compact

COMPUTER EN ACCOUNTANT

UIT DE INHOUD:

- DE ORGANISATIE VAN GEGEVENSBEHEER
- TOEGANGSBEVEILIGINGSPROGRAMMATUUR
- DATA BASE CONVERSIE

Klynveld Kraayenhof & Co.
ACCOUNTANTS

Internationaal KMG Klynveld Main Goerdeler

NUMMER 26 8E JAARGANG WINTER 1981/1982

UIT DE INHOUD:

- DE ORGANISATIE VAN GEGEVENSBEHEER
- TOEGANGSBEVEILIGINGSPROGRAMMATUUR
- DATA BASE CONVERSIE

Internationaal KMG Klynveld Main Goerdeler

NUMMER 26 8E JAARGANG WINTER 1981/1982

ERRATUM

INHOUDSOPGAVE

BIJ NACONTROLE BLEEK DAT DE INHOUDSOPGAVE NIET MEE AFGEDRUKT WAS. VANDAAR DIT INLEGVEL MET ONZE EXCUSES.

REDACTIE

compact

VAN DE REDACTIE

winter 1981/1982

Dit winternummer van Compact 1981/1982 besteedt aandacht aan de volgende hoofdonderwerpen:

- De organisatie van gegevensbeheer.
  Een korte beschouwing over de organisatorische maatregelen en daarmede samenhangende technische aspecten bij het gebruik van het Information Management System IMS.
  Schrijver A.H.C. Koedijk.
- Toegangsbeveiligingsprogrammatuur. Een vergelijkend overzicht van de verschillende soorten van deze programmatuur. RACF staat hierbij centraal. Schrijver drs. B.M. de Vries
- Data base conversie, een praktijkgeval. A. Kamstra beschrijft de ondervonden problemen hierbij.

De redactie verschaft tevens een compilatie van enige eerste reacties bij het nieuwe wetsontwerp op het gebied van Privacy. Het lag in het voornemen om een samenvatting van de lezing "De invloed van kleinschalige automatisering op de accountantscontrole" te publiceren. Wegens gebrek aan tijd is het verslag nog niet gereed; in het volgende Compact lentenummer zal publicatie plaatsvinden. Inmiddels verwijzen wij naar pag. 39 waar een artikel over minicomputers is overgenomen uit EDPACS. De gebruikelijke rubrieken kunt u wederom in deze Compact aantreffen: Boeken, Tijdschriften, ABC-nieuws, Onderwijs.
Geachte lezer, heeft u commentaar of aanvulling laat het de redactie weten. De redactie stelt gaarne ruimte in Compact beschikbaar.

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.

Reacties op het ontwerp van Wet op de persoonsregistraties

Na het indienen van het wetsontwerp is in de pers een aantal reacties verschenen, die wij hieronder kort weergeven.

Het Parool gaf de reactie van de Stichting Waakzaamheid Persoonsregistratie, die stelde dat de wet te laat komt, 5 jaar na het rapport Koopmans, terwijl er weinig verschillen tussen het rapport en het wetsontwerp worden geconstateerd. Verder is er teleurstelling over de voorgestelde termijn van invoering, 3 jaar.
De stichting verwacht dat het wetsontwerp dan door de technische ontwikkeling zal zijn ingehaald.
Ook in het redactionele commentaar van de Volkskrant klinkt teleurstelling over de trage ontwikkeling. De bescherming, die door de wet zou worden geboden, wordt relatief genoemd.
De effectiviteit van de wettelijke regeling zal moeten komen uit een zo goed mogelijke uitwerking in maatregelen van bestuur en uitvoering.
De NRC (F. Kuitenbrouwer) stelt in een uitgebreid commentaar dat de traagheid in de totstandkoming van het ontwerp niet gerechtvaardigd wordt door een grotere voortreffelijkheid van het wetsontwerp dan de negen Europese wetten die reeds tot stand zijn gebracht.
Er wordt gewezen op de mogelijkheid uitzonderingen te treffen indien dat vereist wordt krachtens een wettelijk voorschrift; daaronder kan heel wat vallen waarop slechts zeer beperkte parlementaire controle is. Een andere uitzondering waarop gewezen wordt is het gegevenstransport binnen een concern, dat zowel omvangrijk als ingrijpend kan zijn.
De nadruk in het rapport Koopmans lag op het registreren, terwijl de oorzaak van privacyproblemen ligt in het vergaren van persoonsgegevens. Aan dit bezwaar wordt in het wetsontwerp slechts gedeeltelijk tegemoetgekomen door introductie van de neutrale term "het aanleggen van persoonsregistraties".
Onzerzijds merken wij op dat ook de term "beheerder van de persoonsregistratie" nadere uitwerking behoeft.
De minister schat dat de wet van toepassing zal zijn op 50.000 à 100.000 persoonsdatabanken. De tien leden tellende registratiekamer zal zich laten bijstaan door tussen de 30 en 60 ambtenaren.
Hoewel accountants deskundigen bij uitstek zijn op het gebied van de administratieve controle en een aantal van hen tevens deskundig is op het gebied van de controle van geautomatiseerde registratiesystemen, heeft de brief van het NIVRA (eindrapport commissie Koopmans pagina 200 t/m 202) geen zichtbare sporen in het ontwerp van wet nagelaten.

Tenslotte: Het NGI organiseert op 26 april 1982 te Amsterdam een symposium onder de titel "De privacywetgeving in de Nederlandse samenleving".

Redactie

compact

winter 1981/1982

DE ORGANISATIE VAN GEGEVENSBEHEER

door A.H.C. Koedijk

1. Inleiding

Integratie van gegevensverzamelingen, waarvan vervolgens gemeenschappelijk gebruik wordt gemaakt, is een doelmatige mogelijkheid om te voorzien in:

- het door verschillende afdelingen nodig hebben van ten dele dezelfde actuele gegevens en
- de behoefte aan bestuurlijke informatie over de afdelingen heen.

Integratie van gegevensverzamelingen biedt voorts betere standaardisatiemogelijkheden van gegevensdefinities, alsmede betere mogelijkheden om gegevensconsistentie te bereiken, doordat de gegevens maar éénmaal ingevoerd en bijgehouden behoeven te worden.

In de automatisering heeft de behoefte aan het gemeenschappelijk gebruik van gegevens geleid tot de ontwikkeling van data base management systemen (dbms): de geautomatiseerde gegevens worden opgeslagen in een data base en bijgehouden/opgevraagd door tussenkomst van het dbms. Door de omvang van het aantal gegevens en door de complexiteit van de relaties tussen de gegevens zullen de gegevens veelal gespreid moeten worden over meerdere data bases. Hierbij zal het soms noodzakelijk zijn gegevens meer dan éénmaal op te slaan, hetgeen de onderlinge consistentie kan aantasten.

Integriteit van gegevens wordt bij het gemeenschappelijk gebruik ervan des te meer een eis; de coördinatie tussen informatieprocessen moet derhalve optimaal zijn.
De integratie en het gemeenschappelijk gebruik van gegevensverzamelingen met de hieruit voortvloeiende vraag WIE, WAT, WANNEER met WELKE gegevens mag doen, noopt tot een centrale beheersing van het gebruik van gegevens; het instrument hiertoe wordt gevormd door metagegevens (gegevens over gegevens).

Dit artikel gaat nader in op de beheersing van het gebruik van gegevens met behulp van meta-gegevens in de situatie met geïntegreerde en gemeenschappelijk gebruikte gegevensverzamelingen. Ten behoeve van een praktische concretisering wordt hier als voorbeeld uitgegaan van een omgeving waar als dbms het door IBM geleverde IMS in gebruik is.

2. Instrumenten ten behoeve van het gegevensbeheer

Globaal kunnen de volgende instrumenten worden onderscheiden:
1. Het gegevensmodel (conceptuele schema).
2. Beschrijving van de gegevensopslag (interne schema).
3. Beschrijving van het gebruik van gegevens (externe schema).

2.1 Conceptuele schema

Het gegevensmodel beschrijft alle gegevenselementen die voor het bedrijf van belang zijn alsmede hun onderlinge samenhang. Gegevens moeten eenduidig worden gedefinieerd qua beschrijving van de inhoud en aard en qua relaties met en afhankelijkheden van andere gegevens.
In principe dient het gegevensmodel de normatieve, op het soort bedrijf (en de omvang ervan) gebaseerde informatiebehoefte als basis te hebben '). De informatiebehoeften van de gebruikers dienen hiervan een afgeleide te zijn.
Toch zullen de informatiebehoeften van de gebruikers ook zelf een basis kunnen vormen voor de bepaling van de informatiebehoefte van het bedrijf, daar bij de gebruikers materie-deskundigheid aanwezig is en omdat bovendien sprake is van niveaus van informatie (relevant voor het bedrijf, een afdeling of voor een persoon). Hier is derhalve sprake van een wisselwerking.

In het model dient tevens te worden aangegeven wie de beheerder is van de actuele gegevens. Gezien het gemeenschappelijk gebruik van gegevens moet als gebruiker-beheerder diegene worden gekenschetst, die als zodanig verantwoordelijk is gesteld. Veelal zal de gebruiker-beheerder benoemd worden binnen het gebied waar de gegevens ontstaan. De beheerderskarakteristiek is voornamelijk van belang met betrekking tot de bevoegdheid tot en de verantwoordelijkheid voor het wijzigen van gegevens (hierin is toevoegen en laten vervallen mede begrepen). De gebruiker-beheerder is verantwoordelijk voor de juistheid, volledigheid en actualiteit van "zijn" gegevens. Ook dient te zijn vastgelegd welke bevoegde gebruikers verder te onderkennen zijn, alsmede welke afspraken tussen en voorschriften voor de verschillende gebruikers bestaan.

De eisen die (ten behoeve van de beschikbaarheid en de wering van onbevoegden) aan de beveiliging van de verschillende gegevens moeten worden gesteld, dienen op basis van het belang voor het bedrijf te worden vastgesteld en vastgelegd in het gegevensmodel.

Het gegevensmodel bestaat derhalve uit een meta-gegevensverzameling. Gegeven de omvang van het model alsmede de complexiteit van het vervaardigen en onderhouden ervan, wordt een onontbeerlijk hulpmiddel hierbij gevormd door de dictionary functies die worden geboden door een Data Dictionary/ Directory System (DD/DS).
Een aantal van dit soort pakketten is op de markt verkrijgbaar. (Verwezen kan o.m. worden naar A Survey of Data Dictionaries, Datamation, maart 1981). De meta-gegevens worden dan opgeslagen in een meta-data base, de dictionary.

Overigens wordt opgemerkt, dat het gegevensmodel naast de geautomatiseerde ook de niet-geautomatiseerde gegevens beschrijft.

') Niet bedoeld is hier de indruk te wekken, dat het opstellen van het model een karwei van geringe omvang zou zijn.

2.2 Interne schema

In de data base worden de actuele gegevens opgeslagen. Het middel voor het definiëren en het onderhoud van de data base wordt geleverd door het dbms, IMS. Voor het definiëren van een data base is een data base definitie (DBD) nodig, waarin opslagstructuur, toegangspaden en dergelijke zijn vastgelegd. Het betreft hier een technische beschrijving (technische meta-gegevens).
De functionaris die een data base definitie verzorgt, dient datgene wat in het gegevensmodel is vastgelegd in technische specificaties om te zetten, hierbij onder meer rekening houdend met de door de verschillende gebruikers gewenste servicegraden (response-tijden). Bedacht moet worden, dat het in de volgende paragraaf aan de orde komende externe schema van invloed kan zijn op de bouw van het interne schema.
Vanzelfsprekend dient bij de bouw van het interne schema rekening te worden gehouden met de beveiligingseisen zoals die in het conceptuele schema zijn vastgelegd; deze eisen worden onder meer in recovery- en reorganisatieprocedures uitgewerkt.

2.3 Externe schema

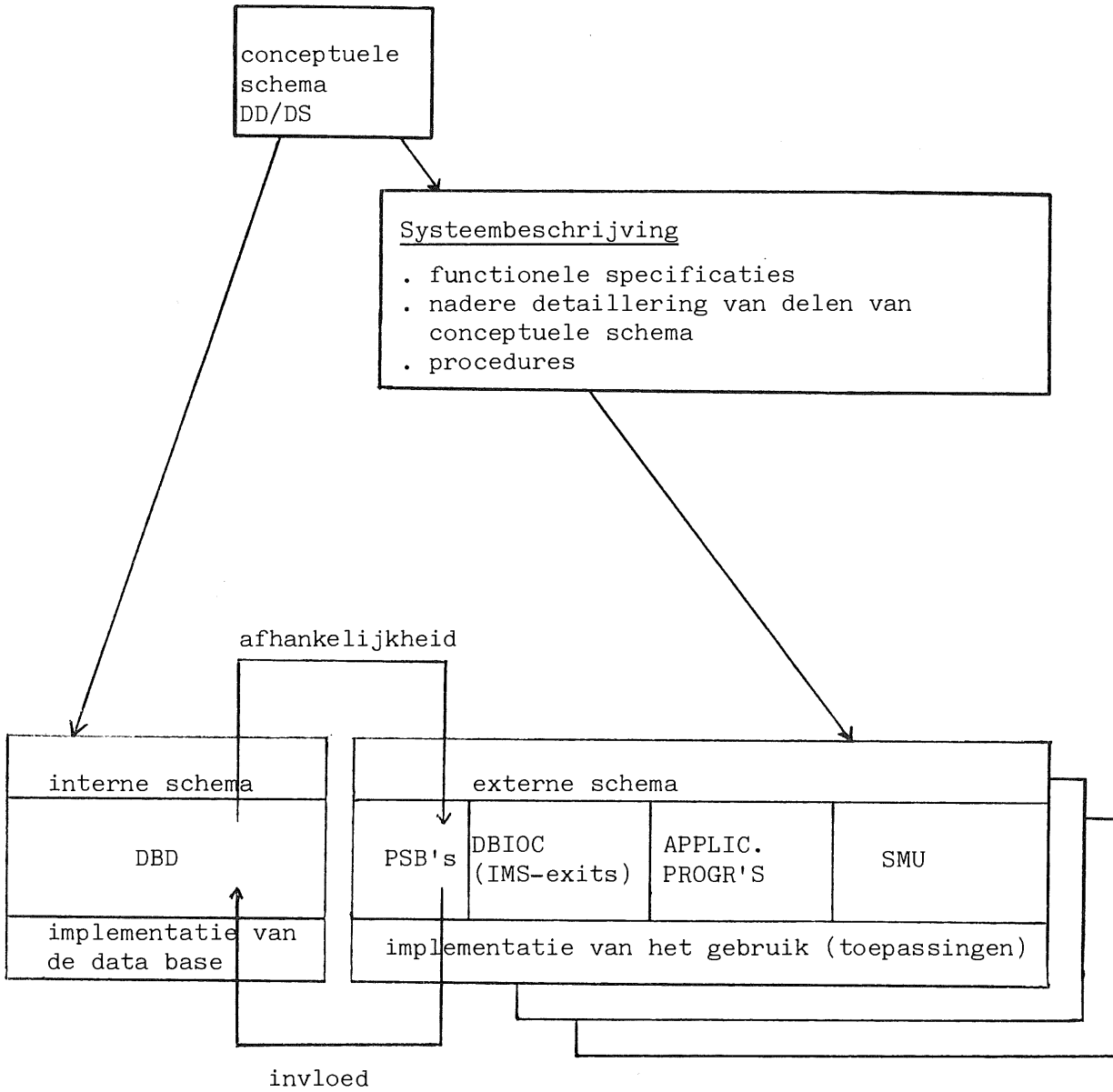
Het gebruik maken van actuele gegevens uit de data base door de afdelingen in het bedrijf geschiedt door middel van applicaties. Door het gebruik van een dbms is sprake van een zekere mate van ontkoppeling tussen de toepassingsprogramma's enerzijds en het aan deze programma's beschikbaar stellen van gegevens uit de data base volgens bevoegdheden (lezen, wijzigen, toevoegen, verwijderen) die ten aanzien van deze gegevens aan gebruikers zijn toegekend, anderzijds. Het "anderzijds" geschiedt door middel van externe schema's, via welke de actuele gegevens benaderd worden.
In een data base situatie met IMS als dbms vormen de Program Specification Blocks (PSB's) één van de middelen voor de bouw en het onderhoud van de externe schema's.

De structuur van de data base (DBD) legt beperkingen op ten aanzien van de mogelijkheden tot definiëring van PSB's. De bouw en het onderhoud van de externe schema's zijn derhalve niet alleen van het conceptuele schema afgeleide, maar ook door het interne schema beïnvloede activiteiten.

Regels en voorschriften ten aanzien van het gebruik van gegevens, zoals die zijn vastgelegd in het conceptuele schema, worden voorts geëffectueerd door middel van specifiek ontwikkelde software (data base input/output controller (DBIOC); in een IMS-omgeving te implementeren door middel van de IMS-exits) en in applicatieprogramma's. Voor de realisering van in het conceptuele schema vastgelegde beveiligingseisen is in de IMS-situatie voorts SMU (Security Maintenance Utility) beschikbaar; hiermee kunnen passwordtabellen worden gebouwd en gevuld alsmede terminalkoppelingen en bevoegdheden worden gedefinieerd. (Van de eventuele aanwezigheid van beveiligingspakketten als RACF en ACF2 wordt hier afgezien; denkbaar is, dat deze programmatuur SMU-functies overneemt.)

2.4 Résumé

Schematisch kunnen de relaties tussen de drie schema's als volgt worden uitgewerkt:



3. Plaats van de functies in de organisatie

3.1 Conceptuele schema

De benaming voor de functie die zich bezighoudt met de bouw en het onderhoud van het gegevensmodel is Enterprise Administrator (E.A.). De functie omvat echter mede het vaststellen en wijzigen van het beleid inzake gegevens en informatie. De beslissingen te dien aanzien en de verantwoordelijkheid hiervoor liggen bij de hoogste leiding, die tevens methodes en procedures ten aanzien van het gegevensbeheer dient vast te stellen.

