***Valeur de p pour la fréquence absolue moyenne*** |
|---|---|---|
| 1 | 10 $ | 1 une fois en 300 ans (100 000 jours) |
| 2 | 100 $ | 2 une fois en 30 ans ( 10 000 jours) |
| 3 | 1 000 $ | 3 une fois en 3 ans ( 1 000 jours) |
| 4 | 10 000 $ | 4 une fois en 100 jours |
| 5 | 100 000 $ | 5 une fois en 10 jours |
| 6 | 1 000 000 $ | 6 une fois par jour |
| 7 | 10 000 000 $ | 7 10 fois par jour |
| | | 8 100 fois par jour |

Formule de calcul de la perte totale anticipée

$$PTA = \frac{10^{(p + v - 3)}}{3}$$

Het verwachte totale verlies wordt afgeleid zoals aangegeven in bovenstaand Tableau IV. Er wordt alleen gerekend in machten van 10.

Voorbeeld

Indien de vernietiging van een (specifiek) bestand naar schatting $ 10.000,-- schade per geval meebrengt en de frequentie wordt geschat op eens per 100 dagen wordt het jaarlijks te verwachten verlies getaxeerd op:

$$\$\ 33.333,-- = \frac{10^{(4+4-3)}}{3} = \frac{10^5}{3}$$

De taxaties berusten op subjectieve overwegingen, waarbij uiteraard van gepubliceerde statistieken gebruik kan worden gemaakt, hoewel het soms niet eenvoudig is de bruikbaarheid daarvan te toetsen. Specialisten veronderstellen dat slechts 15% van de (geconstateerde?) computerfraude bekend is en in statistieken is verwerkt.

De kwalitatieve evaluatie van de risico's

De kwantitatieve benadering blijft een omvangrijk werk omdat vele activiteiten, bestanden en gebeurtenissen in ogenschouw dienen te worden genomen. In feite, echter, zijn lang niet alle activiteiten in de informatieverwerking kritiek. Anderzijds komen bepaalde gebeurtenissen zo vaak voor dat ze een voorkeursbeoordeling verdienen. Met name deze klassering van de risico's heeft bijgedragen aan de kwalitatief genoemde benaderingen.

Het primaire doel is niet het meten van de risico's maar het rangschikken naar prioriteit van onderzoek gericht op het voorkomen c.q. ontdekken en herstellen.

In het artikel worden twee kwalitatieve methoden besproken:
A - Matrix-benadering.
B - Churchman Achoff-benadering.

Ad A.

De matrix-benadering is samengevat in Tableau VI.

Ad B.

De Churchman-Achoff-benadering richt zich rechtstreeks op het mogelijke totale verlies dat uit een gebeurtenis voortvloeit. De frequentie wordt niet expliciet in de beoordeling betrokken. De beoordeling geschiedt in twee fasen:

1. Rangschikking naar het relatieve belang van de mogelijke schade door het toekennen van een verhoudingsgetal.
   Steeds worden twee gebeurtenissen t.o.v. elkaar gewogen.

**Tableau VI**
**Définition des paramètres dans une approche qualitative**

| Codes | *Définition pour la fréquence: F* |
|---|---|
| 0 | Très improbable, ex.: tremblement de terre à Montréal |
| 1 | Très peu fréquent mais possible, ex.: attentat à la bombe |
| 2 | Assez fréquent, ex.: panne de courant |
| 3 | Très fréquent, ex.: erreur de codage<br>erreur de programmation |

| Codes | *Définition de la perte unitaire: P* |
|---|---|
| 0 | Infime, ex.: fluctuation de la puissance, vol d'un disque vierge |
| 1 | Légère, ex.: taux élevé de température ou d'humidité |
| 2 | Sérieuse, ex.: vol d'un fichier de données confidentielles |
| 3 | Catastrophique, ex.: incendie majeur |

**Matrice de classement**

| F \ P | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | (**) | | 11 | 9 |
| 1 | | | 7 | 5 |
| 2 | 12 | 8 | 4 | 3 |
| 3 | 10 | 6 | 2 | 1(*) |

(*) Les chiffres à l'intérieur de la matrice sont donnés uniquement à titre d'illustration et représentent l'ordre de priorité accordé aux événements qui seraient inclus dans la case correspondante.
(**) Les éléments de la partie hachurée ne seraient pas retenus dans l'analyse.

2. In de tweede fase wordt de samenhang van de in fase 1 toegekende verhoudingen getoetst. De verdeling van het beveiligingsbudget geschiedt tenslotte naar rato van de verhoudingsgetallen.

Een en ander is samengevat in Tableau VII.

Nadeel van deze methode is dat bij het toenemen van het aantal te onderscheiden gebeurtenissen het aantal paarsgewijze verhoudingen erg groot wordt (10 gebeurtenissen leiden tot 362.880 te beoordelen verhoudingen).

Ten aanzien van het keuzemodel voor de beveiligingsmaatregelen wordt verwezen naar een eerder artikel van Pérès, waarvan een uittreksel is opgenomen in Compact nr. 23, lente 1981, pag. 44 e.v.

**Tableau VII**
**Méthode Churchman-Ackoff — Exemple d'application**

***1) Évaluation des événements***

| Symbole représentant l'événement | Nature de l'événement | Nombre correspondant à l'évaluation |
|---|---|---|
| E(1) | Incendie majeur dans le centre informatique | 5 |
| E(2) | Erreur de programmation | 4 |
| E(3) | Destruction accidentelle d'un fichier maître | 2 |
| E(4) | Tremblement de terre | 1 |

***2) Équations exprimant les relations entre ces événements***

E(1) < E(2) + E(3) + E(4)
E(1) < E(2) + E(3)
E(1) ⩾ E(2)
E(2) < E(3) + E(4)
E(2) ⩾ E(3)
E(3) ⩾ E(4)

***3) Vérification de la cohérence et correction le cas échéant***

| Équation | Évaluation | Correction |
|---|---|---|
| E(3) ⩾ E(4) | 2 > 1 | Aucune |
| E(2) ⩾ E(3) | 4 > 2 | Aucune |
| E(2) < E(3) + E(4) | 4 < 2 + 1 | E(2) = 2,5 |
| E(1) ⩾ E(2) | 5 > 2,5 | Aucune |
| E(1) < E(2) + E(3) | 5 < 2,5 + 2 | E(1) = 4 |
| E(1) < E(2) + E(3) + E(4) | 4 < 2,5 + 2 + 1 | Aucune |

***4) Résultats corrigés: E(1) = 4 E(2) = 2,5 E(3) = 2 E(4) = 1***

Keuzemodel voor beveiligingsmaatregelen

Aan het slot van het artikel geeft Pérès een cijfervoorbeeld. Hierin weegt men af a. ten opzichte van b.:

a. de kosten die verbonden zijn aan het invoeren van nieuwe beveiligingsprocedures;

b. de benadering van mogelijke schaden in geld uitgedrukt. Grondslag van de berekening is getaxeerd verlies per geval x getaxeerde frequentie van voorkomen.

Conclusie

De conclusie eindigt met een korte beschouwing over dit optimalisatievraagstuk, citaat:
"Même si l'analyse des risques est un effort imparfait, difficile et laborieux, elle n'en demeure pas moins nécessaire car elle permet de fonder le choix des contrôles sur des critères bien comme des administrateurs."