De functie van de E.A. kan worden uitgeoefend door een onder de hoogste leiding geplaatst staforgaan. Deze afdeling voert dan het feitelijke beheer over de gegevensdefinities, hetgeen in wezen het beheer van het dictionary deel van de DD/D inhoudt. Dit laatste zal met name betrekking hebben op gegevens van hogere niveaus (enerzijds qua mate van detaillering, anderzijds in de betekenis van "relevant voor het bedrijf").

Voor het beheer van definities van gegevens van lagere niveaus danwel nadere detailleringen van gegevens van hogere niveaus zal sprake zijn van delegatie. Hiervoor komen de systeembeheerders') aan gebruikerszijde (die ook reeds applicatieprogramma's beheren) in aanmerking. Ten aanzien van de meta-gegevens vormen de systeembeheerders functioneel onderliggende functies van de E.A. Ten aanzien van het gedelegeerde beheer zullen door de E.A. regels worden gesteld. De naleving van deze regels zal door de E.A. moeten worden getoetst. (Overigens is het denkbaar dat de DBA een dermate grote kennis heeft van het gegevensmodel, dat hij overtredingen van regels reeds vroegtijdig zal kunnen signaleren.)
Door het gemeenschappelijk gebruik van gegevens is het waarschijnlijk, dat er een functionele hiërarchie van systeembeheerders zal ontstaan, namelijk steeds boven de "partijen" staand.
De systeembeheerders zullen gedeeltes van het dictionarydeel van de DD/D beheren (gedeeltes van het conceptuele schema voor zover die binnen het door hen te beheren gebied vallen).

Uit hoofde van de in paragraaf 2.1 vermelde wisselwerking ten aanzien van het conceptuele gegevensmodel (normatieve informatiebehoefte bedrijf versus informatiebehoeften gebruikers) is het aan te bevelen met betrekking tot gegevens en informatie een stuurgroep in te stellen, waarin naast hoofden van afdelingen de E.A. (secretaris) en de hoogste leiding (voorzitter) zitting hebben.

') De systeembeheerder dient te worden onderscheiden van de eerdergenoemde gebruiker-beheerder; de laatste beheert actuele gegevens, de eerste meta-gegevens.

3.2 Interne schema

De benaming voor de functie die zich bezighoudt met de bouw en het onderhoud van het interne schema is Data Base Administrator. In de literatuur en praktijk wordt aan de DBA een veelheid aan taken toegekend; vele hiervan vallen buiten de in dit artikel gegeven typering, met name waar het taken aangaande het conceptuele schema en het beheer van de externe schema's betreft.
Verantwoordelijk voor de materiële inhoud van de data base is de DBA niet; deze verantwoordelijkheid ligt bij de gebruiker-beheerder.

Het bouwen en onderhouden van de data base definitie (DBD) is de taak van de DBA. Hoewel de program specification blocks (PSB's) één van de middelen vormen voor de bouw van het externe schema, is het gezien de wederzijdse invloed van de DBD op de PSB's doelmatig het bouwen en onderhouden van de PSB's eveneens tot de taak van de DBA te rekenen. Vanuit gezichtspunt van interne controle is hiertegen geen bezwaar zolang hier sprake is van een uitvoerende taak. Beslissingen terzake van PSB's dienen te worden genomen door de beheerder van de externe schema's (zie 3.3).
Het doen vervaardigen van de ACB'S (Application Control Blocks, de in de on-line-situatie vereiste, door IMS gecontroleerde combinatie van DBD en PSB's) kan eveneens gezien worden als een uitvoerende taak van de DBA.
Ook het bouwen van de data base input/output controller (DBIOC) kan, door de aard van dit werk, het beste tot de taak van de DBA worden gerekend, evenals het bouwen van password-tabellen met behulp van SMU.

De DBA-functie kan worden ondergebracht in de automatiseringsafdeling. De functie kent echter zowel ontwikkelingsaspecten als operationele aspecten (te denken valt bij voorbeeld ook aan performance aspecten). Om die reden dient de DBA naast de ontwikkelingsfunctie en de produktiefunctie te worden geplaatst.
Een in te stellen procedure dient te bewerkstelligen, dat het werk van de DBA inzake het externe schema getoetst wordt aan het conceptuele schema en de systeembeschrijving door de E.A. en/of systeembeheerders.

3.3 Externe schema

Het beheer van de externe schema's (niet de bouw) en het beheer van de applicatieprogramma's (gebouwd door de ontwikkelingsafdeling van de afdeling automatisering) laten zich het best combineren in de functie van systeembeheerder aan gebruikerszijde. De systeembeheerders dienen ten aanzien van beide beheersaspecten een zekere automatiseringsdeskundigheid te bezitten.
De systeembeheerder neemt met betrekking tot bepaalde gegevens een centrale plaats in ten opzichte van het conceptuele schema, externe schema's, gebruikers, systeemontwikkelaars en de DBA.

Ook het beheer van de inhoud van password-tabellen (met behulp van SMU) kan bij de systeembeheerders worden ondergebracht. De hiervoor benodigde jobs kunnen worden voorbereid door de DBA. Overigens zou het benoemen van een speciale security-officer ten aanzien van het password-beheer een veel sterkere maatregel kunnen zijn.

De mogelijkheden die het masterterminal van IMS biedt terzake van het tijdelijk wijzigen van de beveiliging, dienen in principe uit de software te worden verwijderd. Indien dit in de praktijk tot verstoringen van informatieprocessen zou leiden, dienen beslissingen hierover te worden genomen door de E.A./Systeembeheerders.

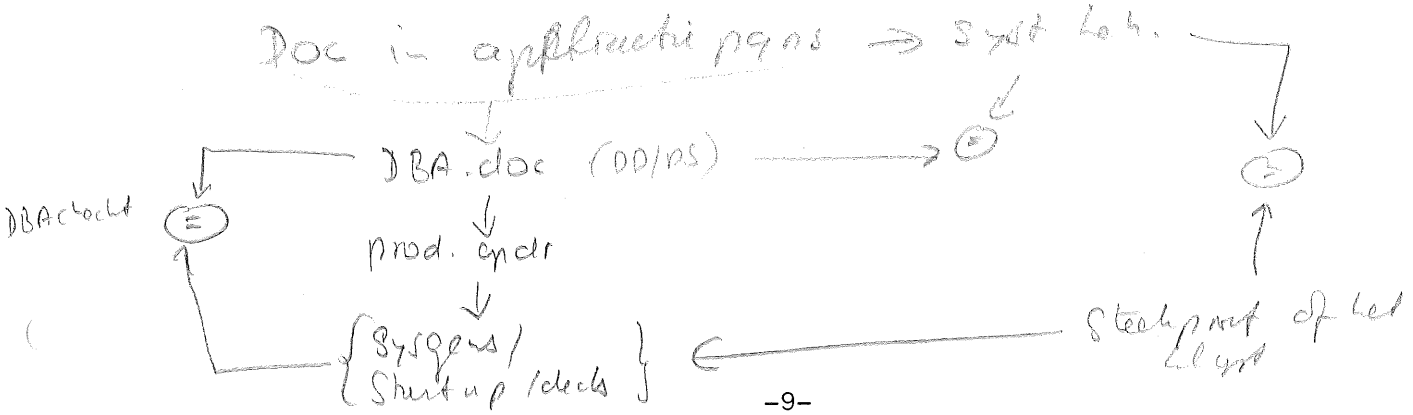
3.4 IMS-beheer

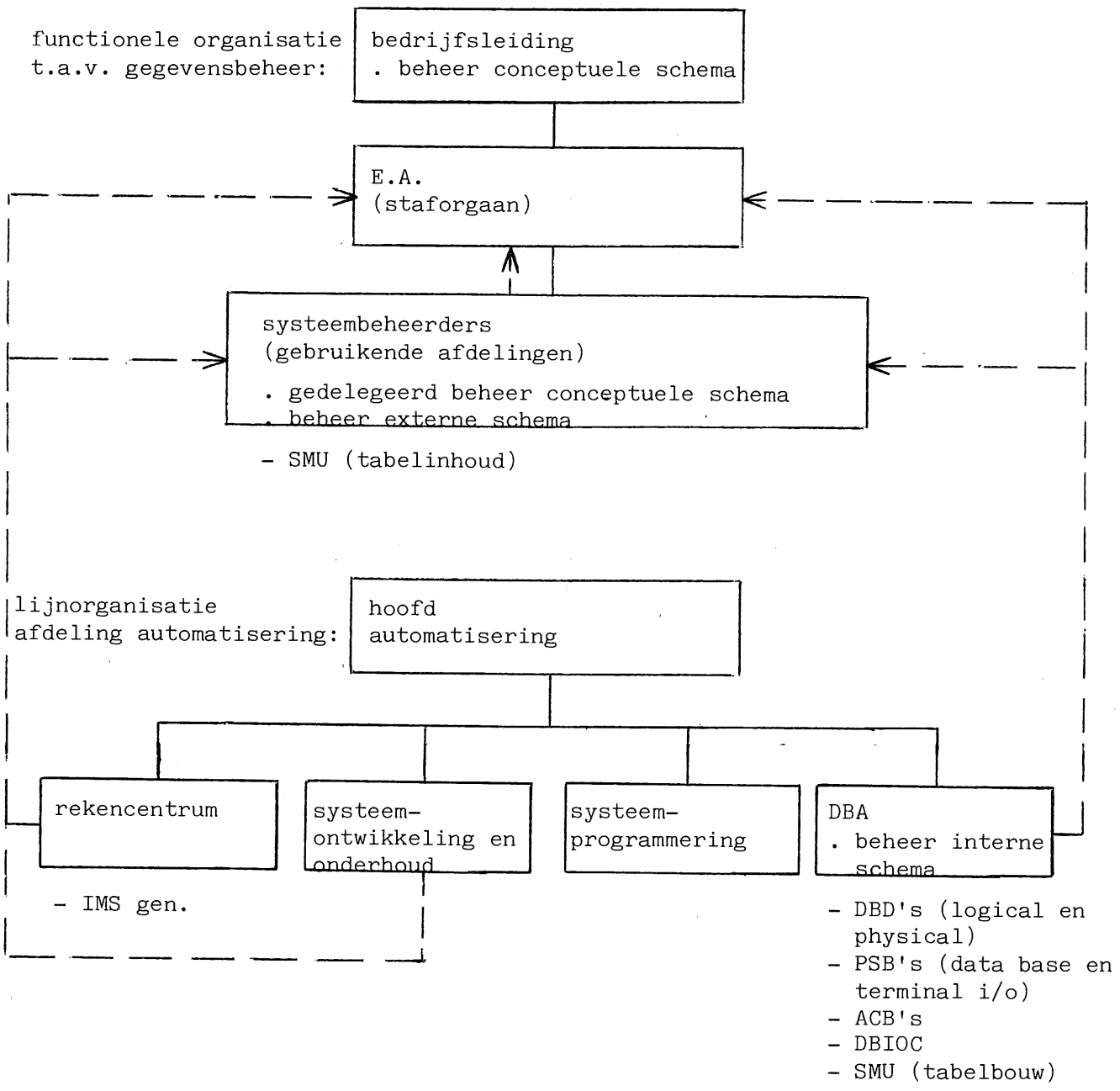
Het daadwerkelijk operationeel maken van DBD en PSB's geschiedt door middel van het bekend maken van DBD- en PSB-namen aan IMS bij IMS-systeemgeneratie. Deze activiteit, voorbereid door IMS-systeemprogrammeurs en DBA, wordt verricht door de produktie-afdeling van de afdeling automatisering (het rekencentrum).

Een procedure dient te bewerkstelligen, dat alleen door de DBA en de E.A. en/of systeembeheerders gefiatteerde interne en externe schema's (DBD's respectievelijk PSB's, DBIOC alsmede ACB's) worden geïmplementeerd. Terzake van de genoemde instrumenten is een goede overdrachtsprocedure van testsituatie bij de DBA naar produktiesituatie bij het rekencentrum noodzakelijk.

3.5 Samenvatting

Schematisch kan het in dit hoofdstuk besprokene als volgt worden weergegeven (de stippellijnen duiden rapportagelijnen aan; de functionele rapportages zullen in een aantal gevallen uit source-listing-achtige computeroutput bestaan).




functionele organisatie
t.a.v. gegevensbeheer:
bedrijfsleiding
. beheer conceptuele schema
E.A.
(staforgaan)
systeembeheerders
(gebruikende afdelingen)
. gedelegeerd beheer conceptuele schema
. beheer externe schema
- SMU (tabelinhoud)
lijnorganisatie
afdeling automatisering:
hoofd
automatisering
rekencentrum
systeem-
ontwikkeling en
onderhoud
systeem-
programmering
DBA
. beheer interne
schema
- IMS gen.
- DBD's (logical en
physical)
- PSB's (data base en
terminal i/o)
- ACB's
- DBIOC
- SMU (tabelbouw)

4. Slot

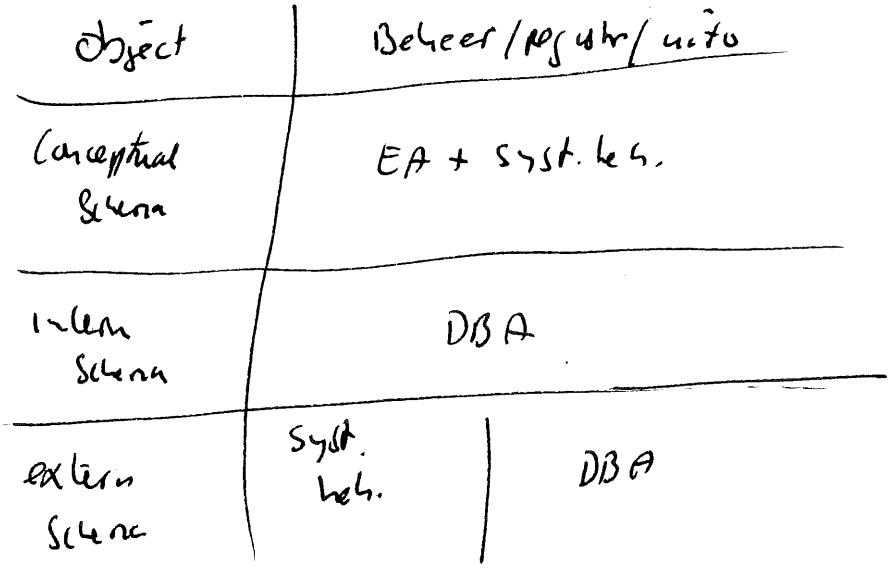
In dit artikel is getracht functies met betrekking tot gegevensbeheer te definiëren en te plaatsen in de organisatie, alsmede aan te geven welke technische gereedschappen gestalte geven aan de instrumenten van gegevensbeheer (uit meta-gegevens bestaande schema's).

De in dit artikel beschreven situatie kan als ideaal worden gekenschetst. In vele gevallen zal naar een dergelijke situatie moeten worden toegegroeid. Hierbij dient de weg van de geleidelijkheid te worden bewandeld. Dienstig lijkt het, dit proces te starten met een gerichte inventarisatie (uitgaande van een globaal informatiebehoefteplan) van aanwezige gegevens in een projectmatige aanpak door de E.A. en medewerkers van de afdeling Automatisering (DBA, informatie-analisten, systeemontwikkelaars). De resultaten van deze inventarisatie dienen door de E.A. te worden verwerkt in een eerste versie van het gegevensmodel.

De functie-uitoefening ten aanzien van gegevensbeheer en de naleving van procedures als in het voorgaande beschreven kunnen controle-objecten voor, indien aanwezig, edp-auditors van een interne accountantsdienst zijn.

In het artikel is uitgegaan van een IMS-omgeving, doch ook bij gebruik van een ander soort dbms (bij voorbeeld Codasyl-systemen), of in een situatie zonder dbms, zal een koppeling tussen de geboden technische gereedschappen en de beschreven drie schema's kunnen worden gelegd.

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



TOEGANGSBEVEILIGINGSPROGRAMMATUUR

door B.M. de Vries

1. Inleiding

De bescherming van de eigendommen van een onderneming zal door een ieder als vanzelfsprekend worden beschouwd. Alhoewel gegevens ook tot de eigendommen gerekend kunnen worden, is tot voor kort weinig aandacht besteed aan de bescherming van gegevens tegen ongeoorloofd gebruik. De behoefte aan toegangsbeveiliging (dat is het beperken van de toegangsmogelijkheden) van de binnen de onderneming aanwezige gegevens is de laatste jaren sterk toegenomen, hetgeen nauw samenhangt met de ontwikkeling van de geautomatiseerde gegevensverwerking. De toegenomen behoefte aan gegevensbeveiliging wordt veroorzaakt door:

- verruiming van de toegangsmogelijkheden tot de gegevens, waardoor het gemeenschappelijk gebruik van gegevens is toegenomen;
- groter volume van gegevens, dat centraal verzameld en/of opgeslagen is;
- het in staat zijn om op eenvoudige wijze gegevens aan elkaar te relateren, waardoor de gevoeligheid van de daaruit voortvloeiende informatie toeneemt;
- privacy wetgeving, waardoor toegangsbeperkende maatregelen verplicht gesteld worden.

In dit artikel zal aandacht worden besteed aan enige hulpmiddelen in de vorm van computerprogrammatuur, waarmee het beperken van de toegangsmogelijkheden tot gegevens bij geautomatiseerde gegevensverwerking kan worden gerealiseerd.