THE EXTERNAL AUDITOR'S REVIEW OF COMPUTER CONTROLS

Charles R. Litecky
Larry E. Rittenberg

Communications of A.C.M., may 1981
AC-Documentatie S 730
Trefwoorden: E60, E58, E59.

door drs. B.M. de Vries

Zowel het computer management') als de accountant zijn vanwege een toenemende behoefte aan controleerbaarheid van de onderneming en vanwege voorschriften van de Foreign Corrupt Practices Act van 1977, meer dan voorheen genoodzaakt tot evaluatie van het stelsel van interne controlemaatregelen betreffende de automatisering. Het artikel heeft ten doel het computer management een overzicht te geven van de reikwijdte en aanpak van het onderzoek naar de automatiseringsorganisatie, zoals die door externe EDP-auditors wordt toegepast. Het computer management kan deze kennis gebruiken voor de eigen analyse van interne controlemaatregelen en voor de voorbereiding van eventuele EDP-onderzoeken. Tevens kan deze kennis gebruikt worden als basis voor accountantsrapporten over het systeem van interne controle. Dergelijke mededelingen worden mogelijk in de toekomst verplicht gesteld.
Centraal in het artikel staan de resultaten van een onderzoek naar de opvattingen van de accountant over het belang van de te onderscheiden interne controlemaatregelen.
Deze opvattingen berusten op ervaring, die accountants hebben met interne controle op automatiseringsgebied. De resultaten van het onderzoek kunnen binnen organisaties gebruikt worden om de zwakke en sterke punten binnen de gegevensverwerking vast te stellen. Ook kan daarmee het overleg tussen computer management en accountants bevorderd worden.

De externe accountant stelt belang in de volgende punten (uit SAS no. 3), die ook binnen de interessesfeer van het computer management liggen:

"1. Errors or irregularities that might occur in the system (for example, transactions may be lost, duplicated, etc.).

2. Controls which might prevent or detect such errors or irregularities.

3. The evaluation of whether or not such controls provide reasonable assurance that the transaction processing objectives are achieved."

---

') In het artikel worden de termen "computer administrator" en "computer management" door elkaar gebruikt. Duidelijkheidshalve is in onze beschrijving voor het laatste begrip gekozen.

Voor de evaluatie van interne controlemaatregelen gebruikt de accountant zowel de positieve als de negatieve benadering. De positieve benadering, ook wel genoemd "objectives approach" houdt in, dat de accountant nagaat of er voldoende interne controlemaatregelen zijn getroffen om aan de gestelde doeleinden van de gegevensverwerking te voldoen. De aanpak bestaat uit interviews, observatie, analyse van system flow charts, e.d.

De negatieve benadering (controle op de volledigheid) verloopt als volgt:

"1. The auditor considers the errors or irregularities that could occur in the system.

2. Establishes whether controls to either prevent or detect such errors or irregularities are, in fact, present.

3. Determines of these controls, working as they are purported to provide reasonable assurance that the desired processing objectives are achieved."

(Vergelijk onze beschrijving van het artikel "Information Systems Audit" uit Compact nr. 25, herfst 1981, blz. 50 e.v.)

Bij deze aanpak worden veelal vragenlijsten gebruikt om de controlemaatregelen te inventariseren en aan te geven welke maatregelen getroffen moeten worden om fouten te voorkomen en op te sporen. De benaderingen vullen elkaar aan; bij de positieve benadering ligt het accent op de controledoelstelling, bij de negatieve benadering op de controlemaatregelen.

Het verschil in benadering tussen externe accountant en computer management is:

"The external auditor's control concerns focus on:

1. The correctness of financial data included on various files and

2. The likelihood that the data processing system is reliable and will remain so for the period under audit. The auditor's view of transaction processing controls starts with transaction origination (including manual processing procedures) and is much broader than simple computer-based functions.

The computer management's concern stands in contrast to those of the auditor, they more fully focus on:

1. Allocation of resources within computer administration.
2. The plan of organization and procedures for developing, documenting and maintaining systems.
3. The security of the data processing resource.
4. Data and processing integrity."

Het onderzoek bestond uit het inventariseren van de belangrijkste maatregelen van interne controle, die bij de 9 grootste CPA firms ten behoeve van de controle geëvalueerd werden. De deelnemers (146) aan het onderzoek werd gevraagd de controlemaatregelen naar belangrijkheid te rangschikken. De resultaten van het onderzoek zijn in de volgende tabel weergegeven:

TABLE I. IMPORTANCE OF COMPUTER CONTROLS.

| Variable | Description of control | Mean | Standard deviation |
|---|---|---|---|
| | *Highly important controls* | | |
| 4 | Program change controls | 6.35 | 86 |
| 20 | Quality of on-line controls | 6.28 | 92 |
| 16 | Segregation of duties | 6.21 | 99 |
| 7 | Input/output control group | 6.08 | 1.21 |
| 13 | Data base management controls | 5.74 | 1.24 |
| 5 | Application validation tests | 5.72 | 1.20 |
| | *Important controls* | | |
| 19 | File protection and backup | 5.64 | 1.56 |
| 3 | Quality of EDP Documentation | 5.48 | 1.15 |
| 8 | Physical access controls | 5.23 | 1.36 |
| 10 | Management support of control standards | 5.19 | 1.35 |
| 9 | Librarian controls | 5.16 | 1.40 |
| | *Moderately important controls* | | |
| 2 | User participation in design process | 4.96 | 1.48 |
| 18 | Quality assurance function | 4.95 | 1.30 |
| 15 | Quality of EDP personnel | 4.74 | 1.44 |
| 11 | EDP internal audit staff | 4.67 | 1.48 |
| 12 | Data base administrator function | 4.64 | 1.56 |
| | *Controls of lower importance* | | |
| 1 | User understanding of EDP | 4.35 | 1.76 |
| 14 | Computer operations administrative control | 4.20 | 1.40 |
| 6 | Responsiveness to user complaints | 3.64 | 1.47 |
| 17 | Long-range EDP planning | 3.53 | 1.46 |

De in de tabel aangegeven standaard deviaties geven aan, dat de waardering van vele van de geselecteerde controlemaatregelen tussen de accountants onderling nogal verschillen.

Opvallend (maar niet verbazingwekkend) is, dat de categorie "Highly important controls" gerelateerd is aan de betrouwbaarheid van een applicatie gedurende een bepaalde periode. De laagst scorende categorie is meer gericht op efficiency en lange termijneffectiviteit van de automatiseringsafdeling.

In het artikel worden de zes hoogst scorende maatregelen van interne controle nader behandeld.

De in het onderzoek geselecteerde 20 interne controlemaatregelen staan echter niet geheel los van elkaar. Tussen sommigen van hen bestaat vanuit het gezichtspunt van de accountant een sterke relatie. Door middel van de statistische data reductietechniek factoranalyse heeft de schrijver getracht de 20 controlemaatregelen te groeperen in 6 categorieën, waardoor de achtergrond van het selectieproces van de accountant duidelijker wordt.

Het resultaat van de hergroepering vindt u in tabel II.

TABLE II. DIMENSIONS OF COMPUTER CONTROLS.

| Dimension | Variable | Description of controls |
|---|---|---|
| | | Factor 1. (% variation = 30.1%) |
| Control consciousness of computer management | 15 | EDP personnel quality (.71 = loading) |
| | 6 | User complaint responsiveness (.65) |
| | 17 | Long-range EDP planning (.59) |
| | 10 | Management control standards (.51) |
| | 18 | Quality assurance function (.49) |
| | 14 | Computer operations control (.41) |
| | | Factor 2. (% variation = 10.8%) |
| Systems integrity and security controls | 20 | On-line controls (.65) |
| | 16 | Segregation of duties (.64) |
| | 4 | Program change controls (.47) |
| | 7 | I/O control group (.41) |
| | 5 | Application's validity tests (.40) |
| | | Factor 3. (% variation = 6.6%) |
| Data base controls | 12 | Data base administrator (.79) |
| | 13 | Data base management systems controls (.71) |
| | | Factor 4. (% variation = 5.7%) |
| Library and physical access controls | 9 | Librarian (.73) |
| | 8 | Physical access controls (.62) |
| | | Factor 5. (% variation = 5.4%) |
| User design participation | 2 | User design participation (.92) |
| | | Factor 6. (% variation = 5.1%) |
| File protection and backup | 19 | File protection and backup (.74) |

Op basis van de uitgebreide interviews met de externe accountants komt de schrijver tot de volgende aanbevelingen ter verbetering van de interne controle.

"1. Carefully supervise and document procedures for approving and making program changes.

2. Closely examine the user area controls surrounding on-line controls.

3. Do not neglect the proper distribution of duties among computer personnel.

4. Continue to emphasize the input/output control group.

5. Allow the data base administrator to be the main interface for the auditor on data base management system control issues.

6. Encourage management to continue emphasizing the traditional controls of validation tests, file integrity, physical access, documentation and library.

7. Support the development of computer auditing.

8. Do not neglect intangibles such as user satisfaction.

9. Use the control dimensions (those factors listed in the previous section) for starting points on control evaluations.

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

# Automatisering Beveiliging Controle NIEUWS

door J.F.C. van Epen en drs. H.C. Kocks

## Automatisering

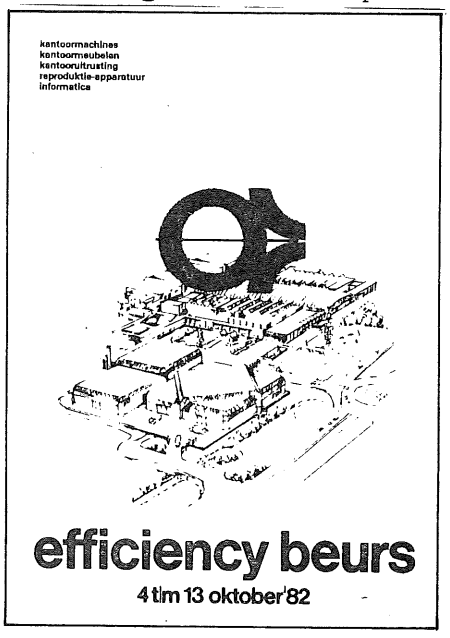
Een belangrijke internationale gebeurtenis, ook voor automatiseringsfunctionarissen, is de jaarlijks in april te houden Hannover Messe. Vele voor- en nabeschouwingen van de Messe '82 zijn inmiddels verschenen.
Omdat op de beurs een aantal opmerkelijke nouveauté's is gelanceerd, waardoor zelfs het automatiseringsjargon weer met enkele termen kan is verrijkt, laten wij uit de nabeschouwing van de Automatisering Gids (28.4.1982) enkele fragmenten volgen.

## Doorbraken op micro-gebied in Hannover

Op de Hannover Messe '82, lagen de accenten vooral op de kleinere apparatuur. Diverse fabrikanten toonden hun nieuwe microcomputer, terwijl aan de onderlinge koppeling van de apparaten de nodige aandacht werd besteed.

Op de Messe nam het CeBIT gebeuren dit jaar een meer beduidende plaats in.
Voor het overgrote deel was hal 3 gevuld met nieuwigheden op het gebied van de microcomputer. Meest opvallend daarbij het Synfobase systeem van AEG-Telefunken, met behulp waarvan een microcomputer een "intelligente database" kan bijhouden. Kern van Synfobase wordt gevormd door het zogeheten "associatieve geheugen".
Dat laatste is een hardware component, ontwikkeld door professor Sydney Lamb uit de VS, waarmee de in een bestand opgeslagen gegevens op hun inhoud aanspreekbaar zijn. Dit maakt een intelligent zoekproces mogelijk.
Vanuit Japan komen er ook de nodige nieuwe ontwikkelingen op ons af.
Epson bijvoorbeeld, komt met een microcomputer ter grootte van een vel A4.

Het apparaat is voorzien van een ingebouwde printer, 16k RAM, 40k ROM, een Liquid Cristal Diode (LCD) afleesvenster, mogelijkheid tot inbouw van een modem, en een minicassette-recorder.
Gewerkt kan worden in de bekende Microsoft Basic. Het apparaat beschikt over een ingebouwde klok met kalender, en de prijs zal rond de 2000 gulden liggen.
Even terug naar Amerika, Commodore toonde een aantal grote micro's, meest aangeduid met de term small-business micro's. Deze vallen uiteen in twee groepen, de 500-serie en de 700-serie.
Eerstgenoemde is in staat kleuren weer te geven op ieder normaal TV-toestel. De interne opslag loopt, afhankelijk van het model, van 64 tot 256 kilobytes.
De 700-serie bestaat uit de tot nu toe grootste micro's in de commodore-reeks. Bij de opzet van de 700-serie heeft men veel aandacht besteed aan ergonomische aspecten. De maximale grootte van het werkgeheugen bedraagt 512 kilobytes.
Niet alleen op microgebied waren de nodige primeurs te bespeuren, ook de "grote jongens" lieten op de Messe duidelijk van zich horen. Zo kwam Digital Equipment met een nieuwe telg in de VAX- serie voor de dag.
Deze nieuwe VAX-11/730 heeft het formaat van een redelijk formaat koelkast, draait onder VAX-VMS en heeft een maximale geheugencapaciteit van 5 megabytes. Communicatie kan plaatsvinden via de volgende protocols: DECnet, 3270 en X.25 packet-switching.
National Advanced Systems annonceerde te Hannover haar nieuwe PCM, de AS 6100-serie. Deze is volledig IBM-compatibel en de twee modellen waaruit de serie tot nog toe bestaat zijn vergelijkbaar met de 4341 model 2 en de 3083.
Het kleinste model draagt de typeaanduiding 6130. Zonder veel moeite is dit model om te bouwen tot de grotere 6150. In de basisconfiguratie beschikken beide modellen over een intern geheugen van 4 megabytes en 6 communicatiekanalen. In de 6100 computers is gebruik gemaakt van speciale chips, de zogeheten customized logic




Ook in Nederland wordt dit jaar weer een aantal belangrijke beurzen gehouden op onder meer automatiseringsgebied. De meest algemene daaronder is wel de Efficiencybeurs, die van 4 tot en met 13 oktober 1982 in de Amsterdamse RAI zal worden gehouden.

In Fem-trends van 4 maart 1982 troffen wij een berichtje aan over een nieuwe prestatie op microgebied.