Voor wat betreft de wijze van toegang wordt bij gebruik van toegangsbeveiligingsprogrammatuur onderscheid gemaakt in het lezen (READ), wijzigen (UPDATE), creëren (CREATE) en verwijderen (DELETE) van gegevens. Binnen het te beveiligen systeem (bestaande uit bestanden, programmatuur, terminals, personen, procedures, etc.) zal gespecificeerd dienen te worden wie bevoegd is om op welke wijze (wijze van toegang) toegang te verkrijgen tot welke gegevens, alsmede welke bewerkingen zijn toegestaan. Deze bevoegdheidsregelingen zijn vastgelegd in zogenaamde access rules, die de basis vormen van de toegangsbeveiligingsprogrammatuur; elk verzoek om toegang tot beveiligde gegevens wordt onderwerp van controle met behulp van access rules.
Ook de middelen, waarmee toegang tot gegevens verkregen kan worden, zoals applicatieprogramma's, terminals, data base transacties, utilities, systeemsoftware dienen onder de beveiliging te vallen.

2. Normen, waaraan toegangsbeveiligingsprogrammatuur moet voldoen

Het toekennen van de bevoegdheden is een belangrijk onderdeel van de toepassing van toegangsbeveiligingsprogrammatuur. De toegekende bevoegdheden dienen in essentie de binnen de organisatie bestaande bevoegdheidsregelingen (en dus functiescheidingen) te reflecteren.

Het ontbreken van deze eis zou betekenen, dat de interne controle uit hoofde van bestaande functiescheidingen teniet zou gaan. Deze regelingen zijn echter veelal moeilijk toe te passen op informatiesystemen, waarin een zekere mate van gegevensintegratie (dat is het gemeenschappelijk gebruik van gegevens) plaatsvindt. In dergelijke situaties is het raadzaam een hoofdgebruiker (owner of eigenaar) aan te wijzen, die in sommige gevallen echter niet eenduidig aan te wijzen is.

Naast de toekenning van de aan functies gerelateerde bevoegdheden is van belang het centraal beheer van het beveiligingssysteem. Tot de taken van deze functie i.c. het centraal beheer dienen gerekend te worden:

- toekennen van de initiële (d.i. de bij de implementatie toegekende) bevoegdheden aan de hoofdgebruikers;
- toezien op het gebruik van het toegangsbeveiligingssysteem (monitoring van het systeem);
- het signaleren van pogingen tot doorbreking van het beveiligingssysteem via boodschappen op de terminal of via een afdruk op de printer van de systeembeheerder en het nemen van actie hierop;
- het zonodig aanbrengen en wijzigen van bevoegdheden binnen het systeem (bijvoorbeeld voor nieuwe owner of t.b.v. een reorganisatie);
- toezien op het verrichten van onderhoud aan het beveiligingssysteem.

De centrale systeembeheerder, ook wel genoemd security officer of security administrator (in dit artikel wordt de term security officer gehanteerd) beschikt derhalve over vergaande bevoegdheden. De bevoegdheden van security officer dienen (in verband met plaatsvervanging) aan slechts 2 à 3 functionarissen te worden toegekend. Het belang van de functie brengt met zich mee dat de security officer op het hogere niveau in de organisatie dient te zijn opgenomen; de security officer dient geen gebruikerstaken te verrichten en zal bij voorkeur geen deel uitmaken van de automatiseringsafdeling. Vanuit de hogere leiding is effectief toezicht op het functioneren van de security officer nodig om het autonoom optreden van hem en de daarmee verbonden gevaren te voorkomen (b.v. frauduleuze handelingen van deze functionaris).
Het toegangsbeveiligingssysteem dient voorzieningen te bevatten, waardoor ongeautoriseerde toegang via systeemsoftware (bijvoorbeeld operating system, T.P.-monitoren, data base managementsystemen) en standaard utilities wordt voorkómen of tijdig aan de security officer wordt gesignaleerd.

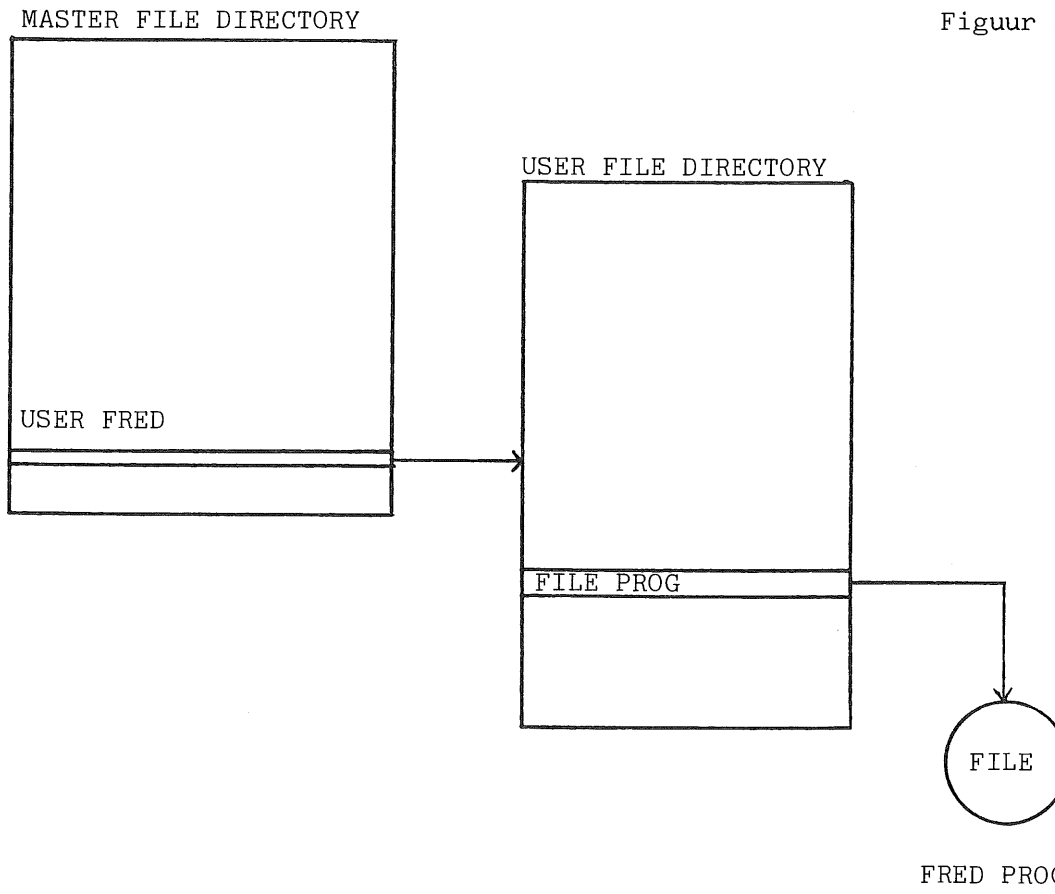
Tot slot zal het toegangsbeveiligingssysteem zo weinig mogelijk beslag op geheugenruimte en op de processor dienen te leggen. Het daardoor ontstane verlies aan performance is niet alleen afhankelijk van de toegepaste toegangsbeveiligingsprogrammatuur, maar ook van de omvang van toegangsbeveiliging (hoeveel gegevens, applicatieprogramma's, terminals zijn beschermd) en van de structuur van de access rules.

3. Praktische toepassingsvormen van toegangsbeveiligingsprogrammatuur

Toegangsbeveiliging wordt thans gerealiseerd door:

a. Het onderbrengen van access rules in het operating system. Daarbij is het begrip operating system ruim gedefinieerd. De access rules zijn ondergebracht in het file management system, hetgeen een onderdeel vormt van het operating system.
Deze wijze van toegangsbeveiliging is te vinden binnen GCOS (operating system) van Honeywell Bull systemen.
In figuur 1 wordt de werkwijze van deze vorm van toegangsbeveiliging aangegeven. De bevoegde gebruikers zijn gespecificeerd in de master file directory (MFD) van waaruit via een pointer verwezen wordt naar de per bevoegde gebruiker gespecificeerde user file directory (UFD), waarin alle bestanden en applicatieprogramma's zijn opgenomen, waartoe de gebruiker (in voorbeeld user Fred) bevoegdheden heeft. In de user file directory zijn tevens de aard van de bevoegdheden (bijv. UPDATE, READ) per bestand en applicatieprogramma aangegeven. De bevoegdheid van een gebruiker tot een bestand of programma kan worden vastgesteld door in de MFD na te gaan of de gebruiker daarin voorkomt. Vervolgens wordt via de pointer een link naar de UFD van de gebruiker gelegd om vast te stellen, welke bevoegdheden de gebruiker heeft ten aanzien van het gevraagde bestand of applicatieprogramma. (In het voorbeeld de bevoegdheid van gebruiker Fred ten aanzien van file Fred PROG.)

Figuur 1



b. Het toepassen van een afzonderlijk toegangsbeveiligingspakket. De access rules zijn daarbij ondergebracht in tabellen. In dit artikel worden de volgende pakketten in het kort behandeld: RACF, ACF2, SAC en SECURE.

De werkwijze van beide vormen van toegangsbeveiliging komen grotendeels met elkaar overeen. Voor beide vormen geldt, dat de mate van interne controle die bereikt wordt sterk afhangt van de wijze waarop bevoegdheden zijn toegekend.
Geen van beide vormen van toegangsbeveiliging bieden een beveiliging van ongeoorloofd gebruik (wijziging!) van het operating system. Aangezien toegangsbeveiligings-software alleen werkt via het operating system, dient bij gebruik van toegangsbeveiligings-software aan de betrouwbaarheid van het operating system hoge eisen te worden gesteld.

Bij een onderzoek naar de wijze van toepassing van toegangsbeveiligingsprogrammatuur dient daarbij altijd de betrouwbaarheid van het operating system te worden betrokken.
Bevordering van de betrouwbaarheid moet vooral worden gezocht in de structuur en opzet (architectuur) van het operating system.

4. Overzicht van toegangsbeveiligingspakketten

In dit overzicht komt een viertal toegangsbeveiligingspakketten aan de orde, beginnend met RACF. De overige 3 pakketten (ACF2, SECURE en SAC) worden in vergelijking met RACF (met name de verschillen met RACF) behandeld. De toegangsbeveiligingspakketten worden in dit hoofdstuk niet in extenso behandeld; de vanuit betrouwbaarheidsaspecten belangrijkste kenmerken zullen evenwel aan de orde komen. Teneinde de werkwijze van toegangsbeveiligingspakketten te verduidelijken wordt één pakket namelijk RACF uitvoeriger behandeld dan de overige pakketten.

RACF (Resource Access Control Facility).

RACF is een produkt van IBM en kan alleen onder het operating system MVS (Multiple Virtual System) draaien. De beveiliging van RACF strekt zich enerzijds uit tot TSO (Time Sharing Option) en IMS (Information Management System) gebruikers, maar ook tot gebruikers bij batchverwerking, anderzijds tot de systeemelementen IMS transactions, DASD (Direct Access Storage Device) of tape volume, TSO of IMS terminal en applicaties. De beveiliging van gebruikers, groepen van gebruikers en systeemelementen (resources) wordt gespecificeerd in access rules, binnen RACF profiles genoemd. De beveiliging per groep van gebruikers maakt het mogelijk om de toegangsbeveiliging per afdeling te regelen. Binnen de groep kunnen bevoegdheden worden gedelegeerd aan de leden van de groep of afdeling (hiërarchische structuur). De relaties tussen de individuele en de groepsbevoegdheden van iedere gebruiker zijn vastgelegd in de zogenaamde CONNECT-profiles.
De individuele gebruikersbevoegdheden zijn vastgelegd in USER PROFILES, de groepsbevoegdheden in GROUP PROFILES en de bevoegdheden per systeemelement in RESOURCE PROFILES. De inhoud van de profiles wordt gemodificeerd, toegevoegd, vervallen verklaard en uitgelijst door middel van RACF-commando's.

Tot het gebruik van RACF-commando's zijn de security officer, degene met AUDITOR-bevoegdheid (de accountant of interne controleur), degene met OPERATION-bevoegdheid (voor verrichten van onderhoudsactiviteiten) en de hoofdgebruikers (owners) bevoegd.
Alle toegangsbevoegdheden zijn vastgelegd in een data set, de zogenaamde RACF data set.

De mate van gegevensbeveiliging welke gerealiseerd wordt door toepassing van RACF is derhalve afhankelijk van de wijze, waarop bevoegdheden binnen RACF over de organisatie verdeeld zijn. Iedere gewenste gegevensbeveiliging dient binnen RACF expliciet te worden aangebracht. De gebruiker kan toegang tot het door RACF beveiligd systeem verkrijgen na het verifiëren van het password en de gebruikersidentificatie met de gegevens in de RACF data set. Het password dient binnen een verplicht te vermelden tijdsinterval te worden gewijzigd.
Na deze verificatie vindt de vaststelling van de eventuele bevoegdheid van de gebruiker ten aanzien van het gevraagde bestand plaats.

Groepen worden aan RACF gedefinieerd via het ADD GROUP-commando. Van iedere groep wordt een group profile opgebouwd, waarin:
- informatie over de groep
- welke gebruikers tot de groep behoren
- de groepsbevoegdheden van de leden
  (in volgorde van hoogste tot laagste bevoegdheid, waarbij een hogere bevoegdheid tevens de lagere omvat; derhalve bevat b.v. JOIN-bevoegdheid tevens de CONNECT, CREATE, USE-bevoegdheden):
  - JOIN: definiëren van nieuwe gebruikers en groep aan RACF en het toekennen van de groepsbevoegdheden.
  - CONNECT: toevoegen van reeds bestaande RACF-gebruikers aan de groep en het toekennen van groepsbevoegdheden (met uitzondering van JOIN).
  - CREATE: aanmaken en onder RACF-beveiliging brengen van group data sets (data set, waarvan de owner wordt aangegeven door een group id(entification).
  - USE: toegang tot data sets waarvoor de groep geautoriseerd is.

In de USER profile wordt opgenomen:
- gebruikersidentificatie
- password
- groep waartoe hij behoort
- bevoegdheden.

Bij iedere access van de gebruiker wordt door middel van het password in de user profile gecontroleerd of de gebruiker het juiste password heeft ingetoetst.
Per gebruiker kunnen onder andere de volgende bevoegdheden worden toegekend:
SPECIAL: Geeft de gebruiker onbeperkte bevoegdheden. Hij mag alle RACF-commando's gebruiken. Deze bevoegdheid dient alleen aan de centrale beheerder (en zijn vervanger), de security officer te worden toegekend.

AUDITOR: Biedt mogelijkheid tot beoordeling van de beveiliging door het specificeren van logging-opties, uitlijsten van pogingen tot doorbreking van de RACF-beveiliging.

CLAUTH: Stelt gebruiker in staat andere gebruikers en data sets onder RACF te brengen.

ADSP: Alle door de gebruiker aangemaakte data sets worden automatisch onder RACF gebracht (ADSP = Automatic Data Set Protection).

Per resource (data set) dient een (user of group) owner aangewezen te worden. De owner beschikt over de hoogste bevoegdheden ten aanzien van zijn resource(s). De toewijzing van owners gedurende het installatieproces van RACF brengt veelal organisatorische problemen met zich mee. Bij het gemeenschappelijk gebruik van bestanden is het, zoals reeds vermeld, moeilijk om een owner aan te wijzen.
De RESOURCE-profile bevat o.a.:

a. User of group owner.
b. Universal Access Control Code (UACC) ⟶ default toegangsbevoegdheid per resource voor gebruikers die niet binnen RACF gedefinieerd zijn.
c. De bevoegdheden van gebruikers, die met name vermeld staan in de access list van de data set.

De mogelijke bevoegdheden zijn:

ALTER: Gebruiker heeft de volledige bevoegdheid over de data set en kan andere gebruikers of groepen toegangsbevoegdheid tot de data set geven.

CONTROL: Toegangsbevoegdheid bij VSAM (VSAM = Virtual Storage Access Method) data sets.

UPDATE: Bevoegdheid tot lezen en schrijven van de data set.

READ: Bevoegdheid tot lezen van de data set.