## IBM-CHIP VOOR 288.000 BITS

Er lijkt geen eind te komen aan de opslagmogelijkheden van bits en chips. IBM onthulde onlangs erin geslaagd te zijn een produceerbare chip te ontwikkelen die 288.000 bits kan opslaan: de informatie die op ca. 25 dichtbetikte vellen staat. Tot dusverre was er sprake van hooguit 64.000 bits, terwijl een 72k-bit in onderzoek was.
De 64k-bit-chip vergt nog altijd niet meer dan het minuscule formaat van 10 bij 6 mm. Een nieuw circuit-ontwerp en nog dunnere bedrading (spoortjes van 2 micron dikte) liggen aan de nieuwe chip ten grondslag. De produktie zal evenals bij de 64k-bit gebaseerd zijn op een grote mate van uitval.
Op dit moment zal slechts 8 à 10 procent van de produktie foutloos zijn. Er worden er gewoon zoveel gemaakt dat er voldoende werkende chips overblijven.

Soms blijkt interessante hulpprogrammatuur te worden ontwikkeld. Onderstaand artikel uit Computerworld van 15 februari 1982 meldt een aantal utilities voor het IBM Systeem 34, die deels voor documentatie- en audit-doeleinden zouden kunnen dienen.

## SCREEN, LIBRARY UTILITIES OFFERED FOR SYSTEM/34

AMARILLO, Texas - DBA Systems, Inc. has introduced four packages for screen and library handling for IBM System/34 users.
DBA-1 is designed to screen catalog information for each file and library residing on disk. It reportedly can be used to check the status of a file at any time.
DBA-2 is a utility that is intended to stop all procedures in a specific library from logging the statements to the system's history file, the vendor said. The start, stop and console messages are still logged, but the individual procedure statements will not be written to the history file. This will reportedly reduce disk read verifies and disk writes.
The third utility, DBA-3, is designed to save user and IBM language libraries residing on disk, with no operator intervention. The procedure reportedly writes to the magazine drive, eliminating the need for the operator to count magazine slots in order to fully utilize all 10 diskettes in a magazine. The second part of this system will condense all user and IBM language libraries with one procedure, the vendor said. Both procedures read the library control sector directly to obtain the needed information.
DBA-5 (4) is said to read a library and produce a set of reports that documents the files, programs and procedures in the library. A flowchart of the procedures is produced, in addition to a cross reference by program and procedure.

Another report documents each file used in the library. The documentation package is said to read any procedure statement without any restrictions concerning the length of the file names.

Ter afsluiting van het onderdeel Automatisering een aantal korte berichtjes en commentaren aangaande IBM produkten, overgenomen uit Update, Xephon Newsletter, March 1982.

### *MVS/XA MAY FORCE CONVERSION TO VSAM*

Large MVS sites with non-VSAM datasets may be in for a nasty surprise in the next few years. When they move to MVS/XA, a forced conversion to VSAM will be necessary-unless IBM changes either MVS/XA or VSAM itself in the near future. This and other potential pitfalls opened up by the MVS/XA announcement are among the issues discussed in IBM '82.

### *THE COST OF MOVING FROM OS/VS1 TO MVS*

As part of its research for the Consultancy Briefing OS/VS1 to MVS, Xephon surveyed all known VS1-to-MVS converts in the UK. Some of the questions asked concerned the cost of the conversion. On average, the move took 2 man years (mostly spent on training operators and programmers), and required additional processing power (0.5 MIPS on average) and main memory (1.8 megabytes on average), as well as an increase in DASD capacity for 60% of sites.

### *4300 NOW OBSOLETE?*

Will the 4300 be replaced this year? Persistent rumours that the new "Olympia" series will be announced in mid-1982 are to some extent supported by the very low purchase: lease ratio of the latest 4300 models (as low as 25:1, compared with original ratios of 39:1). This is frequently a sign of impending obsolescence, as IBM clears its stocks. If so, the resulting drop in residual values will come as an unpleasant shock for users and lessors relying on the usual life-expectancy of about five years. On the other hand, with 4341s still on 12 months' delivery, a 1982 Olympia announcement may not make commercial sense for IBM either.

### *8100 DOWN BUT NOT (YET) OUT*

Out of the 50,000 "first day" orders placed for the 8100 on its launch in October 1978, it is reported that fewer than 1000 have been installed worldwide. Not surprisingly, many observers predict an early retirement for what has proved an embarrassing commercial flop. Nonetheless, recent enhanced models and new software (DPPX/PDA, DPPX/POF) suggest that at least someone in IBM believes the system has a future.
Users who have based their office automation plans on DISOSS/DOSF will certainly be relieved by any reprieve.

## NEW STORAGE DEVICES COMING SOON

A double-density 3380 with a 4.5-6 MB/second transfer rate, and fast streaming tape drive to back it up, are among the imminent IBM announcements predicted at IBM '82: The Key Questions. Also expected are a 16 megabyte version of the 3880-11, supporting twice as much DASD storage and effectively permitting the use of 3380s as paging devices, a solid-state drum using the reputedly discredited bubble technology, and a 96-megabyte "internal" paging device for the 3081.

## WHO NEEDS WATER COOLING?

Air-cooling is one of Amdahl's main selling points against the 3000 series, but one user found that the only way he could cool the motor that drove the fan to cool his Amdahl was to plumb it into the water-cooling of his 3033!

Some commentators believe that the heat emission on the 3081 is low enough to dispense with plumbing altogether. If so, why does IBM specify that water-cooling is needed? Virtually all current 3081 prospects already have plumbing installed, so IBM is not losing any sales advantage by specifying watercooling; on the other hand, 3033 sales might suffer if users believed that the cost of installing plumbing would be entirely wasted when the time for an upgrade came.

**Beveiliging**

Vorig jaar ontdekte men bij Wells Fargo Bank in de Verenigde Staten een computerfraude van 65 miljoen gulden. Het besef dat er nog meer computermisdaden worden gepleegd, die veelal onopgemerkt blijven, doet twijfelen aan de houdbaarheid van de wijsheid dat misdaad niet loont.
Dat de bestrijding van computermisdaad wel loont, is inmiddels geen punt van discussie meer. Eind maart 1982 organiseerde Cii Honeywell Bull een congres over computerbeveiliging en privacybescherming.

Uit het verslag dat hiervan in Computable verscheen (2 april 1982) citeren wij de volgende passages.

# Belang van adequate gegevensbescherming wordt alom ingezien

"Honderd procent zekerheid betekent nul procent produktiviteit." Aldus een van de ruim tweehonderdtwintig deelnemers aan het onder auspiciën van de onlangs door de Franse regering genationaliseerde computeronderneming Cii Honeywell Bull georganiseerde congres Top Secret '82. Voor de tweede maal vond deze bijeenkomst plaats, volgens velen in de wandelgangen in een wat soberder sfeer dan vorig jaar.

Dat het belang van gegevensbeveiliging steeds meer wordt ingezien werd op het congres Top Secret '82 wel duidelijk. Het accent verschuift daarbij steeds meer van de beveiliging tegen fraudeurs en andere kwaadwillende geesten naar het tegengaan van de totale ontregeling van computersystemen door meer prozaïsche aangelegenheden als brand of overstroming. De gevolgen van zulke verschijnselen kunnen inderdaad nogal diep ingrijpen in een organisatie.

Dr. Kenneth Wong, voorman van de Britse deskundigen op het gebied van computer- en gegevensbeveiliging, schilderde ze met verve.
Zo duurt volgens hem het vervangen van een om een of andere reden teloorgegaan computersysteem minstens twee weken, maar meestal langer; vooropgesteld dat de betreffende apparatuur inmiddels niet is verdwenen uit de leveringsprogramma's, één van de redenen overigens om apparatuur regelmatig te vernieuwen. Maar met nieuwe apparatuur is men er vanzelfsprekend nog niet. Volgens Wong is er veel

inspanning en overwerk voor nodig om nieuwe apparatuur binnen twee weken weer helemaal aan de praat te krijgen. Voordat een organisatie helemaal over de gevolgen van zo'n ramp heen is zouden nog drie tot negen maanden verstrijken.

Dat zoiets een organisatie niet in de koude kleren gaat zitten laat zich raden. Vooral bij commercieel opererende organisaties komt dat tot uiting in forse verliezen. Een leverancier van landbouwchemicaliën zag zijn administratiesysteem in rook opgaan en moest gedurende lange tijd wekelijkse verliezen van vijf tot tien miljoen gulden incasseren. Een bierbrouwerij kampte een half jaar lang met verliezen die van een nog grotere orde waren en zag na die tijd zijn marktaandeel aanmerkelijk gereduceerd. Zulke aanslagen kunnen de doodsteek voor een onderneming betekenen.
Het is dan ook duidelijk dat een organisatie zich moet wapenen tegen rampen met het computersysteem en de gevolgen daarvan.
Wong propageert dat - met name grotere - organisaties een van de leidinggevenden belasten met de coördinatie van de opvang van de gevolgen. Hij moet daartoe van tevoren een plan opstellen. Niet alleen de "wederopbouw", maar ook de directe opvang moet daarin worden geregeld. Voor deze laatste kan de hulp worden ingeroepen van een bevriende onderneming met een rekencentrum - hoewel daarbij volgens Wong talloze problemen van technische aard om de hoek komen kijken - of van de langzaam maar zeker overal van de grond komende speciale ondersteuningsrekencentra voor noodgevallen zoals het onlangs opgerichte Computer Uitwijk Centrum in Lelystad.
Ook zou de installatie van een nieuw computersysteem al van te voren moeten zijn uitgedacht. Wong vindt het niet zo'n gek idee dat een grote organisatie alvast een ruimte reserveert voor de vervangingscomputer, zodat deze al kan worden neergezet voor het oorspronkelijke centrum helemaal op orde is.

Kenneth Wong trok van leer tegen de gedachte dat een gedistribueerd gegevensverwerkend systeem in de regel veiliger is dan een centraal systeem. Volgens hem worden de effecten van koppelingen over het algemeen sterk onderschat. Een calamiteit op een van de punten van een netwerk kan een sneeuwbaleffect elders in het systeem veroorzaken. Tegenover het feit dat een ramp in een gecentraliseerd systeem noodlottiger gevolgen kan hebben staat de gemakkelijker beveiliging van het systeem, vooral tegen allerlei fysieke benaderingen.
Met name over deze fysieke beveiliging onthulde André Sabbe, projectleider bij de bouw van een groot computercentrum van de Belgische verzekeringsmaatschappij Assurances Générales de Belgique, wat zoal de mogelijkheden zijn. Dit nieuwe centrum biedt een staaltje beveiliging die bijna een uitdaging op zich is.
Met behulp van eigen reservoirs voor drie soorten water, in slagorde opgestelde niet-verouderde accu's en halongasinstallaties moet het computercentrum volgens Sabbe nog blijven functioneren wanneer er tegelijkertijd een terroristische aanval met pantserwagens, een explosie gevolgd door brand en een intensieve poging tot storing met behulp van electromagnetische golven plaatsvindt.

Het gebouw kan, met het personeel erin, drie weken achtereen volkomen afgesloten van de buitenwereld blijven bestaan. De strenge beveiligingsmaatregelen verhoogden de prijs van het gebouw met ongeveer een kwart.

## LAP PLASTIC EN SCHAAR

De Amerikaan Robert H. Courtney jr., met een lange staat van dienst in de meer duistere krachten van de gegevensverwerking - voor de Amerikaanse marine, de afdeling "spionagesystemen" van IBM en de opleiding van de FBI - en tegenwoordig aan het hoofd van een eigen adviesbureau, benadrukte het belang van "eerlijke, loyale medewerkers". Een recept voor het selecteren daarvan kon hij niet geven, maar wel wees hij er op dat eerlijkheid en loyaliteit geen blijvende eigenschappen zijn en dat het personeel dus eigenlijk voortdurend moet worden gescreend.

Volgens Courtney ligt het accent bij de computerbeveiliging over het algemeen te veel op het fysieke aspect. Verloren gegane apparatuur kan immers betrekkelijk gemakkelijk worden vervangen, maar "all the hardware in the world can't help you back in the business." Veel vervelender zijn de gevaren die de deskundigheid bedreigen, bijvoorbeeld door het weglopen of onbetrouwbaar worden van personeel. "Een verkoper helpt je zo aan nieuwe apparatuur, maar niet aan nieuwe mensen."

Ook het niveau van de fysieke bescherming baarde Courtney zorgen. Vaak wordt, zo stelde hij, te veel geld uitgegeven aan verfijnde beveiligingsapparatuur, terwijl simpele zaken worden vergeten. Een en ander illustreerde hij met een verhaal over een computercentrum dat tegen brand was beveiligd met behulp van een halongasinstallatie, maar waarboven helaas een dozijn verdiepingen waren uitgerust met een sprinklerinstallatie, zodat het toch nog ontaardde in een waterballet in de computerruimte. En, zo vervolgende hij, men had er geen stuk plastic om de apparatuur waarop het lekwater terecht kwam af te dekken.
De nestor van de computerbeveiliging, Donn B. Parker, leek zijn kruit enigszins te hebben verschoten. Kwam hij vorig jaar nog met geruchtmakende theorieën over oorlogvoering per computer, dit keer presenteerde hij een methode om beveiligingsplannen voor een computercentrum op te stellen. Deze, in alle bescheidenheid door Parker als "de beste methode voor het bepalen van computerbeveiliging" aangekondigde vrucht van een jaar arbeid bleek erop neer te komen dat wordt gekeken naar hoe de beveiliging elders wordt verwezenlijkt.

Met de door Parker "baseline concept" gedoopte methode zet hij zich vooral af tegen de in computerbeveiligingskringen opgang makende kwantitatieve risico-analyse. Bij deze methode wordt er impliciet vanuit gegaan dat elke situatie volkomen op zichzelf bestaat, en dat is volgens Parker verspilde moeite. Veel problemen zijn immers

al in andere computercentra opgelost. Kwantitatieve risico-analyse, een methode die volgens Parker het gevaar met zich meebrengt te worden bedolven onder cijfermateriaal, zou alleen kunnen worden gebruikt voor het oplossen van specifieke problemen die andere computercentra niet hebben. "Het heeft geen zin," aldus Donn Parker, "om problemen die allang zijn opgelost telkens opnieuw met ingewikkelde methoden op te lossen."

Het als uitwijkcentrum te Lelystad gebouwde computercentrum heeft na ruim een jaar leeg te hebben gestaan eindelijk een bewoner gekregen, het Computer Uitwijk Centrum (CUC). In Computable van 5 maart 1982 lazen wij het volgende.