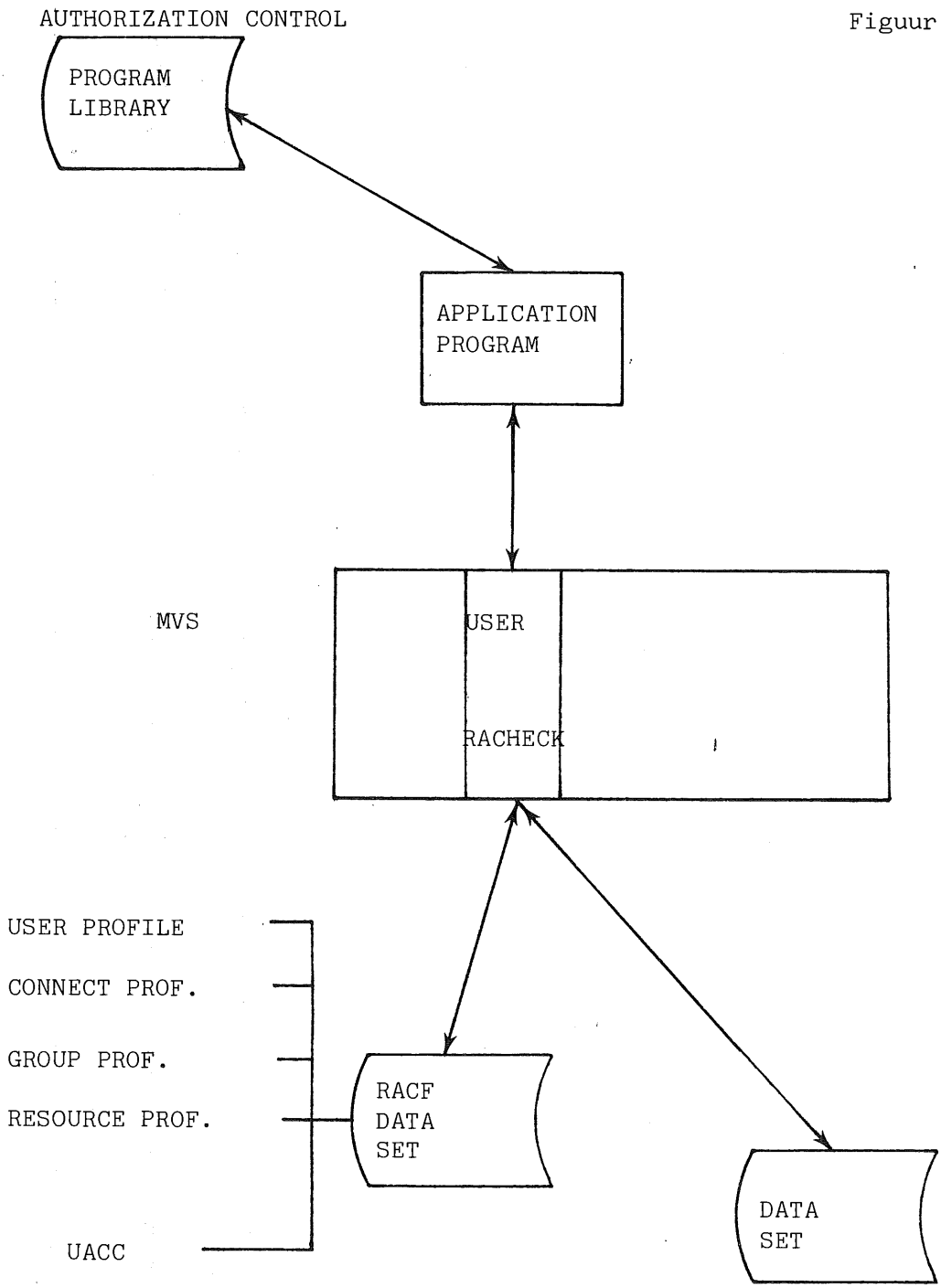
NONE: Geen bevoegdheid tot de data set.

Het verkrijgen van toegang tot de door RACF-beveiligde resources (data sets, volumes, e.d.) gaat als volgt:

1. De gebruiker dient via TSO log-on of eventueel via IMS/VS sign-on de gebruikers-/groepsidentificatie én het password te specificeren (het password dient binnen maximaal 30 dagen te worden gewijzigd ')). Via de RACF-macro RACINIT SVC wordt gecontroleerd, of de betreffende gebruiker binnen RACF is gedefinieerd en tot het systeem kan worden toegelaten.

') Onder release 4 van RACF is het mogelijk, dat de security officer beschikt over een password, dat niet periodiek gewijzigd dient te worden.

2. De gebruiker verzoekt via de OPEN-macro in zijn applicatieprogramma toegang tot een data set. Indien de data set onder de beveiliging van RACF valt, is in de data set label een beveiligingsbit aangezet. Via dit beveiligingsbit constateert het operating system, dat de data set via RACF is beveiligd. RACF ontvangt de besturing en controleert (via RACF-macro RACHECK) met behulp van de inhoud van de profiles of de gebruiker voldoende bevoegdheid heeft (zie figuur 2).



Figuur 2

Logging-faciliteiten

Vanuit RACF worden records in SMF geschreven, die betrekking hebben op:
- modificeren van profiles;
- uitvoeren van RACF commando's;
- gebruik van RACF options;
- toegang tot door RACF beschermde resources;
- ongeautoriseerde pogingen om toegang tot het systeem te verkrijgen;

De security officer heeft de volgende faciliteiten:
. SPECIAL-bevoegdheid;
. security console met signalering van ongeautoriseerde pogingen om toegang;
. uitgebreide logging;
. kan profiles wijzigen en toevoegen, inclusief de AUDITOR-bevoegdheid;
. het toekennen en wijzigen van de AUDITOR-bevoegdheid.

Uit bovenstaande mag duidelijk zijn, dat de security officer bij RACF een sleutelfunctie bekleedt. Zijn positie binnen de organisatie zal moeten zijn, dat een zekere onafhankelijkheid ten opzichte van gebruikers en automatiseringsafdeling is gewaarborgd. Voorts dienen de activiteiten van de security officer te worden beoordeeld door de gebruiker met de AUDITOR-bevoegdheid (toe te kennen aan de chef van de security officer en aan intern controleur/accountant).

De gebruiker met AUDITOR-bevoegdheid beschikt over logging faciliteiten. Het verkrijgen van bruikbare listings van de SMF-records (logging) vereist echter het gebruik van de report writer (optioneel) of van retrieval-programmatuur (zoals CULPRIT, EASYTRIEVE). De logging faciliteit verschaft de AUDITOR-gebruiker geen inzicht in de binnen RACF toegepaste bevoegdhedenstructuur, waardoor een vergelijking met de binnen de organisatie bestaande bevoegdheden niet mogelijk is. Zoals reeds genoemd kan de security officer de AUDITOR-bevoegdheid toekennen en buiten werking stellen.
Alhoewel deze handeling van de security officer voor de "AUDITOR" nog wel wordt gelogged, is dit vanuit het gezichtspunt van de "AUDITOR" een tekortkoming van RACF.

Beperkingen van RACF:
- Het operating system kan bij gebruikmaking van tapes de beveiliging door RACF signaleren middels de aanwezigheid van de RACF-bit in de tapelabel (bestandsidentificatie) van het bestand. Het gebruik van de labels kan worden omzeild door gebruikmaking van JCL met zogenaamde by-pass labeling (BLP)-faciliteiten. De beveiliging via RACF wordt dan niet door het operating system gesignaleerd.
- Programmatuur- en systeem-libraries, die exclusief door systeemprogrammeurs worden gebruikt, zijn niet via RACF beveiligd.

ACF2

ACF2 (Access Control Facility 2) is een produkt van de Cambridge Systems Group en kan evenals RACF alleen onder het operating system MVS draaien. Als belangrijk verschil van RACF ten opzichte van ACF2 zijn bij ACF2 in principe alle bestanden beveiligd, tenzij binnen ACF2 anders gespecificeerd. Niemand krijgt toegang tot een bestand, tenzij deze toegang door de owner, de security officer of via een access rule wordt toegekend.
Aangezien ieder access wordt bepaald door LOGON ID, password, gebruikersnaam, etc., dienen deze gegevens van alle gebruikers te worden gedefinieerd binnen ACF2. Dit geschiedt door voor iedere gebruiker een LOGON ID record te specificeren.

Een uit toegangsbeveiliging belangrijk data element binnen het LOGON ID record wordt gevormd door de USER ID String (UID string), die een combinatie van gebruikerskenmerken bevat, bestaande uit afdelingsnummer, ploegnummer, functienummer, aard van werkzaamheden, TSO LOGON ID of batch gebruiker ID. Met behulp van de UID-string is het mogelijk een aantal gebruikers te groeperen naar afdeling, functie, e.d.
Aangezien de UID-string onderdeel uitmaakt van de access rule, kan door middel van het groeperen van gebruikerstoegangsbeveiliging op groeps-(lees: afdelings-, functie-, e.d.) niveau worden gerealiseerd.
In de access rules kunnen behalve de UID-string de volgende gegevens worden opgenomen:
- data set specificatie;
- JCL data definition (DD) naam;
- programmanaam;
- naam van de programmabibliotheek;
- expiratiedatum van tijdelijke access rules.

ACF2 biedt de mogelijkheid om het wijzigen van programma's te beveiligen. Het toevoegen, verwijderen en wijzigen van programma's is dan alleen mogelijk via een programma in de Authorized Program Facility (APF) *, mits de naam van dit programma in de access rule is gespecificeerd.
In tegenstelling tot RACF bevat ACF2 de bevoegdheid EXECUTE-only, hetgeen de gebruiker met uitsluiting van anderen de bevoegdheid geeft tot verwerking van het programma.
Het doen aanbrengen van wijzigingen in het programma is binnen deze bevoegdheid niet toegestaan.

SECURE

SECURE is een produkt van Boole en Babbage. Het werkt onder ieder IBM operating system. Evenals bij RACF dient toegangsbeveiliging expliciet gespecificeerd te worden.

---

*) Toegang tot APF-programma's is binnen het operating system MVS beveiligd.

Ter identificatie van de gebruiker worden door SECURE bepaalde velden van de JCL (JOBNAME, password, naam programmeur, e.d.) omgezet in een code, de zogenaamde Access Identifier String (AIS). De inhoud van de AIS wordt bij iedere poging tot toegang vergeleken met de inhoud van de control data set, waarin de codes van de bevoegde gebruikers zijn opgenomen. De AIS bestaat uit het Data Set Name-gedeelte bevattende de naam van de gevraagde data set en uit het Job-Identifier gedeelte, hetgeen de gebruikersidentificatie bevat.
Na via de AIS-afstemming toegang tot de beveiligde data set te hebben verkregen, wordt een link gelegd met een access rule, die aangeeft over welke bevoegdheid de gebruiker ten aanzien van de gevraagde data set beschikt.

SAC (Secure Access Controller).

SAC is een pakket van Electronic Data Systems. Over dit pakket kunnen wij kort zijn, omdat vele van de reeds genoemde beveiligingsfaciliteiten in dit pakket terug te vinden zijn. Evenals bij RACF en SECURE dient beveiliging expliciet gedefinieerd te zijn. SAC heeft als voordeel ten opzichte van RACF en ACF2, dat het behalve onder het operating system MVS ook onder VS1 en MVT toepasbaar is. SAC beveiligt evenals RACF de toegang op het niveau van IMS transactions (SECURE niet). Evenals bij SECURE wordt de identificatie van de gebruiker berekend op grond van informatie uit de JCL.
De access rules zijn opgeslagen op de Rules Data Set, waarvan de inhoud door middel van encryption (het versluieren van informatie middels een geheime code) en fetch-protection (update beveiliging in operating system) is beveiligd.

Samenvatting

De mate van toegangsbeveiliging die bereikt wordt door toepassing van access control programmatuur is niet alleen afhankelijk van de faciliteiten, die door een pakket geboden worden maar vooral van de wijze, waarop het in de organisatie wordt geïmplementeerd.
Belangrijk is, dat de via het pakket toegekende bevoegdheden de binnen de organisatie aanwezige bevoegdhedenstructuur reflecteert.
Van belang is voorts:

- de wijze waarop de functie van security officer als centraal beheerder van het toegangsbeveiligingssysteem wordt vervuld;
- de controle op het functioneren van de security officer door management en door de (interne) controlefunctie.

Voor alle genoemde pakketten is het mogelijk aanvullende opties en exit routines toe te passen, waardoor (een deel van) de beveiliging kan worden uitgeschakeld.
Het gebruik hiervan dient derhalve met de nodige voorzorgen te worden omgeven (controle en registratie van gebruik).

Schema 1 geeft een overzicht van RACF, ACF2, SECURE en SAC. In het algemeen kan gesteld worden, dat via RACF en ACF2 meer verfijning in de toegangsbeveiliging verkregen wordt, aangezien naast individuele gebruikers ook groepen van gebruikersbevoegdheden kunnen worden toegekend.
Alhoewel verschillen tussen de pakketten bestaan, zal de mate van gerealiseerde interne controle nauw samenhangen met de toekenning van de bevoegdheden.

OVERZICHT VAN ACCESS CONTROL SOFTWARE

	RACF	ACF 2	SECURE	SAC
Beveiligde resources	Data Sets, Volumes (schijven en tapes), Terminals, IMS transactions	Data Sets, Volumes, TSO-commands, Programma's, IMS transactions, Terminals	Data Sets, VTOC's	Data Sets, IMS transactions VTOC
Controlemethoden	USERIDENTIFICATION	USERIDENTIFICATION	Gegevens uit JCL	Gegevens uit JCL
Toegangsbevoegdheden	READ UPDATE ALTER (CREATE, DELETE)	READ WRITE (update only) EXECUTE ONLY ALLOCATE (CREATE, DELETE)	READ WRITE SCRATCH EXECUTE ONLY	READ UPDATE ALTER (CREATE, DELETE)
Aard van beveiliging	Beveiliging indien gespecificeerd	Beveiliging is standaard	Beveiliging, indien password protection bit is geïnitieerd	Beveiliging indien gespecificeerd
Benodigd operating system	MVS	MVS	Alle IBM operating systems	MVS, VS1, MVT
Interfaces met operating systems	OPEN, END OF VOLUME, ALLOCATE, SCRATCH	OPEN, END OF VOLUME, ALLOCATE, SCRATCH, CATALOG, RENAME	OPEN, END OF VOLUME, SCRATCH, RENAME	OPEN, END OF VOLUME ALLOCATE, SCRATCH CATALOG, RENAME

Literatuur

RACF General Information Manual
Installation Reference Manual
Messages and Codes Manual
IBM Info-System over Release 4 van RACF

ACF 2 2.2 Diverse manuals

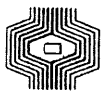
SAC General Information System

Computer Access Control Software
door Linda Vetter, EDPACS februari 1980

RACF Een voorbeeld van geautomatiseerde autorisatie
door drs. C.P. Aland, Informatie maart 1980

Data base security: requirements, policies and models
door Wood, Fernandez en Summers, IBM Systems Journal
Vol. 12, november 1980

Fundamentals of Operating Systems,
door A.M. Lister, 2e druk, Macmillan Press



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

winter 1981/1982

DATA BASE CONVERSIE, een praktijkgeval

door A. Kamstra

Inleiding ')

In dit artikel wordt ingegaan op de problematiek met betrekking tot het converteren van een data base. Vooral hoe een dergelijke conversie kan plaatsvinden en welke interne controlemaatregelen genomen kunnen worden om de goede gang van zaken te kunnen vaststellen, worden in dit artikel behandeld. Het betreft hier een data base conversie zoals in de praktijk heeft plaatsgevonden. Omtrent de organisatorische aspecten verwijzen wij u naar de aangehaalde artikelen.

Omgeving en gestelde eisen

Om een indruk te krijgen van de risico's en de omvang van deze conversie is het goed te weten dat het hier betrof:
- een overgang naar een andere computer;
- een gedeeltelijke overgang naar een andere programmeertaal;
- een overgang op een ander besturingssysteem;
- een overgang naar een ander data base systeem;
- een overgang naar een ander data communicatiesysteem.

Het geheel heeft exclusief voorbereidingen meer dan één jaar geduurd. Vooral het converteren van de data base- en data communicatieprogrammatuur heeft zeer veel tijd gevergd. Gedurende de laatste maanden heeft men de volledige beschikking gehad over beide typen computers.

In de oude situatie was sprake van een codasyl-achtige data base structuur terwijl in de nieuwe situatie zonder meer sprake was van een data base management system volgens de codasylnormen. De eis die aan een conversie van een bestand en dus ook aan de conversie van een data base gesteld moet worden is dat geconstateerd kan worden dat alle gegevens volledig en juist zijn omgezet.

° Volledigheid: zijn alle records overgenomen.
° Juistheid:
- is de inhoud van de records juist overgenomen;
- zijn de bestaande relaties tussen de records juist overgenomen.

Een extra moeilijkheid hierbij was dat de interne representatie van de tekens in de oude computer niet volledig gelijk waren aan die van de nieuwe computer, zodat conversie van tekens diende plaats te vinden. Een voordeel was wel dat voor de organisatie (incl. gebruikers) een mutatiestop van enkele dagen acceptabel was. Wel was de omvang van de bestanden bijzonder groot waardoor de doorlooptijd van de processen erg lang was.

') Voor algemene aspecten met betrekking tot een conversie verwijzen wij u naar de artikelen van J.C.P.M. Vermeeren met als onderwerp "Programmaconversie-systeemontwikkeling met handicap" Compact zomer 1981 en het artikel van A.W. Neisingh e.a. met als onderwerp "Conversie van bestanden" Compact voorjaar 1975.

Opzet van de conversie

In bijgaand schema is in een stroomdiagram weergegeven hoe de conversie van de data base heeft plaatsgevonden. Hoewel de belangrijkste records tot identieke records in de nieuwe data base leidden was het toch in een aantal gevallen noodzakelijk om records samen te voegen of uit te splitsen.
Een aansluiting van het aantal records van begin tot eind kan dus niet van ieder recordtype plaatsvinden.

Toelichting op schema 1.

Algemeen: In de stappen 2 tot en met 6 werd in ieder programma afgedrukt per recordtype het aantal gelezen en weggeschreven records.

Stap 1. Door middel van een statistiekprogramma werd een telling gegeven van ieder recordtype in de te converteren data base.

Stap 2. De oude data base wordt ontladen op een tape.

Stap 3. In dit programma wordt de gegevensrepresentatie aangepast aan de nieuwe computer.

Stap 4. Hier wordt de nieuwe data base geladen. Bij dit proces vinden enkele samenvoegingen en uitsplitsingen van records plaats zodat voor een deel aansluiting tussen het aantal gelezen en geschreven records niet plaats kan vinden.

Stap 5. De nieuwe data base wordt ontladen op een tape.

Stap 6. De tape ontstaan uit stap 2, wordt door een ander programma dan door het programma uit stap 3 gelezen en geconverteerd ten behoeve van het vergelijkingsproces in stap 7.