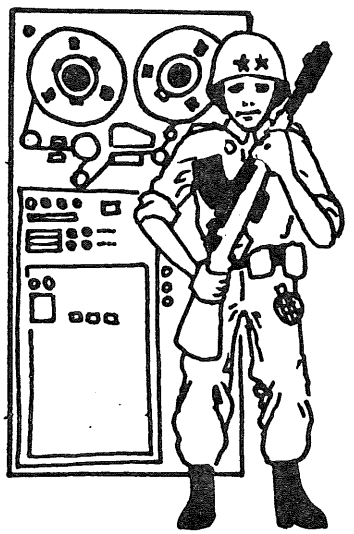
# Computeruitwijk is medio dit jaar ook in Lelystad mogelijk

Het Computer Uitwijk Centrum blijkt eind vorig jaar te zijn opgericht als besloten vennootschap. De deelnemers hierin zijn de Amfas Groep (voor vijftien procent), Delta-Lloyd Verzekeringsgroep (twintig procent), FGH Hypotheekbank (vijftien procent), de KLM (twintig procent) en de Franse Société General de Service et Gestion (SG2) (met dertig procent). Het geplaatste aandelenkapitaal bedraagt drie en een half miljoen gulden.
Dat het servicebureau SG2 in de onderneming participeert, is niet zo verwonderlijk daar het Franse concern in eigen land al ruime ervaring met computeruitwijkcentra heeft. Van de technische en organisatorische kennis van SG2 heeft men in Nederland gebruik kunnen maken.

Het Computer Uitwijk Centrum krijgt slechts één taak, namelijk diegene die in de naam besloten ligt. Instellingen of bedrijven kunnen er dus, wanneer in het eigen rekencentrum een calamiteit zich voordoet, hun gegevensverwerking tijdelijk in onderbrengen. Daartoe zal het centrum worden uitgerust met twee IBM 3033-U computersystemen met elk een werkgeheugen van acht megabytes en een zeer omvangrijke schijven- (waaronder 40 3350's en 32 3330's) en magneetbandconfiguratie. Bovendien is het centrum uitgerust met een voor het doel geoutilleerde reservezaal, waarin onmiddellijk wanneer dit wordt gewenst, een computer kan worden neergezet.

De activiteiten van het Computer Uitwijk Centrum gaan zich niet alleen tot het in handen van FGH zijnde pand beperken. Men wil ook een mobiele uitwijkservice verlenen, waarbij men aan een soort van directiekeet zoals in de bouw wordt gebruikt, moet denken. Deze bij de klant voor de deur neer te zetten "computerkeet" zal naar de wensen en eisen van de klant qua grootte en inrichting worden samengesteld.

Directeur van de nieuwe onderneming is J.L. Nuissl, assistent daarvan J. Kooy. De laatste vertelt dat de start van het centrum - medio dit jaar gepland - nog even afhankelijk is van enige aanpassingen op technisch gebied en het aftasten van de exacte mogelijkheden die men op datacommunicatiegebied zal kunnen bieden. "Datanet-1 (dat begin maart 1982 officieel door de PTT werd opengesteld, red.) speelt bij onze beslissing ook een rol," aldus Kooy.



Controle

In het volgende artikel gaat Bruce Rollier in op de gemeenschappelijke belangen van de data administrator (enterprise administrator) en de accountant in een situatie waar sprake is van gemeenschappelijk gegevensgebruik (data sharing).
De instelling van de data administrator functie wordt bepleit alsmede de inbreng van de accountant (of edp-auditor) als het om controle-aspecten gaat.

Niet voorbij dient te worden gegaan aan het feit dat Rollier aan data administration een ruime interpretatie geeft.
Het artikel wordt onverkort overgenomen omdat het in een "nutshell" de problematiek van data administration en auditor bespreekt.

Data administrators and auditors have many objectives in common. Without compromising their operational independence, the two groups can and should work together to achieve them.

# TWO TEAMS, ONE GOAL

BY BRUCE ROLLIER

In most companies, data administrators have been frustrated in their attempts to move toward long-range goals like a high degree of data sharing or significant reductions in maintenance programming. It takes several years to realize these objectives, and few managements are willing to commit the resources for a payoff so far in the future, particularly when the potential benefits are so uncertain.

At the same time, auditors often encounter great difficulties in coping with the rapid growth and increasing complexity of data processing. Real-time systems, database management systems, distributed processing, and other innovations make it increasingly difficult to audit "around the computer". The ideal auditor is generally expected to have a strategic understanding of the business and an encyclopedic knowledge of the detailed procedures and data, as well as expertise in auditing techniques, internal controls, probability, statistics, data analysis, and fraud detection. Now, in addition, auditing "through the computer" is necessary, so the auditor has to develop even greater breadth of data processing expertise than the increasingly specialized systems professional. The auditor must know hardware operations, operating systems, database management systems, distributed processing and distributed databases, systems programming, and applications programming.
Obviously, not many people possess such a wide range of skills. The emerging specialty of edp-auditing helps alleviate the problem, but this is not a total solution; the edp-auditor still needs an extensive repertoire of skills.

Another auditing concern is that many computer applications are developed without adequate controls. Usually this is not discovered until after implementation, when fixing the problem costs much more than it would have during development. In fact, it may be so expensive to impose effective controls after the system is in operation that it is no longer cost-justifiable. A frequently proposed solution is to assign experienced auditors to application development projects. But besides being very expensive, this can compound the problem of finding enough skilled people.

Auditing and data administration (which is used here to include not only database administration but also such functions as planning and database architecture) are distinct functions, and should remain organizationally independent of each other. Despite dissimilarity in day-to-day tasks, however, there is a surprisingly high degree of commonality in their major objectives. Without compromising their operational independence, these two groups can and should jointly develop complementary long-range strategies that accomplish these objectives much more effectively than separate strategies.

## DEVELOP CONTROLS EARLY

The data administration staff is responsible for the integrity of the corporation's data, and is concerned with adequate controls to prevent unauthorized modifications to the databases, preserve data security and privacy, ensure that output is consistent with input, and provide effective backup and recovery facilities.
Auditors may have additional concerns that do not involve databases, but they are certainly interested in all of the above. The Foreign Corrupt Practices Act of 1977 (which requires greatly increased emphasis on internal accounting controls and imposes penalties against company officials found responsible for the loss of company assets owing to inadequate controls) has made good control even more important.

Both data administrators and auditors recognize that it is impossible to control the dp environment adequately by means of spot checks; effective controls must be built into the daily routine as integral parts of the information system. They must be established early in the development cycle, not tacked on after implementation.

The old concept of an "application owner" who is responsible for controls and for data integrity is no longer viable. As data flow from an order entry system to a sales record system to an inventory system to an accounts receivable system, and on to perhaps dozens of other applications, there is no way an individual application owner can control them. Controls must be established at a level high enough to track data through these processes. The data administrator and the edp-auditor have the required perspective; the application owner and the project development manager do not.

The auditing staff is best qualified to determine what types of controls are necessary. Data administrators can provide expertise on how best to implement the controls, particularly when the environment includes a DBMS. The two departments can jointly develop standards to ensure compatibility of controls across systems. A data dictionary can be valuable here to control data and track relationships, to store edit rules, and to map field-level or segment-level sensitivity indicators.

Both data administrators and auditors must thoroughly understand the dp environment. Both must be able to navigate the system, and to understand what happens to the data at each step. At minimum a good audit trail should allow one to track any piece of data from source to output, or from output to source. (Wenselijker is om over beide audit-trails te kunnen beschikken (RED.).)

The data dictionary can be particularly valuable in achieving auditability objectives because it helps the auditor understand the operational systems and the relationships between entities. It also improves data consistency and controls data definitions.
"Where used" information in the dictionary can simplify determination of the impact of audit-recommended modifications to application systems - an important factor in deciding whether to implement the recommendations.

There is a catch, however: these are only potential advantages of the dictionary; they won't happen without careful planning. For most current users, the dictionary is primarily a support tool for the DBMS. Very few attempt to use it for modelling the current or future environment or as a central documentation source. Auditors cannot expect the dictionary to provide these capabilities unless they activily participate in planning for them. Managing the dictionary is clearly a data administration function, but auditors should have influence in the following:

- design of naming standards and some usage standards;
- establishment of effective enforcement procedures for the standards;
- storage and maintenance of clear, unambiguous data definitions and an accurate set of attributes;
- implementation of adequate security procedures over dictionary data, with good internal control.

CHANGE NOW, SAVE LATER

One of the major justifications for establishing the data administration function is programmer productivity, which can be achieved primarily through data independence and reduced maintenance programming. There are also productivity benefits from the dictionary and from rules-driven languages.

Data administrators proclaim integration to be their number one goal, but few of them have made any noticeable progress toward it.

Auditors' interest in productivity is less direct, but nevertheless very important. A number of studies clearly indicate that modifications to application systems are inexpensive in the early phases of development, but become many times more costly later in the development cycle. One IBM study showed that a change to a program after implementation costs more than 30 times as much as it would have if the change had been made during the coding phase. If the contemplated share is the addition of a control, and if the decision is based on potential risk minus control cost, it is clearly much more difficult to justify adding the control after the project has been completed. Controls established as a part of system design, rather than patched in later, will be more operationally effective and many times more cost-effective.

But can the right controls be put in place early in the project? There are several alternatives:

1. Require that an experienced auditor be part of the application development project team. A number of companies have adopted this approach, and for some it has worked well. It can be quite expensive, however, if there are many separate projects, and it is difficult to find enough experienced auditors with the requisite systems design and auditing skills. Also, the special assignments can interrupt career paths.

2. Rely on the regular system design personnel and let auditors and application owners review each phase for proper controls, provision for audit trails, backup and recovery plans, and effective testing. This is the most widely used approach, and the results are generally poor. Project personnel are concerned with the amount of work finished by the target date; they are not accustomed to being measured on the adequacy of controls or even on the effectiveness of a test plan.
   There may be a low level of understanding of good internal control concepts. Much work may be accomplished between phase reviews, so that after the review it may already be too expensive to make the needed changes. In addition, it is extremely difficult for auditors and users to understand a project well enough by review time to devise effective recommendations. When the information systems staff is resistant to making changes, auditors and users may not be persuasive enough to sell the recommendations.

3. Use database administrators already heavily involved in the project to ensure inclusion of the needed controls, audit trails, recovery facilities, and other capabilities. Here again, data administrators and auditors have similar object-

have a longer-term and higher-level perspective than the typical project manager, and are more concerned with how a new application fits into the present and future dp environment. With the data dictionary, data administration can provide clear documentation and improved system understanding. Auditors and users should continue to be involved in phase reviews and in establishing control standards, reviewing the test plan and test results, etc. This should result in more complete and more effective controls, established earlier and therefore at a substantial saving.

## *IMPROVING THE DATABASE*

We in data administration often proclaim integration to be our number one goal, although few of us are making any noticeable progress toward it. While we have done little to make the concept comprehensible or to justify it as a goal, it is extremely important, and we will have to find ways to persuade the rest of the world of its significance. Fundamentally, integration reduces the total database to a more manageable size, and it can greatly improve data consistency. It simplifies the dp environment by greatly reducing the number of interfaces between files; as the number of files increase, the number of potential interfaces increase much more rapidly. Interfaces between files are established by programming, and all those programs have to be maintained. A change to one key file may necessitate changes to a large number of interface programs. Thus, in many dp environments, integration can substantially reduce programming maintenance.

Integration may be even more important to the auditor, or at least to the corporate controller, than to the data administrator. If a number of redundant files are separately maintained (probably a very common situation), there are often people whose job it is to reconcile the differences between files. In some organizations many people are engaged full time in just that kind of reconciliation, and they aren't needed after the redundancies are eliminated Also, having one file instead of many redundant ones to represent an asset is probably better protection for the asset. The data dictionary can provide information about the degree of redundancy as it is gra lly eliminated.

The major goals of data administration - increased programmer productivity through data independence and greater data integrity through data integration - have proved extremely difficult to attain. They require a substantial up-front investment, scarce skills, the imposition of standards and other restrictions, and more dependence on planning. Benefits may be far in the future and difficult to quantify. What often happens, therefore, is that data administration does not receive the management support it needs.

But the fact that the objectives are difficult to achieve does not make them any less valid; it simply means that we must find better approaches than we have up to now. The organization that elects not to integrate its data today is electing to let uncontrolled redundancy proliferate. The interfacing and integrity problems will get steadily worse and efficiency will decline. Making the start toward an integrated environment will be more difficult the longer it is postponed, and it cannot be postponed indefinitely.

Although this dilemma cannot be solved easily, there is one approach worth trying: build support within other organizational functions. A well-planned data administration program can provide control and auditability benefits in the short run and help justify management support while establishing the bases for longer-range goals. The key tool here is the data dictionary.

Since control and auditability are major audit objectives, the auditing function can and should provide strong support. Auditors should recommend or even demand that the data administration function be established, with the skills and resources, time, and management backing it needs to accomplish its objectives. The auditing department should also participate in developing those aspects of data administration planning which involve control and auditability, particularly the data dictionary plan. Since the areas of cooperation would involve only planning tasks, this recommendation should not seriously affect operational independence. Auditors should understand that their support is essential, and can lead to a more efficient, less complex, better controlled dp environment.

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

## ONDERWIJS

### Cursussen 1982

De nieuwe brochure 1982 is verschenen.

Uit de inhoud citeren wij:
- Inleiding;
- Programma;
- Algemene informatie en reserveringsvoorwaarden.

Ons Bureau Opleidingen zal u gaarne een brochure toezenden.
U kunt daartoe schrijven of telefoneren naar
Klynveld Kraayenhof & Co.
Bureau Opleidingen
Postbus 7137
1007 JC AMSTERDAM
Tel. 020 - 5410541 (na 1 juli 1982: 5469111) waar u kunt vragen naar Pien Meijer.

# Inleiding

Klynveld Kraayenhof & Co. is een groot Nederlands accountantskantoor. De werkzaamheden, die variëren van controle van jaarrekeningen tot adviseren op bedrijfseconomisch, organisatorisch, administratief en fiscaal terrein worden uitgevoerd voor een brede schakering bedrijven en instellingen, nog startend, groeiend of sinds jaren gevestigd. Cliënten zijn zowel ondernemingen in de industrie, handel en transport als dienstverlenende bedrijven, non-profitorganisaties en instellingen alsmede overheidslichamen.

Door onze relaties wordt in toenemende mate een beroep gedaan op het in onze werkuitvoering verkregen inzicht in de bedrijfsproblematiek. Immers, ondernemingen en organisaties staan voor vraagstukken van complexe aard, waarvoor niet altijd de benodigde kennis en ervaring in voldoende mate in eigen kring aanwezig zijn.