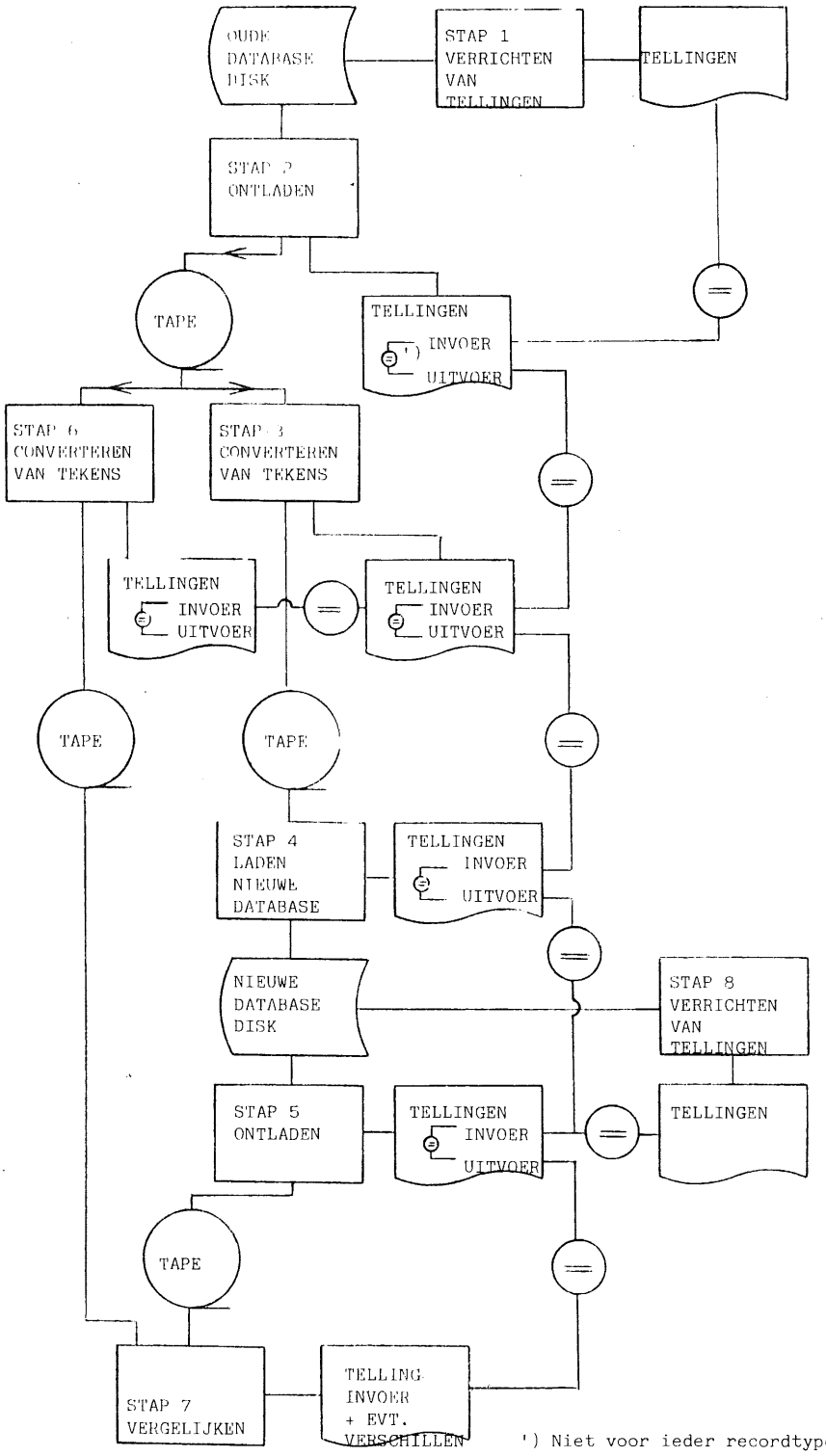
Stap 7. Hierbij wordt de tape uit stap 5 vergeleken met de tape uit stap 6. Hierbij wordt dus de inhoud van de data base gecontroleerd. Mogelijke verschillen alsmede het aantal gelezen records (per recordtype op beide bestanden) wordt afgedrukt.

Stap 8. Met behulp van een standaardprogramma wordt een telling per recordtype vervaardigd. Tevens wordt aangegeven de relatie tussen de verschillende recordtypen (owners/members in aantallen).

Opmerkingen

De controle op de volledigheid kan op deze wijze voor de meeste en belangrijkste recordtypen goed plaatsvinden. Echter of bepaalde recordtypen volledig in het goede recordtype zijn opgenomen kan niet via tellingen worden geconstateerd. Voor recordtypen die uitgesplitst werden naar verschillende nieuwe recordtypen is de volledigheid te controleren echter of de uitsplitsing op zich juist heeft plaatsgevonden kan via tellingen niet worden geconstateerd.

STROOMSCHEMA CONVERSIE VAN DE DATABASE



') Niet voor ieder recordtype.

Zoals uit het schema en de toelichting blijkt, vindt de controle op de juistheid plaats in stap 7.

Enkele zwakke plekken in deze procedure zijn wel te onderkennen, genoemd kunnen worden stap 2 en de stappen 3 en 6.

Indien in stap 2 de inhoud van de records niet juist wordt weggeschreven dan zal dit binnen de procedure van dit schema niet ontdekt worden. Wel moet hierbij worden opgemerkt dat dit een programma betrof dat reeds enige jaren voor reorganisatiedoeleinden werd gebruikt en waarbij zich geen problemen hebben voorgedaan, zodat de goede werking in ruime mate was aangetoond. Voor de stappen 3 en 6 geldt dat indien in beide programma's bepaalde tekens op dezelfde wijze verkeerd geconverteerd worden, dit ook in de verdere procedure niet ontdekt zal kunnen worden. Wel waren de programma's in stappen 3 en 6 separaat ontwikkeld en moesten ze respectievelijk op de oude en nieuwe machine worden uitgevoerd.

Aanvullende procedures vóór en direct nà de conversie

Het zorgvuldig uittesten van de programma's, het uitvoeren van schaduwruns en het betrekken van de gebruikers bij de controle daarop zijn zonder meer van grote betekenis om een goede overgang te waarborgen. In dit geval waren er door de gebruikers testgroepen gevormd. De conversie kon pas van start gaan nadat deze testgroepen akkoord waren gegaan met de resultaten van test- en schaduwruns.
Ter meerdere zekerheid op de in het schema weergegeven procedure zijn de volgende maatregelen genomen te weten:

- Overzichten zijn vervaardigd van zowel standen (totaaltellingen) als detailoverzichten van de te converteren als ook van de geconverteerde data base.
- De gebruikers is gevraagd deze overzichten direct te controleren.
- De oude computer bleef stand-by om bij onverwachte moeilijkheden terug te kunnen vallen op de oude programmatuur.

Slot

Slechts een geheel van maatregelen kan bijna waarborgen dat een conversie goed verloopt. Toch zijn er tegenvallers waartegen de organisatie geen enkel verweer heeft (bijv. hardware- en stroomstoringen). Indien deze optreden, zoals in het onderhavige geval, juist tijdens de conversieslag, dan is het adequaat reageren en beslissen van enorme betekenis voor het welslagen. Het veelal permanent beschikbaar zijn van deskundigen is gedurende deze periode een noodzaak. Door alle betrokkenen dient gerealiseerd te worden dat gedurende de eerste maanden na invoering de programmatuur zo nu en dan nog fouten zal vertonen. Een extra kritische controle op de werking in deze periode is geboden.

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

BOEKEN

door J. Philippo

AC 373. Control and Audit of minicomputer systems. Working party of British Computer Society. 1981

Dit boekje, dat gemaakt is door de Working Party van de Auditing by Computer Specialist Group, geeft een kort overzicht van de hoofdgebieden van controle en audit, welke zich voordoen bij het toenemend gebruik van minicomputers in commerciële organisaties.
Hoewel het de werkgroep bleek, dat er weinig fundamentele verschillen bestaan in de controles bij minicomputers en die bij grotere systemen, was er echter een aantal gebieden met belangrijke verschillen en potentiële moeilijkheden. Op deze gebieden is de werkgroep ingegaan en heeft daardoor afgezien van het maken van een complete handleiding.

Na een aantal opmerkingen over minicomputers in het algemeen en de gebruikte hard- en software wordt in een afzonderlijk hoofdstuk ingegaan op de controles en audit by stand-alone mini's. In dit hoofdstuk wordt mede aandacht gegeven aan het gebruik van software-pakketten en de testprocedure daarvoor. Ten aanzien van de audit wordt een aantal behartenswaardige opmerkingen gemaakt voor de te volgen strategie.

In een afzonderlijk hoofdstuk wordt ingegaan op audit information retrieval methoden welke dienen om de accountant die informatie te verschaffen, welke niet direct leesbaar aanwezig is maar wel in computerbestanden is opgeslagen.

Ten aanzien van het gebruik van minicomputers in grotere organisaties zijn twee hoofdstukken gewijd aan Corporate Minicomputer Policy en Data bases on Minicomputers. Beide vragen vooral aandacht van het management, terwijl voor het laatste item erop gewezen wordt dat: "from an audit viewpoint, as the data structure is more complex, good control procedures will become more critical as errors and failure may be harder to detect and to recover".

Alles te zamen een goed boekje om zich de problemen bij mini's te realiseren, echter geen audit guide. Daarvoor zou de lezer zich moeten bedienen van AICPA Guideline "Audit and Control considerations in a minicomputer environment" (AC 357) waarin de risico's en de controles, welke deze reduceren, zijn vermeld. Dit is echter evenals het hiervoor besproken boekje, ook een "minibook".

AC 344. Information Security Handbook
B.J. Wilkens The Institute of Internal Auditors

Het uitgangspunt van de schrijver is, dat Information Security een veel wijder gebied bestrijkt dan data security. Er zijn meer plaatsen in een organisatie waar informatie bloot staat aan ongeautoriseerde toegang en er zijn technieken als reproduktie alsmede teleprocessing van documenten, schijfjes van schrijfmachines, etc., waarbij "snelle afvoer" naar ongewenste plaatsen mogelijk is.
In eerste instantie behoort information security tot de verantwoordelijkheid van het management, hetgeen kan leiden tot een information security program.
De methode, welke de schrijver hiervoor aanbeveelt, is die van selectieve identificatie en bescherming van informatie. Deze methode omvat 4 stappen, namelijk:
1. Identificatie en classificatie van informatie.
2. Waardeer deze en geef prioriteiten (rangschikken).
3. Stel het gebruik van de sleutelinformatie vast.
4. Ontwikkel een gedocumenteerd Information Security Plan.

Voor de bepaling van de beveiligingsmaatregelen zal een kwantitatieve risico-analyse alsmede een evaluatie van de waarde en kosten van de mogelijke maatregelen worden opgesteld.
Als maatregelen noemt de schrijver:
- de traditionele beveiligingsmaatregelen zoals versluiting, toegangsrestrictie en bewaking (incl. islands of security);
- organisatorische controles (scheiding van functies en taken binnen functies, security-verantwoordelijkheid) en personele controles (screening, beleid, jobrotatie, etc.);
- beheersing van de Informatie-services (communicatie, postkamer, reproduktie-afdeling, secretariaten, etc.);
- administratie van de loop en verblijf van top-secret documenten;
- actief beleid ten aanzien van het personeel door voorlichting en handhaving van de voorschriften;
- vernietiging van hoog geclassificeerde informatie, welke niet meer gebruikt zal worden (in verband met hoge kosten voor beveiliging).

Een van de voorwaarden van het beveiligingsplan is, dat het beoordeeld wordt op ontwerp en werking. Daartoe zijn voor de hiervóór genoemde maatregelen in het boek checklists opgenomen.

Een afzonderlijk hoofdstuk is gewijd aan de beveiliging in het EDP-center, dat dezelfde materie weergeeft als in de overige literatuur op dit gebied. Door uitbreiding van het beveiligingsgebied - namelijk van gegevens (data) naar informatie - komen enige bijzondere aspecten naar voren.

In de laatste drie hoofdstukken wordt de informatie-beveiliging audit behandeld, waarin opgenomen:
- de audit benadering;
- audit checklist
- uitvoering van de audit.

Een voorbeeld van een informatie-audit is toegevoegd.

De schrijver, die voor de informatiebeveiliging een belangrijke taak ziet weggelegd voor de interne accountant, besluit met de oproep:

> "The internal audit profession must accept the challenge and develop an effective information security audit program to assist management in assessing the information-security posture of its company. It is hoped that the framework presented here will be of assistance.
> Internal auditors, armed with a checklist tailormade to the needs of their company and sufficient background knowledge in data security, will immediately detect significant information-security exposures within any company.
> It takes years to develop an effective information-security program; now is the time to get started."

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

Tijdschriften

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

LOCKING AND RECOVERY IN A SHARED DATA BASE SYSTEM
AN APPLICATION PROGRAMMING TUTORIAL C.J. Date

Publicatie: IBM General Products Division

Vooraf

Dit artikel is primair gericht op de toepassingsprogrammering. Het bevat een uitstekende beschrijving van de "locking" en "recovery" in data base systemen. Aangegeven wordt hoe in de toepassingsprogrammatuur afgeweken kan worden van de opties van het DBMS. De "concurrency" problematiek komt diepgaand aan de orde.

Globaal overzicht van het artikel

Locking en recovery worden behandeld met betrekking tot een als volgt gedefinieerd data base systeem.
Een data base systeem is (voor dit artikel) een systeem dat gelijktijdige toegang tot één of méér DB's mogelijk maakt vanuit meerdere tegelijkertijd (= concurrent) in uitvoering zijnde programma's onder besturing van een DBMS (Data Base Management Systeem).
Zoals bekend ontstaan in dit soort systemen specifieke problemen met betrekking tot:
- het herstellen van fout beëindigde processen (recovery);
- en de integriteit van de data.

De oplossing houdt doorgaans enigerlei vorm van locking in, dat wil zeggen tijdelijke afsluiting van data voor andere programma's. In het algemeen geschiedt dit "transparent to the user (program)". Het programma dat de DB gebruikt hoeft er geen rekening mee te houden.

Om een zo groot mogelijke mate van concurrency te verkrijgen dient te worden vermeden dat één programma gedurende te lange tijd een te groot deel van de data base voor andere concurrente programma's afgesloten houdt. Het moet, naar behoefte, mogelijk zijn deze standaardregels van het DBMS te "overrulen" (lees: te verfijnen).
Deze verfijning kan nodig zijn om redenen van verwerkingslogica en/of uit performance-overwegingen. De verfijning kan worden gerealiseerd door beperking van de tijdsduur en/of de omvang van de locking.

Er is programmatuur die terzake mogelijkheden biedt: DL/1 en DBTG-COBOL/DML.

Het artikel gaat uit van:
- bekendheid met de behoefte aan integriteit en consistentie van de data base;
- recovery is beperkt tot de z.g. "in-process" recovery.

Speciale problemen met betrekking tot gedistribueerde gegevensverwerking worden niet gericht aan de orde gesteld.

Hierna wordt in het kort een overzicht gegeven van de achtereenvolgens behandelde onderwerpen. De geïnteresseerden wordt de lezing van het artikel zelve aanbevolen.

- The application programming language

  De voorbeelden in het artikel worden opgehangen aan een "verzonnen" taal (Unified Data base Language), die bestaat uit wijzigingsvoorstellen ten aanzien van PL/1 en COBOL. Dusdoende wordt eenheid van definitie verkregen.

- Transaction processing

  Het begrip "transactie" wordt gedefinieerd. Aliassen zijn process; task; run-unit. Afgeleid wordt het begrip "recoverable unit". Iedere transactie bestaat uit een reeks van recoverable units.

- Locking

  Aangegeven wordt, dat een of ander coördinerend mechanisme aanwezig moet zijn dat tot doel heeft:
  a. de mate van concurrency te maximaliseren;
  b. de invloed op het logische ontwerp te minimaliseren.
  Een en ander wordt bestuurd door de "lock manager". De behoefte aan locking ontstaat door drie probleemgebieden:
  - lost updates (verloren mutaties);
  - transaction rollback;
  - inconsistent analyse.

- Lost updates

  Het begrip "serializable" wordt geïntroduceerd. Het systeem moet zodanig zijn opgezet dat ongeacht de volgorde van transactieverwerking hetzelfde correcte resultaat wordt bereikt. Locking kan worden gebruikt om serializability te verkrijgen.

- Deadlock

  Twee transacties zijn beide wachtend gesteld door locking, waarbij ze over en weer op elkaar wachten. Een eindeloze geschiedenis ..... als er geen uitweg voorzien is. In een "terzijde" wordt een drietal maatregelen ter voorkoming van deadlock aangegeven.

- Transaction rollback

  Rollback is een mechanisme waarbij om bepaalde redenen transacties in bewerking worden teruggedraaid en hun resultaten worden geëlimineerd. Behalve ter voorkoming van deadlock is rollback van toepassing bij:
  - abnormal end van verwerking:
  - system crash;
  - integrity violation.

Bij de rollback speelt het recovery log (ten onrechte audit trail genoemd) een onvervangbare rol.
Rollback kan leiden tot lost updates, immers een transactie bestaat uit meerdere recoverable units die "concurrent" verwerkt worden.
Daarom wordt het begrip "commitment" ingevoerd. Door recoverable units aangebrachte mutaties worden pas "gecommit" als de transactie succesvol is beëindigd. Niet "gecommitte" updates moeten "locked" blijven tot de succesvolle beëindiging van de transactieverwerking vaststaat.

- Inconsistent analysis

Zelfs wanneer een transactie niet het doel heeft te muteren kan de noodzaak bestaan data te locken. Bijvoorbeeld in het geval dat een programma een salditotalenlijst produceert, terwijl andere concurrente update transacties actief kunnen zijn.

In dit stadium wordt onderscheid tussen de diverse locks geïntroduceerd:
X - lock = exclusive
S - lock = shared
IX - lock = intended exclusive
SIX - lock = shared, intended exclusive
IS - lock = intended shared

- Lock granularity en lock types

Onder lock-granularity wordt verstaan dat het lock betrekking kan hebben op een groter of kleiner deel van de data. Voorts wordt de samenhang (hiërarchie) in de lock types geanalyseerd.

- UDL intent specifications

In deze paragraaf wordt nader ingegaan op de INTENT declaratie (IX, SIX, IS).

- Levels of isolation

Isolation geeft de mate van interactie (met andere transacties) aan die de transactie kan toestaan, bijvoorbeeld:

Level
1. Sta me niet toe andermans niet "ge-committe" mutaties te muteren.
2. Laat me andermans niet "ge-committe" mutaties niet zien.
3. Laat geen ander het record wijzigen, dat ik nu selecteer.
4. Laat geen ander een record wijzigen, dat ik binnen de uitvoering van mijn recoverable unit heb gezien.
5. Laat me niets merken van de aanwezigheid van anderen.

- Nonrecoverable data

  De recovery van data is afhankelijk van kostenoverwegingen. Er kan van worden afgezien. Dit heeft gevolgen voor de locking.

- Update locks

  In deze paragraaf wordt U(pdate)-lock geïntroduceerd. Het geeft een iets grotere mate van recovery dan het X-lock.

- Summary

  Hierin worden o.a. de ontwerpdoelstellingen nog eens samengevat:
  - begrijpelijk;
  - eenvoud in het normale geval;
  - veilige "defaults"; integriteit gaat voor concurrency;
  - systeemonafhankelijkheid;
  - uitbreidbaarheid.

Het artikel wordt besloten met een uitgebreide bibliografie.

CORPORATE MANAGEMENTSROLE IN SYSTEMDEVELOPMENT E. Nikulainen

Informatie en Management, 1981-3

De automatisering kan gezien worden als een middel ter verkrijging van een betere produktiviteit en beheersbaarheid van de huishouding. Om die reden moet de automatisering beantwoorden aan de behoeften van de huishouding en worden onderworpen aan bestuurlijke maatregelen. Deze laatste dienen te zijn gericht op de produktiviteit van de gehele automatiseringsinspanning zelve.

Nadere beschouwing van (formeel) adequate organisatie-structuren en -processen leert, dat (bijvoorbeeld) het (materiële) functioneren van de stuurgroep automatisering geïmproviseerd en wisselvallig is.
Anderzijds is voor het voortdurend handhaven van de automatiseringsproduktiviteit een creatieve aanpak en aanpassingsvermogen nodig. Dit moet niet gericht worden op technisch georiënteerde experimenten. Deze experimenten verhogen de kosten, verminderen de betrouwbaarheid en onderhoudbaarheid van systemen.

De beheersbaarheid van de automatiseringsinspanning is dan ontoereikend, omdat:
- systemen vaak ontwikkeld zullen worden in gebieden waar de gebruikersbehoeften niet het grootste zijn;
- de systeemontwikkeling vaak wordt vertraagd door gebrek aan projectbeheersing en standaards;
- onderhoud op lopende systemen vaak de budgetten overschrijden.

De schrijver stelt vast, dat het doorgaans moeilijk zal zijn een bedrijfseconomische rechtvaardiging te vinden voor systemen die een verwachte levensduur van minder dan zeven jaar hebben.
"Return on investment" is ten opzichte van administratieve toepassingen vaak hoger in de produktie en procesbesturing.

Er dient nadruk gelegd te worden op het leiden van het systeemontwikkelingsproces.
Geconstateerd wordt dat bij managers vaak de idee bestaat dat geautomatiseerde gegevensverwerking niet te besturen is. Voorts dat de invloed van de ondernemingsleiding zich vaak richt op de hardware-kant, terwijl de investeringen aan de software- en toepassingenkant worden overgelaten aan de lagere leiding. Terwijl de kosten daarvan veel hoger en de invloed op de medewerkers veel groter is.

Toch bestaan er methoden voor doelmatig besturen en leiden van de automatiseringsfunctie. Een wezenlijke aanleiding voor de laissez-faire-benadering is dus niet aanwezig. Er kunnen parallellen getrokken worden tussen systeemontwikkeling en produktontwikkeling, tussen computerapparatuur en produktie-installaties en machines.

Om die redenen kan het beleid en de leiding beter gericht worden op de gegevens (data resources) dan op apparatuur in engere zin. De automatisering dient datagericht te worden benaderd.

Sommige factoren leiden tot een "management by crisis"-benadering, die als nadeel heeft dat het leereffect laag is tengevolge waarvan fouten vaak herhaald worden.
Oorzaken hiervoor zijn onder andere:
- vage doelstellingen;
- voorbijgaan aan c.q. onderschatten van risico's;
- pogingen te omvangrijke en complexe systemen te ontwikkelen waarvoor de ontwikkeltechnieken tekort schieten;
- ontwikkeling gericht op korte termijn efficiency zonder voldoende greep op de eisen op langere termijn.

Een betere bestuurlijke benadering is "management-by-improving-organizational-learning" samengevat in het onderstaande schema.

1. Development of an Effective, but not too Detailed DP-Strategy and Plan.
2. Development of an Environment of and Organization by Adapting the Agreed DP Strategy.
3. Ascertaining the Measurability of Lower-Level Objectives.
4. Conducting Post Installation Reviews.
5. Making Decisions on Investment Proposals.

Fig. 1. Corporate Management's Role in Systems Development.

In het artikel wordt op de rol van de leiding, weergegeven in bovenstaande figuur, nader ingegaan in niet technische bewoordingen.

De conclusie van het artikel is van zoveel belang te achten dat deze hieronder in zijn geheel wordt weergegeven.

> "De activiteiten van de ondernemingsleiding worden vaak beschreven en gezien in termen van mechanische procesregulering. Afwijkingen worden ontdekt door controlemaatregelen en door correctieve actie hersteld.

Twee belangrijke factoren worden daarbij vergeten.
Ten eerste: het is de taak van de leiding uiting te geven aan haar wensen alsmede de richtlijnen te geven voor de beheersing. Ten tweede: noch controlegegevens noch impulsen vanuit de leiding zijn absoluut en juist. Menselijke inaccuratesse en persoonlijke invloeden spelen hun rol. Zelfs de accuratesse van de automatisering is schijnbaar. Een cijfer kan niet actueel zijn, het kan aan iets anders refereren dan wordt verondersteld, of het kan beïnvloed zijn door onbekende effecten.
De deelname van de ondernemingsleiding in de systeemontwikkelingsfase vergroot de bekendheid met de door het systeem te produceren gegevens. Belangrijker nog, de ondernemingsleiding dient inzicht te verwerven in toekomstige ontwikkelingen en aan de hand daarvan trachten adequate strategieën, die aansluiten op de ondernemingsdoelen, te ontwikkelen. In dit kader is het nuttig te evalueren wat de status van een informatiesysteem is, welke problemen resulteren uit zwakke leiding en welke voortvloeien uit natuurlijke groei."

AUDIT CONCERNS ABOUT MINICOMPUTERS Max. Gottlieb

EDPACS, oktober 1981

Het toenemende gebruik van minicomputers zowel bij grote als bij middelgrote en kleine bedrijven, zal de accountant niet ontgaan zijn. In hoeverre hij gebruik kan maken van de werking van het systeem van interne controle in en rondom de geautomatiseerde gegevensverwerking bij toepassing van een minicomputer zal afhangen van zijn oordeel hierover. Dit oordeel kan echter niet in alle gevallen verkregen worden door bestudering van de output, met name niet, indien belangrijke controleerbare vastleggingen ontbreken. Kennis van de interne controle-aspecten van de system software en van de application software van minicomputers is dan onontbeerlijk. Het hierna opgenomen artikel behandelt beknopt de voor de accountant belangrijke attentiepunten van interne controle van minicomputers.

AUDIT CONCERNS ABOUT MINICOMPUTERS

Minicomputers are relatively inexpensive and make it easy to perform interactive programming. As evidenced by their recent 35% annual growth rate, these factors make minis very attractive to the business community. With this kind of growth, obviously they will be used more and more for applications which are of concern to the auditor.

Initially, minis were utilized for scientific and manufacturing applications where the possibility of unauthorized transactions or alterations of data were not a great concern. Furthermore, minis' low prices and somewhat frivolous name caused some people to employ them for business purposes without giving much thought to control and security considerations. Because of the relatively small size of the businesses involved and the highly integrated nature of the systems developed, minis make it difficult to provide the separation of duties an auditor seeks. In addition, the kinds and sources of software used for minis created other audit concerns. Many programmers working on commercial minicomputer applications come from a scientific environment and have little appreciation for the kinds of controls required in business data processing. Therefore, the auditor must pay particular attention to the controls provided in the minis' systems and application software.

SYSTEM SOFTWARE

Operating systems for minis were primarily designed with ease of operation in mind. Minis are intended to function in a "friendly" environment.

Consequently, they usually furnish inadequate control over data access and alteration. The auditor should be concerned with the controls within the operating system. He should give particular attention to such things as terminal authorization, passwords, protection of files, program library protection, integrity of programs, data alteration utilities, system activity logs, and system commands. A discussion of those follows.

Terminal Authorization

It is possible to limit access to some programs and records to designated terminals. This feature should be used where the ability to access or change confidential data must be restricted. For terminals with dial-up access to the system, special screening controls are needed.

Passwords

The password capabilities supplied by vendors usually offer limited protection against unauthorized use. In most cases, the password owner can access the computer and one or more specific applications or files. This level of control may be insufficient. For many applications there may be a requirement to provide for additional controls, such as having two people approve changes in receivable balances. In assigning password authority, no one individual (including the "boss") should completely control a transaction.

Recognizing that the password capabilities provided by manufacturers are usually inadequate, users may want to program their own multi-level password scheme within their application software. A discussion of all facets of password protection would warrant a separate article. However, experience has shown that four is the minimum number of characters for a password. Moreover, passwords should be assigned at random because, if clerks are permitted to select their own passwords, most will choose their own initials.

Another point is also worth consideration. If a computer can be accessed remotely, the control program should disconnect the terminal after a specified number of consecutively wrong passwords have been entered. Typically, two or three such attempts are the maximum.

Protection of Files

Normally, in order to use a minicomputer, one has to have a user ID number. Some numbers may be designated as "privileged", meaning that their owners can perform tasks not generally available to other users. If a system employs passwords to restrict the writing or reading of certain files, users having privileged ID numbers can remove such restrictions. Only one individual, therefore, should be in the privileged group.

To make sure this rule is followed, a special control program might be written to log and give access to privileged users.

Some organizations do not like to give separate ID numbers to individuals. They often assign one number to a group of users. This defeats one of the purposes of ID numbers, namely, establishing individual accountability for computer utilization.

Program Library Protection

Program libraries in minicomputer systems are usually not adequately protected against unauthorized modifications or use. Some computers do not even keep programs in a library but may intermix them with data files. In fact, in one computer, a program executed from data files runs faster than one taken from the library. A printout of the program directory, which shows each program's privilege code, may indicate the existence of bootleg (illegale) programs, or programs that have unauthorized access to protected data files.

Integrity of Programs

Many minis are programmed using a friendly version of the BASIC language. BASIC was designed to make it easier for students to debug their programs. BASIC commands, or instructions, are usually converted to machine language using "interpreter" software which converts every line of code individually as it is executed. This approach can be contrasted with a compiler which translates the entire program into machine language only once prior to execution. While running a BASIC program, it is possible to hit a special key on the keyboard, stop in the middle of program execution, change the program on the fly, and then continue running the modified program. Such a capability is very useful for debugging programs, but it presents a serious control problem because of the changes that could be made to production programs without approval and checking. The best solution to this is to use another language or a version of BASIC which must be compiled. If this can be done, the regular BASIC compiler should be removed from the production system. This will strengthen the protection against unauthorized program changes.
In many minis it is also possible to change machine language code by entering patches from the keyboard. Patching is error-prone, dangerous, and uncontrolled. The use of patches should be forbidden.

Data Alteration Utilities

A standard feature of most minis is data alteration utilities. They permit changes in files and programs, hence make it difficult to control unauthorized changes. In addition, almost every mini has an EDIT utility.
These utilities may also be used by the operating system to perform routine functions such as disk access, making it very hard to remove the utilities from the system. If it is impossible to remove such utilities from the production system, consideration should be given to disabling some of their more dangerous functions.

System Activity Log

This log provides information that can be used to identify processing errors, unauthorized use of computer programs or utilities, use of patches, and other non-routine events. Unfortunately, some minicomputers do not produce full activity logs. In other systems it is possible to suppress the production of the activity log. There are also minis on which the console function may be reassigned to another unit; e.g., any terminal may be designated the console. In fact, reassignment of the console function may even be concealed by issuing the proper command prior to the reassignment. In such situations, the hard copy console log will be of little help to the auditor. However, a control program that will detect a console change can be written. When a log capability does exist, it is often useful to capture log data on disk for subsequent review. The auditor may then select and print the data needed to meet audit objectives. Volume of data may make review of an entire log an impractical exercise.

System Commands

These are used to invoke programs, identify files, override dates, and perform other operations that may circumvent controls. Since the manual entry of a series of commands by a console operator may cause or result in errors, the commands associated with a given job should be catalogued. The catalogued string of commands is then invoked by a single command from the console operator. An additional improvement would be to write the application program so that a step in a job will not be executed if there is a serious error in the preceding step. A similar capability is provided by IBM's job control languages. A special code is passed between job steps and the user has the option to abort execution upon the occurrence of an error.

APPLICATION SOFTWARE

Most minicomputers have less sophisticated system software than have the larger computers, so application programs must be used to implement certain control functions. For example, user coding must often be employed to accomplish label checking, recovery, batch and file balancing, maintaining audit trails, and developing information for performance measurement. These control measures are discussed below.

Label Checking

Many minis cannot perform tape label checking, so a wrong tape can be processed. When using tapes, programs should create and check labels, or header records, to determine that the right tape is being used as input. Disk label checks are usually furnished by the minicomputer's system software.

Recovery

In the event of a computer failure, recovery procedures must be available. It is difficult in an online system to determine which inputs were accepted and which files were updated prior to a failure. Ideally, a recovery system should log every input transaction and record images of master records before and after each update. Since such extensive logging is difficult to implement and tends to slow response time, a lower level of automatic recovery is usually provided. Such limited recovery may capture only the input transactions or only the master record images after the updates. Obviously, this is not enough information to accomplish a full recovery automatically. Some transactions may have to be manually reentered.

Batch Balancing

Most minis operate in an on line mode. However, it is often useful to enter financial data from manually prepared batches of transactions. Batch balancing helps to assure that no entries are missing and that most transposition errors (fouten tijdens data-entry) have been caught.
There is always the problem of what action should be taken when a batch does not balance. Experience indicates that two practical answers are available: (1) Either write the entire batch on a suspense file without updating the master files, or (2) update the master files but keep the out-of-balance batch in a suspense file. The system should also be designed to prevent the closing of an accounting period if there are any batches still in the suspense file.

A further control involves maintaining totals of all batches submitted for entry. A clerk can enter this total into the system at the end of the day and have the system compare the control total to the computer-accumulated total for the day. Any differences should be printed out for subsequent managerial review. The clerk(s) who entered the control total should not be allowed to reconcile and balance the batches.

File Balancing

A common procedure for controlling file updates involves the reconciling of file totals with predetermined control figures. The total of the file before update plus the net total of the input transactions should equal the file total after update.

Application Audit Trails

Mainframe computer systems usually employ an on line monitor or data base system to generate a transaction history log. Minicomputers, for the most part, do not have this capability. Audit trails must be programmed by the application programmer. Auditors should request that such trails be designed into any new system.

In addition to keeping a transaction entry log, it would also be useful to institute and enforce a hard and fast rule that no change can be made to an important record without recording that change on a log. The log record should include the identification of the person who made the change.

Performance Measurement

This can be an audit tool. It provides a measure of the time required for all jobs. In addition to helping an installation tune the system, these timings may be used to detect programming errors. For example, if it takes twice as long as usual to run a stable routine production program, there may be an erroneous table search taking place or some additional, unauthorized program steps may have been added.

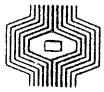
CONCLUSION

In addition to the control problems involved, auditing minicomputer systems is difficult because the number of retrieval packages which will function in a mini environment is limited. It is not easy to develop such general purpose retrieval software since there is a wide variety of disk file structures and formats employed in minicomputer systems. One practical approach to the audit of interactive minis is to use an integrated test facility (ITF). As an audit technique, ITF partially compensates for the lack of retrieval packages and logging capabilities.
Clearly, minicomputer systems are a distinct challenge to the auditor. They are often more difficult to audit than larger systems. In dealing with minis, the auditor must be well versed in computer technology.

Max Gottlieb is EDP audit consultant with Main Hurdman in New York City. Before joining his present firm, he worked for over three years as an EDP auditor at Citibank. His prior background includes more than 10 years of system design.

NOTE: This article illustrates the importance of audit involvement in the system development process of financial applications to be implemented on minicomputers.
Such involvement would help to minimize the audit, control, and security problems often accompanying mini use. The first experience many auditors have with mini installations, however, is of a "fait accompli" with poor controls and auditability.

We should like to hear from readers about what they been able to do about such existing "time bombs" as well as what other audit approaches have been used with minis and micros. -Editor.



compact

winter 1981/1982

Automatisering
Beveiliging
Controle
NIEUWS

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

Automatisering

In het nieuwjaarsbericht van de Directeur-generaal van de PTT, drs. Ph. Leenman, wordt de spoedige start aangekondigd van het openbare netwerk voor digitaal gegevenstransport Datanet 1. Computable van 15 januari 1982 wijdde hieraan een artikel waaruit wij enige fragmenten laten volgen.