Om te voldoen aan de behoefte van de leiding en de medewerkers van onze relaties om in veranderende situaties en voor bepaalde vakgebieden en onderwerpen te worden ondersteund bij het beter doen functioneren van de eigen organisatie heeft KKC een cursuspakket ontwikkeld.

De cursussen worden gegeven door in de praktijkuitoefening van KKC werkende accountants en adviseurs, waardoor een gerichte overdracht van kennis en ervaring mogelijk wordt.

Naast het geven van een standaardcursus uit het cursuspakket is het ook mogelijk dat een cursus voor een bedrijf of organisatie of voor een bepaalde doelgroep wordt ontwikkeld en gegeven. Een dergelijke maatcursus wordt dan in overleg met de bedrijfsleiding toegespitst op de specifieke vraagstukken van de onderneming.

Nadere gegevens of inlichtingen ontvangt u van
Klynveld Kraayenhof & Co.
Bureau Opleidingen
Postbus 7137
1077 WV Amsterdam
Tel. 020 - 5410541 (na 1 juli 1982: 5469111), waar u kunt vragen naar Pien Meijer.

# Programma

De in deze brochure vermelde cursussen zijn als volgt in te delen:

## Open cursussen

De open cursussen worden op vaste data in de loop van 1982 en de eerste helft van 1983 gegeven. Een volledig overzicht van deze cursussen vindt u op blz. 8.

Voor de open cursussen kan door individuele deelnemers of door een groep uit één organisatie worden ingeschreven. Hiervoor kan gebruik worden gemaakt van de inschrijfformulieren die u achter in deze brochure vindt.

## Maatcursussen

Dit zijn cursussen die naar behoefte van de instelling of onderneming worden toegesneden op de specifieke situatie. Deze bedrijfsgerichte trainingen kunnen zowel extern (bijvoorbeeld in een conferentie-oord) als intern (in het bedrijf zelf) worden gegeven op in onderling overleg overeen te komen data.

De maatcursussen of modules daaruit kunnen tevens worden verzorgd in samenwerking met andere deskundigen, bijvoorbeeld ten behoeve van werkgevers- en branche-organisaties, Kamers van Koophandel, overkoepelende lichamen voor het bedrijfsleven, banken, (semi-) overheidsinstellingen, enz.

# Programma Open Cursussen

| Cursus | Doel en werkwijze |
|---|---|
| Inleiding Administratieve Organisatie | De cursus is gericht op het beheersen van verschillende structuren en processen binnen een organisatie d.m.v. een systeem van informatieverzorging en controle. |
| Inleiding Controleleer | De cursus geeft de hoofdlijnen van de controleleer, aangevuld met groepsgewijze behandeling van vraagstukken en problemen. |
| Aanpak Automatisering | Samenwerking tussen deskundigen en managers maakt het nodig dat er één taal gesproken wordt. Deze cursus vormt de basis voor deze communicatie. |
| Het managen van datacenters | Deze cursus wordt gegeven in samenwerking met RAET-opleidingen en is met name bestemd voor managers van rekencentra en aanverwante afdelingen. |
| Basiskennis Automatisering | Door de behandeling van nieuwe begrippen uit de automatisering wordt een totaalbeeld geschetst van de automatiseringsaktiviteiten, alsmede de invloed daarvan op de accountants-controle. |
| Computer Control | In werkgroepen en plenobesprekingen worden de cursisten vertrouwd gemaakt met controlemaatregelen op het gebied van de automatiseringsorganisatie. |
| Data-entry/batchverwerking | Beoordelen van de interne controlemaatregelen in geval van een systeem met data-entry en batchverwerking alsmede van de aanpak van de accountantscontrole. |

| Tijdsduur, datum | Deelnemersbijdrage |
|---|---|
| 5 dagen<br>4 tm 8 oktober 1982 | f 2.500.- |
| 10 tm 15 januari 1983 | f 2.500.- |
| 5 dagen<br>11 tm 15 oktober 1982<br>15 tm 19 november 1982<br>13 tm 17 december 1982 | f 2.800.- |
| 2 dagen<br>19 en 20 oktober 1982<br>23 en 24 november 1982 | f 980.- |
| 3 dagen<br>21 tm 23 september 1982 | f 1.500.- |
| 4 dagen<br>25 tm 28 oktober 1982 | f 2.000.- |
| 4 dagen<br>1 tm 4 november 1982 | f 2.000.- |

Lente 1982

# Programma Open Cursussen

| Cursus | Doel en werkwijze |
|---|---|
| Kleinschalige automatisering | Verschaft inzicht in de aanpak automatisering in het midden- en kleinbedrijf alsmede in de opzet van het controleplan van de accountant. |
| Inleiding COBOL | Opfrissing COBOL-kennis en behandeling van enige kenmerkende begrippen van belang voor de cursus Geïntegreerde Gegevensverwerking. |
| Geïntegreerde Gegevensverwerking | Beoordeling van de interne controle door middel van de Data Dictionary Directory in een on-line geïntegreerd gegevensmodel. De data-base is hands-on beschikbaar. |
| Management | Het ontwikkelen van een eigen management-conceptie. Dat wil eggen een op zichzelf consistent denkbeeld over doel, rol en techniek van management. |
| Boekhouden | De deelnemers maken kennis met de beginselen van het boekhouden door middel van een combinatie van theorie en opgaven. |

| Tijdsduur, datum | Deelnemersbijdrage |
|---|---|
| 3 dagen<br>14 tm 16 december 1982 | f 1.500.- |
| 1 dag<br>30 november 1982 | f 2.800.- |
| 4 dagen<br>4 tm 7 januari 1983 | |
| 15 tm 19 november 1982 | f 3.750.- (incl. kosten van verblijf in het conferentie-oord) |
| 3 dagen<br>30 augustus tm<br>1 september 1982 | f 1.100.- |

Tenzij anders vermeld zijn prijzen exclusief BTW en verblijf (zie reserverings-voorwaarden op blz. 39 van de brochure Cursussen, mei 1982.

# Algemene informatie en reserveringsvoorwaarden

Alle open cursussen, waarvan de cursusdata in deze brochure zijn vermeld, worden gehouden onder voorbehoud van voldoende deelname.

In de deelnemersbijdragen zijn niet begrepen de eventuele kosten van het verblijf en de maaltijden in het conferentie-oord (tenzij anders vermeld). De kosten van een dergelijk arrangement worden door de administratie van het conferentie-oord bij vertrek met de deelnemers verrekend.

Voor of direkt na de cursus wordt de deelnemersbijdrage door middel van een faktuur in rekening gebracht.

In het algemeen wordt de inschrijving één maand voor de datum van aanvang van de cursus gesloten.

Bij onverhoopte annulering van de aanmelding kan 50 % van de deelnemersbijdrage in rekening worden gebracht. Getracht wordt echter te bereiken dat de opengevallen plaats weer door een andere deelnemer wordt ingenomen.

Voor kosten verbonden aan de annulering van reeds gereserveerde kamers geldt de regeling van het betreffende conferentie-oord.

Wilt u voor iedere cursus een afzonderlijk inschrijvingsformulier gebruiken?

Alle aanvullende informatie kunt u krijgen bij

Klynveld Kraayenhof & Co.
Bureau Opleidingen
Postbus 7137
1007 JC Amsterdam
tel. 020 - 5410541
(na 1 juli 1982: 5469111)