Leenman belooft: 'Datanet 1 komt in maart in gebruik'

Gegevensverkeer ook via telefoon

De Europese PTT's verwachten veel van deze nieuwe telecommunicatiemogelijkheid. Een onderzoek van 1979 kwam uit op een verwachting van meer dan tienduizend aangeslotenen in Europa in 1985. Overigens denkt Leenman niet dat de digitale gegevensoverdracht snel helemaal zal verlopen via Datanet 1. Het gewone telefoonnet zal ook veel gegevens blijven transporteren. In 1985, zo verwacht de PTT, zal nog zo'n veertig procent van het digitale gegevensverkeer via het telefoonnet lopen. Dat zal het dubbele van het Europees gemiddelde zijn; volgens Leenman vanwege de goede kwaliteit van het Nederlandse telefoonnet.
De '1' van Datanet 1' zou er wel eens snel kunnen afslijten. Volgens ir. C. Wit, hoofddirecteur Telecommunicatie van de PTT, is van een 'Datanet 2' voorlopig nog geen sprake. Vroeger is een 'Datanet 2', dat evenals de telefoon werkt met geschakelde verbindingen - Datanet 1 werkt met van sleutelwoorden voorziene berichten - wel overwogen, maar Datanet 1 blijkt zo flexibel dat een ander netwerk niet nodig is. "Mochten we meer mogelijkheden voor gegevensverkeer in het leven roepen," zo stelt Wit, "dan zou het toch eerder een Datanet 1a worden, dan een geheel nieuw Datanet 2".

Driemaandelijks wordt door het tijdschrift Computable in samenwerking met het Londense bureau Urwick Dynamics een gebruikersonderzoek gehouden bij de Nederlandse rekencentra. In november 1981 had dit voor de derde maal plaats. Daardoor wordt het thans mogelijk de enqueteresultaten met elkaar te vergelijken en er een mogelijke trend uit af te lezen. In Computable van 22 januari 1982 zijn de volledige resultaten afgedrukt. Wij laten hierna alleen die resultaten volgen die wijzen op ontwikkelingen van belang voor de accountantscontrole.

Computergebruikers in Nederland lijken wat optimistischer

Tendens tot decentralisatie zet zich verder door

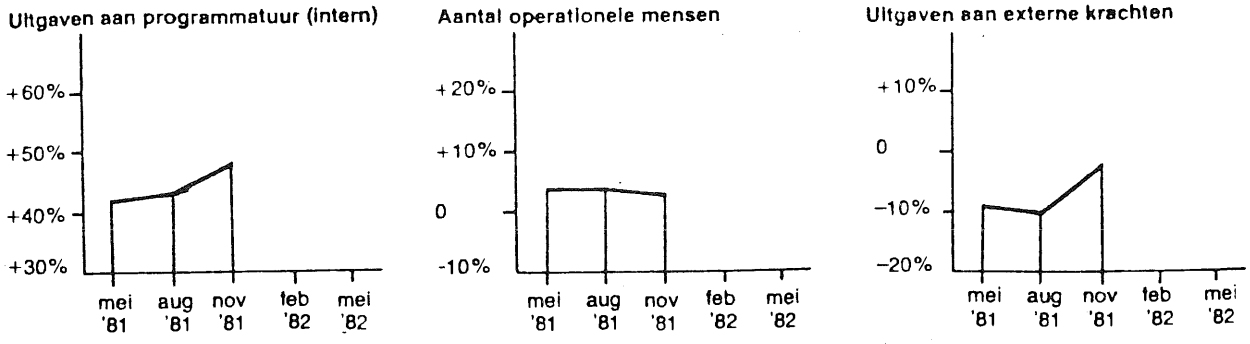
Wanneer men uit het derde Urwick/Computable onderzoek de diverse saldi (het verschil tussen verwachte stijging en daling) bekijkt, dan schijnt het dat de Nederlandse computergebruiker wat programmatuuruitgaven betreft, iets meer denkt te kunnen besteden dan eerder dit jaar werd verwacht. De vooruitzichten voor het personeel zijn echter nogal wisselvallig, afhankelijk van de verschillende categorieën.

Kleine gebruiker past meer op centen

Gemeten naar het saldo kunnen er voor de komende twaalf maanden volgend op november vorig jaar ongeveer gelijkblijvende apparatuuraankopen als bij voorgaande onderzoeken worden verwacht. Dit is met name te danken aan de grotere gebruikers, die kennelijk optimistischer zijn geworden ten aanzien van hun budgetten. Bij de kleinere gebruiker ligt het echter anders, hetgeen mag worden geconcludeerd uit het aanmerkelijk hogere percentage, dat een gelijk bedrag als vorig jaar of minder denkt uit te geven.
De verwachte uitgaven aan zelf te ontwikkelen of van de apparatuurleverancier te betrekken programmatuur zijn hoger dan voorheen. Een lichte stijging in het verwachtingspatroon dus, maar sterk gevoed vanuit de grotere rekencentra. De kleine gebruikers letten hier eveneens scherper op de centen. Toch is de continu stijgende lijn zelfs bij de kleinere opmerkelijk. Zou de huidige economische recessie dan toch een stimulerende invloed op de automatisering hebben?

Situatie op personeelsgebied

Ten aanzien van het (verwachte) uitbreiden van het aantal programmeurs en systeemanalisten in vaste dienst, lijken de computergebruikers wat voorzichtiger te worden. Zowel het aantal bedrijven, dat tot uitbreiding wil overgaan, als het saldo daalt. Toch geven deze gemiddelde cijfers wellicht een enigszins vertekend beeld, daar het juist de grote(re) gebruikers zijn die meer geneigd lijken hun staven uit te breiden. Bij de kleinere gebruikers leeft kennelijk sterk de wens het met hetzelfde aantal mensen af te kunnen. Opvallend is, dat er vrijwel niemand de staf wil inkrimpen.
De situatie van de operationele staf (werkvoorbereiding, operateurs, gegevensvastlegging, beheerders en dergelijke) lijkt beduidend minder rooskleurig. Het saldo is weliswaar nog positief, maar dit is eveneens het gemiddelde. Juist de grotere bedrijven geven te kennen dit type personeel op kleinere schaal in dienst te willen hebben.
En gaat men daar inkrimpen, dan komen de klappen over de gehele linie het hardst aan. De positie van uitzendkrachten verbetert zo te zien iets, maar blijft wankel. Van de gebruikers zegt 23 procent in de komende maanden minder te willen uitgeven aan het aantrekken van automatiseringspersoneel van buitenaf. Daarentegen stijgt wel het aantal dat denkt weer meer mensen op free-lancebasis in te gaan huren.



Het saldo - zij het aanmerkelijk aangetrokken - blijft echter negatief.
Meer personeel van buiten aantrekken wil met name de middelgrote gebruiker. Maar de grote gebruiker zegt dit over het algemeen minder dan het gemiddelde te willen doen.

Meer geld naar eindgebruiker

De steeds voortschrijdende tendens tot gedistribueerde gegevensverwerking of decentralisatie is uiteraard ook uit de onderzoekresultaten te halen. De eindgebruiker krijgt voor eigen automatiseringspersoneel, apparatuur en programmatuur nu al bij 53 procent van de gebruikers meer geld ter beschikking. Bij 42 procent blijft daarenboven zijn budget ongewijzigd. In de twee vorige onderzoeken schommelden deze twee percentages nog rond de 48, 49.
Het zal weinigen verbazen, wanneer het onderzoek hierbij aangeeft, dat het de middelgrote en vooral de grote gebruikers zijn, die de eindgebruiker meer en meer computerhulpmiddelen ter beschikking willen stellen. De meerpercentages lopen daarbij van 52 tot aan maar

liefst honderd procent. Interessant is het echter om te zien dat ook nog boven de veertig procent van de kleine gebruikers verwacht meer geld op dit terrein te gaan spenderen.

Onderhoud blijft grootste probleem

In het Urwick/Computable onderzoek wordt tevens gevraagd naar de drie voornaamste problemen, die men in het huidige werk onderkent. De twijfelachtige eer van koploper, percentagegewijs gezien, valt hierbij onveranderd ten deel aan het programmatuuronderhoud. Vrijwel de helft van de gebruikers heeft op dit gebied grote problemen. Alleen de grootste en kleinste gebruikers uit het onderzoek scoren lager dan het gemiddelde, bijna alle overige categorieën zitten er boven.
Het halen van 'deadlines' blijkt binnen de Nederlandse automatisering het op een na grootste probleem, alhoewel daar de kleine gebruikers iets minder moeite mee schijnen te hebben dan de grotere. Het is en blijft echter over alle drie onderzoeken probleem nummer twee.

Bij de bespreking van het Urwick/Computable onderzoek wordt diverse malen gesproken van kleine, middelgrote en grote gebruikers. Alhoewel bij de enquête zelf de diverse bedrijfsgroottes precies zijn afgebakend, wordt bij de uiteindelijke publicatie erover een wat globalere indeling gehanteerd, waarbij een kleine gebruiker tot ongeveer honderd werknemers in dienst heeft, een middenklasser honderd tot duizend en alles wat daarboven komt, heet groot.

Voor de accountantscontrole kan uit het onderzoek worden afgeleid dat er veranderingen in de organisaties bij meer cliënten dan voorheen kunnen optreden door het brengen van automatisering bij de gebruiker. Of door middel van een lijnverbinding met een centrale computer, óf door middel van kleinschalige apparatuur. De tendens tot kostenbesparing kan tot gevolg hebben dat concessies worden gedaan aan de interne controle en de controleerbaarheid van de automatisering.
Problemen met programmatuuronderhoud kunnen tot gevolg hebben dat systemen verouderen en foutsituaties blijven bestaan.
Vandaar dat wij hiervan enkele delen laten volgen van een interview dat de Automatisering Gids had met James Martin.

JAMES MARTIN OVER ZIJN BOEKEN EN OVER DE TOEKOMST

"DE FACTOR ONDERHOUD MEER SERIEUS NEMEN"

"De kosten van het onderhoud van programmatuur zijn erg hoog. Veel hoger dan de mensen meestal durven toegeven. Van dat geld zit een flink deel in arbeidsuren. Dat betekent dat je minder mankracht overhoudt voor applicatie-ontwikkeling en dat er nogal wat weerzin bestaat tegen het veranderen van bestaande software bij het top-management. Het is dus uitermate belangrijk de factor onderhoud serieus te nemen."

Aan het woord is James Martin over gegevensverwerking.

Je kunt niet de mensen krijgen die je nodig hebt

De in de aanhef geciteerde conclusie dat het onderhoud als kostenfactor serieus genomen moet worden is een deel van het antwoord op onze vraag of de vraag naar programmeurs zal gaan dalen wanneer de gebruiker zelf in staat wordt gesteld aan applicatieontwikkeling te gaan doen. "Er moet nog altijd geprogrammeerd worden, ondanks de nieuwe talen.
Alleen wordt er vandaag de dag erg veel in Cobol geprogrammeerd wat helemaal niet in Cobol zou moeten. Cobolprogramma's zijn erg duur in het onderhoud. De uitgaven voor het onderhoud van Cobolprogrammatuur worden verschrikkelijk. Een van de boeken waar ik momenteel aan schrijf geeft een overzicht van ervaringen op dat gebied.
Voor programmeurs zal er zeker een goede markt blijven bestaan."

In het tweedelige werk van de schrijvers Martin en Finkelstein, "Information Engineering", is een bijzondere plaats ingeruimd voor applicatie-ontwikkeling zonder programmeurs, waarover Martin eerder dit jaar ook al een bestseller schreef. Martin: Het gaat over een set in elkaar grijpende methodologieën om een informatiesysteem op te zetten. Een van de principes daarbij is dat je de gegevens binnen een bedrijf zo kan ontwerpen dat de gegevensstructuren relatief stabiel zijn. Als je alleen procedures ontwerpt betekent dat dat die vrijwel nooit stabiel zijn. Procedures wil iedereen altijd veranderen. De meeste gegevensverwerking is tot nu toe gedaan met procedure-georiënteerde structuurtechnieken. Wanneer je procedures ontwerpt verschijnt de data bijna als een bijprodukt. Bij Information Engineering proberen we de gegevens zo stabiel mogelijk te maken en dan met krachtige hulpmiddelen daar de applicaties boven op te bouwen. Een heel belangrijke basis hiervoor is de data-modelling procedure. Naar mijn mening moet data-modelling worden geautomatiseerd en moet ze ook met gecomputeriseerde gereedschappen up to date worden gehouden. Soms kun je de modellen meteen maken, soms zijn daar heel ingewikkelde procedures voor nodig. Wij zoeken een soort van chartingtechniek, die simpel genoeg is om door de gebruiker te worden gehanteerd en die de procedures kan vermijden. Je vervalt daardoor wel onvermijdelijk in talen van de vierde generatie.

Bij de keuze van de programmeertaal dient derhalve al rekening gehouden te worden met de onderhoudbaarheid van de programmatuur.
Dat deze keuze ook vanuit performance problematiek belangrijk kan zijn, volgt uit het resultaat van een discussiebijeenkomst van IBM Systeem 38 gebruikers. Uit het in Computable van 8 januari 1982 opgenomen artikel inzake de gebruikerservaringen nemen wij enige fragmenten over.

Gebruikers van IBM's Systeem 38 geven hun mening

RPGIII vijf maal sneller dan Cobol

Met name de groep gebruikers van de kleinere modellen uit IBM's 370 serie laten bij de keus tot aanschaf van een 4300 model of het Systeem 38 de voorkeur op de laatste vallen. Met deze ontwikkeling geconfronteerd tijdens diverse sinds 1980 georganiseerde bijeenkomsten met 4300 gebruikers, besloot het Amsterdamse softwarehuis Share Nederland, op verzoek van vele deelnemers, tot een discussiebijeenkomst voor geïnteresseerde gebruikers en potentiële gebruikers van IBM's Systeem 38 eind vorig jaar. Doel van de bijeenkomst was onder meer het uitwisselen van tips en het inventariseren van een aantal positieve en negatieve feiten.

Opvallend is de positieve waardering van RPGIII. Met RPGIII, als meest gebruikte programmeertaal voor het Systeem 38 kon volgens enkele aanwezigen ongeveer vijf maal sneller worden ontwikkeld dan in Cobol. Een aantal van 1.500 programma's door 7 programmeurs in 10 maanden werd genoemd en: "Een systeem dat in Cobol een jaar ontwikkelingstijd vergt, is in RPGIII in drie maanden klaar." De systeemprogrammatuur werkte op de geïnstalleerde systemen zonder problemen; niemand had tot nu toe fouten geconstateerd. De oorspronkelijke door IBM geleverde conversieprogrammatuur voldeed minder goed, maar met de nu beschikbare Canadese 'utility' blijkt probleemloos te kunnen worden geconverteerd van Systeem 3 naar Systeem 38.
Positieve berichten waren er eveneens voor het vooraf converteren op het IBM Servicecentrum, waar de geboden ondersteuning snel werken mogelijk maakte. Minder positief was men over het wegschrijven (saven) van schaduwbestanden. Door geselecteerd weg te schrijven, werd tijd bespaard, maar weer problemen ondervonden bij herstel (recovery); tijden van vier uur per keer werden genoemd.
Slecht werden over het algemeen de responsetijden genoemd. Bij een nachtelijke verwerking stapelsgewijs (batch) werden tijden van vijf tot twintig seconden gemeten. Het meest storend was dit bij programma's met opvraagfuncties (queries). Een oplossing is het uitbreiden van het geheugen of een snellere processor.

Nog meer nieuws over het Systeem 38 komt van IBM zelf (IBM NIEUWS, december 1981):

Financieel administratiepakket voor Systeem 38

Op 4 september 1981 is het financiële administratiepakket voor Systeem 38 aangekondigd onder het programmanummer 5788-HWP.

Het pakket is geheel opnieuw geschreven en ontworpen met als basis de functies van het financieel pakket S/34 met kostenplaatsen/-soorten.

Bij het ontwerp is men uitgegaan van de volgende punten:
- volledig gebruik van Systeem 38 functies;
- data base ontwerp om modificaties en uitbreidingen optimaal mogelijk te maken;
- menu concept met groepering naar functie;
- invoer met controle op sluiting per boekstuknummer, controlelijst per beeldstation;
- onbeperkt multiple workstation gebruik;
- vreemde valuta voor openstaande posten;
- kostenplaatsen intracomptabel opgenomen;
- veldlengtes uitgebreid;
- open "ontwerp" om aanpassingen en uitbreidingen mogelijk te maken;
- inquiries;
- scherm conventies/commandotoets gebruik als gedefinieerd bij de utilities van Systeem 38.

Verwerking

Voor de invoer van journaalposten is gekozen voor het z.g. trechterprincipe: dat wil zeggen, dat alle transacties als journaalpost worden ingevoerd en gecontroleerd. Alleen correcte en sluitende posten worden voor verwerking toegelaten en dan consequent doorgeboekt naar alle gezichtspunten.

- Zowel scherm- als diskette-invoer is mogelijk.
- Meer filialen kunnen naast elkaar worden verwerkt.

De "dagelijkse" verwerking wordt gestart per batchnummer.
De betreffende journaalposten worden veilig gesteld, geëxplodeerd voor kostensoorten/-plaatsen, koersverschillen, BTW, korting etc. en vervolgens verwerkt in het Grootboek, de kostenplaatsen en openstaande posten.
Dagboeken worden afgedrukt op afroep.

In het periode/jaarwerk worden "vergeten" dagboeken automatisch aan het begin van het periodewerk door het systeem afgedrukt.
De keuze bestaat uit twaalf of dertien perioden.
Er is een restperiode veertien die niet door de gebruiker benoemd kan worden maar door het systeem wordt gebruikt om jaarwerk-correcties te verwerken.

De mogelijkheid bestaat om een "voorlopige" balansovername te maken bij de overgang naar het nieuwe boekjaar.
De overzichten die daarvoor in aanmerking komen krijgen wel een indicatie dat de bedragen "voorlopig" zijn.

Het rekeningschema en het kostenplaatsen/-soorten bestand zijn geldig voor het oude en het nieuwe boekjaar en behoeven derhalve niet per boekjaar opnieuw opgegeven te worden. Dit is vooral belangrijk om de balansovername etc. werkbaar te maken.
Tenslotte kunnen allerlei overzichten worden vervaardigd, zoals Controle-overzichten, Dagboeken, Grootboek-overzicht, Sub-grootboek-overzicht, Saldilijst, Rekeningschema, Begrotings-vergelijkingsoverzicht, Proef- en saldibalans en Winst-en-verliesrekening.

Zoals aangeduid is één van de principes het z.g. "open ontwerp". Dit houdt in dat het pakket kan worden aangepast aan de behoefte van de gebruiker. Het open ontwerp impliceert tevens dat in het systeem opgenomen controlemiddelen uitgeschakeld kunnen worden. In iedere situatie zal derhalve beoordeeld dienen te worden of het pakket op de juiste wijze wordt geïmplementeerd.
Computers worden doorgaans toegesproken in hogere programmeertalen, bestaande uit een aantal korte Engelstalige instructies. Dat dit ook anders zou kunnen blijkt uit een artikeltje in NRC Handelsblad van 17 december 1981:

COMPUTER OP KOMST, DIE DUITS VERSTAAT

Tot nog toe bleef, behalve in Amerika, de communicatie met computers beperkt tot een soort geheimtaal. Die geheimtaal was de taal van de computer; er zijn er een serie van en ze worden programmeertalen genoemd. Wilde men zich van de computer bedienen dan moest men een programmeertaal leren. In deze toestand begint verandering te komen. Overal houden computerliguisten zich bezig met de ontwikkeling van de z.g. 'natuurlijke computer' dat wil zeggen computers die ook in gewone taal kunnen communiceren met mensen.

Het eerste succes werd in dit opzicht geboekt door T. Winograd in het begin van de zeventiger jaren. Hij ontwierp een computer die opdrachten in normaal Engels kon begrijpen en uitvoeren. In Amerika

is deze ontwikkeling doorgegaan. Zo werd in Palo Alto (Californië) een computer ontwikkeld waarmee men in dialoogvorm een vliegreis kan boeken.
De eerste computer die in Europa in gewone taal kan worden aangesproken staat in Hamburg, waar onlangs het project "Hamburger Redepartnermodell" (HAM-RPM) werd afgesloten. Met deze computer kan men in dialoogvorm verkeerssituaties bestuderen en een hotelkamer boeken. Het succes van HAM-RPM heeft ertoe geleid dat nu een project is gestart waardoor de toepasbaarheid van de computer met natuurlijke taal algemener zou moeten worden.
Men hoopt zover te komen dat men in het Duits samen met de computer kan discussiëren over moeilijke onderwerpen om zodoende een sneller inzicht in en betere oplossingen voor dergelijke moeilijke problemen te vinden. Met het nieuwe project dat HAM-ANS (Anwendungsorientiertes Sprachliches System) zijn drie en een half jaar en 1.700.000 D-mark gemoeid.

Namen wij in het vorige nummer van Compact (pag. 66) een terugblik op Computer '81 in de Rotterdamse Ahoy op, nu troffen wij aan een voor-aankondiging van Computer '82.
Belangstellenden kunnen de data vast noteren.

Tenslotte ter afsluiting van het onderdeel Automatisering deze uit de rubriek "Bits" in Computable.

Toppunt van vakidiotisme:
Je hond Mega noemen en
een bordje in de tuin zetten met
'Pas op, Mega byt'.

Beveiliging

In de laatste jaren heeft het veiligheidsbewustzijn, alsook de noodzaak tot veiligheid een sterke verandering ondergaan.
Deze duidelijk merkbare veranderingen hebben zich voorgedaan in de prsoonlijke en de publieke sfeer. Vrijwel iedereen is gevoeliger geworden ten opzichte van niet altijd definieerbare bedreigingen en ongewenste openheid van zaken. In deze materie staat de werkomgeving sterk op de voorgrond.

Met deze woorden wordt een artikel ingeleid in De Automatisering Gids van 23 september 1981 van de hand van de Duitse Dipl. Ing. Wolfgang Merz.
In de afgelopen 6 jaar heeft hij zich beziggehouden met een studie betreffende toegangsbeveiligingen. In dit artikel houdt Merz een pleidooi voor een andere denkwijze wat betreft de regulering van personenverkeer. Pasklare systemen presenteert hij niet, doch veeleer een oplossingsmethodiek.
Uit dit artikel nemen wij de belangrijkste fragmenten over.

Veiligheid paren aan zoveel mogelijk vrijheid

Een nieuwe kijk op toegangsbeveiligingen

Al direct wordt de integere portier als de beste bescherming gezien en anders wel een 'closed-shop' oplossing, zoals die bij computercentra en kerncentrales voorkomt. In de laatste situatie speelt toegangscontrole-apparatuur een belangrijke rol. Helaas wordt er dan geen rekening gehouden met de samenhang tussen beveiligd werken, veilig werken en ongehinderd werken. Met andere woorden, er worden slechts deelproblemen opgelost.
Tenslotte gaat het niet alleen om het blokkeren van toegangen of het weren van onbevoegden. Het gaat veeleer om een totaalpakket van in elkaar grijpende beschermingsmaatregelen, die zowel de interne als de externe veiligheid waarborgen.
Het valt niet te ontkennen, dit is overigens al meermalen vastgesteld, dat de meeste gevaren van binnenuit komen. De bescherming van de onderneming wordt pas gewaarborgd door strenge controle en bewakingstechnieken, die in werking treden nadat toegang is verleend. Hierbij zou elke gekozen oplossing het volgende motto moeten hebben: 'Zoveel vrijheid als mogelijk, en zoveel veiligheid als nodig. En niet omgekeerd."

Te beveiligen gebieden

De wetgevende instanties hebben een wetsontwerp ingediend betreffende de bescherming van persoonsgegevens. Ook ondernemingsgegevens hebben behoefte aan een dergelijke bescherming. Bij beveiliging wordt aan dit soort gegevens dan ook het eerst gedacht. Maar ook gecompliceerde apparatuur - en dat hoeft niet uitsluitend computerapparatuur te zijn - moet beschermd worden.
Juist de produktiemachines en de verzorgingsapparatuur van de werkomgeving dienen te worden beschermd tegen sabotage, misbruik, onjuiste bediening en uitval. De meeste bedreigingen komen in deze voorbeelden van binnenuit.
Wat ook niet uit het oog mag worden verloren is de bescherming tegen ongevallen. Zulks kan geschieden door mensen uit het bedrijf te weren die niet vertrouwd zijn met de omgeving. Bedrijven waarvoor een dergelijke aanpak in het bijzonder geldt zijn bijvoorbeeld laboratoria, kerncentrales en in het algemeen bedrijven waar met gevaarlijke stoffen wordt gewerkt.
Een andere gevaarlijke situatie kan optreden, wanneer het aantal aanwezige personen een maximum overschrijdt. Iedere aanwezige kan op zich gerechtigd zijn tot toegang, doch de combinatie van al diegenen zorgt voor een gevaarlijke situatie.

..... (einde citaat; nieuw citaat volgt)

Er valt een reeks van redenen te noemen, om over te gaan tot een gereguleerde bescherming tegen diefstal, bedrog, misbruik of verkeerd gebruik, ongelukken en fraude. Vooral fraude is in zeer veel gevallen mogelijk gebleken doordat de mensen op bepaalde tijden ongeoorloofd ergens aanwezig konden zijn. Wat ook zeker niet uit het oog mag worden verloren is een beveiliging tegen het lastigvallen van het personeel.
Vanuit psychologisch gezichtspunt en ook door kostenoverwegingen is het vrijwel onmogelijk om bij iedere deur de reeds genoemde integere portier in wisseldienst te plaatsen. Dat zou er overigens op lijken, alsof men met een kanon probeert vliegen dood te schieten. De andere mogelijkheid, toegangscontrole apparatuur, biedt ook niet het summum aan beveiliging. Er zijn slechts twee mogelijkheden, er wordt toegang verleend, of, er wordt geen toegang verleend.
Er zijn echter situaties, waarbij toegang verleend mag worden op basis van bijkomende factoren. Zo kan het zijn, dat normaliter toegang wordt verleend, maar dat onder invloed van tijdscondities, speciale gebeurtenissen of andere redenen de toegang toch beperkt dient te worden.

.....

Functies

Afhankelijk van de combinatie van veiligheidswensen en noodzaak tot beveiliging worden maatregelen getroffen. In de praktijk zijn deze maatregelen voor iedere bedrijfssituatie verschillend, maar er is

een aantal wezenlijke functies te noemen, die in alle gevallen voorkomen. Deze functies zijn:

- Het reguleren van de bewegingen van personen door het invoeren van beperkingen bij in-, door- en uitgangen.
- Het afsluiten van ruimten en terreinen.
- Bewaken van de beveiligingsinrichtingen in samenhang met de hiervoor genoemde punten.
- Bescherming van personen in geval van rampen of panieksituaties door het vrijgeven van vluchtwegen.
- Het vastleggen van gebeurtenissen binnen de beveiligde omgeving.

Een bijkomend aspect is, dat de genoemde functies op elkaar zijn afgestemd. Met andere woorden, de functies moeten in verbinding met elkaar werken. Een ander belangrijk punt is, dat zij aanpasbaar zijn aan tijdscondities. In de avonduren gelden andere toegangsrechten dan overdag en in het weekend gelden weer andere rechten dan op doordeweekse dagen.

Dynamisch probleem

Het is niet voldoende om slechts een oplossing te maken voor een huidig probleem, er moet wel degelijk bij een dergelijke beveiliging naar de toekomst worden gekeken. In die toekomst kunnen namelijk veranderingen optreden, die een wijziging in het beveiligingssysteem nodig maken. Dergelijke veranderingen kunnen al binnen afzienbare tijd optreden, en zij hoeven niet eens van permanente aard te zijn. Zo kan er bijvoorbeeld een onvoorziene verbouwing van bedrijfsruimten plaatsvinden, of kan worden besloten tot een tijdelijke opslag van belangrijke documenten. Op dergelijke situaties zal het beveiligingssysteem aangepast moeten worden.
Een beveiligingsprobleem draagt dus een dynamisch karakter. Hierdoor moet de beveiligingsinstallatie aan enkele voorwaarden voldoen. De interne voorwaarden binnen het systeem moeten te veranderen zijn, doch ook de vorm en samenstelling van het beveiligingssysteem moeten eenvoudig gewijzigd kunnen worden.

Systeemoplossing

Om aan de hiervoor genoemde voorwaarden te kunnen voldoen dient te worden voorzien in een centraal opgestelde 'Intelligentie'. Dit intelligente hart van het systeem dient in verbinding te staan met alle beveiligde toegangen, de daarbij horende apparatuur alsmede alle bij de beveiliging betrokken personen. Die personen bestaan uit de beveiligingsbeambten, degenen die de toegangsregels bepalen en zij die van de status van het systeem constant op de hoogte moeten zijn. Ook moet die centrale intelligentie zelf te modificeren zijn. Als de genoemde centrale intelligentie kan men zich bijzonder goed een computersysteem voorstellen.

.....

In dit centrale concept is het zeer belangrijk, dat een stringente scheiding wordt gehanteerd tussen twee zaken: het 'pasje' en het toegangs- c.q. aanwezigheidsrecht. De koppeling tussen beide zaken mag slechts vanuit een bepaalde plaats tot stand worden gebracht. Het spreekt vanzelf, dat die centrale plaats alsmede de programmatuur van het systeem nog eens extra beveiligd moeten worden.
Een bijkomende voorwaarde is, dat alle mechanische constructies binnen het beveiligingssysteem met de hand bediend moeten kunnen worden. Tevens moet in een noodgeval de toegang tot het systeem worden geregeld. Vanwege de vereiste flexibiliteit dienen de toegangsvoorwaarden in de software vastgelegd te worden. Hiermee voorkomt men voortdurende veranderingen aan de hardware en de daaruit voortvloeiende investeringen.

.....

Personen Verkeerssysteem (PVS)

In de praktijk komt een en ander erop neer dat iedereen, die in het gebouw aanwezig is, de beschikking heeft over een pasje. Deuren van beveiligde ruimten zijn dan aan beide zijden voorzien van een leesapparaat. Doordat in het centrale systeem is vastgelegd wie over welk pasje beschikt en wat de bevoegdheden van de persoon zijn, ontstaat een waterdichte beveiliging. Iedereen komt slechts op de plaats waar hij of zij mag komen en binnen de tijdsgrenzen welke aan die toegang zijn verbonden.
Een Personen Verkeerssysteem is dus een beveiligingssysteem, waarin de navolgende mogelijkheden zijn gedefinieerd:

- Tijdprofielen en geldigheidsduur van het recht tot toegang. Gedacht kan worden aan ploegendiensten, weekend- en avondsluiting van de ruimten en bepalingen die gelden voor bezoekers.

- Ongelijksoortige toegangsmogelijkheden. In het systeem zijn opgenomen: deuren, sluizen en tourniquetten en, wat zeer belangrijk is, bepaalde kastdeuren.

- Verschillende toegangscombinaties, bijvoorbeeld enkelvoudig, paarsgewijs of meervoudig.

- Beheersing van de aanwezigheid. Als een vooraf ingesteld maximum aantal aanwezigen is bereikt wordt geen toegang meer verschaft.

- Persoonlijke toegangstijden.

- Continu volgen van bewegingen van personen. Op die manier is bekend waar een ieder op elk moment is, hetgeen vooral in noodgevallen van groot belang is.

- Mogelijkheden om de verschillende onderdelen van het systeem buiten werking te stellen, zonder de functionaliteit van het geheel aan te tasten. Dat laatste kan voorkomen bij onderhoud, defecten of het wegvallen van de noodzaak tot beveiliging.

Het aantal te bewaken/regelen passageplaatsen dient uiteraard variabel te zijn. Wil een dergelijke PVS kunnen functioneren als een stuk gereedschap voor het beveiligingspersoneel, dan is een voortdurend overzicht van de situatie van belang. Met behulp van een dergelijk overzicht komt bestuurd ingrijpen binnen de mogelijkheden te liggen. Bijkomende factoren zijn dan nog nodig. Deze bestaan uit:

- Constante bewaking van de beveiligingsapparatuur en de foutmelders.

- Aanwezigheid van alarmschakelingen, die actief worden bij ongeoorloofde acties en ongewenste systeemtoestanden.

- Bescherming tegen 'mishandeling' van het systeem, dat wil zeggen ongeoorloofde manipulaties.

- Registratie en opslag van alle gebeurtenissen die binnen het systeem optreden.

- Speciale besturingsfuncties voor noodgevallen.

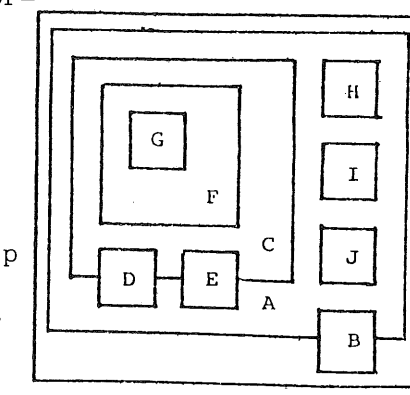
- Een eenduidige rapportage betreffende de opgeslagen informatie.

Overzicht

Voor het beschermen van gebouwen en ruimten met betrekking tot het personenverkeer heeft men ruwweg de keuze uit drie verschillende technische hulpmiddelen.

1. Toegangscontrole met elektronische sleutel.
2. Personen Verkeers Systeem.
3. Automatisch PVS.

De eerste mogelijkheid heeft als voordelen, dat het systeem relatief eenvoudig van opzet is, en daardoor goedkoop te realiseren is. Voorts is het systeem decentraal, redelijk bestand tegen hardwarefouten, maar mist het de nodige registratiemogelijkheden.
De tweede mogelijkheid is complex, centraal van opzet en constant veranderbaar. Een informatiesysteem is in deze oplossing geïntegreerd. De derde mogelijkheid, een automatisch PVS, is zeer complex van opbouw erg kostbaar en vol van extra speciale beveiligingseisen. Een dergelijk systeem is uitermate geschikt voor technisch of administratief zeer kritische omgevingen.
Bij de eenvoudige toegangscontrole met behulp van een elektronische sleutel verkrijgt men toegangsrecht op basis van een pasje. Iedereen die dus een pasje heeft, krijgt toegang. Bij de PV systemen is het bezit van het pasje niet direct een vrijbrief om toegang te krijgen.



In een schema weergegeven is dit de variabele beveiligingshiërarchie van het gebouw. Ruimte G is het zwaarst beveiligd.

Bij een gebouw, dat bestaat uit ruimten met een gelijke beveiligingsgraad is een systeem met elektronische sleutel zonder meer voldoende. Een PVS dient slechts overwogen te worden in een situatie waarin de ruimten niet een gelijke beveiligingsbehoefte hebben. In zo'n geval is sprake van een beveiligingshiërarchie.

.....

Tijdregistratie

Gezien de tijdsafhankelijkheid van een PVS zou men kunnen denken aan een combinatie hiervan met een tijdregistratiesysteem. Men dient dan wel te bedenken, dat een dergelijke combinatie praktische problemen geeft.

.....

Op basis van studies, die in de afgelopen 6 jaar zijn uitgevoerd, moet worden geconcludeerd dat het minder wenselijk is, een PVS te combineren met een tijdregistratiesysteem. Een gedeeltelijke koppeling is wel mogelijk, door de pasjeslezers te gebruiken om informatie te geven aan het registratiesysteem. De verwerking van binnenkomsttijden en dergelijke wordt dan door dat registratiesysteem verder verwerkt.
Computerfraude blijft steeds de interesse wekken. Business Week wijdde een hoofdartikel hieraan. In de "Journal of Accountancy" van oktober 1981 troffen wij een samenvatting van dit artikel aan.

PREVENTING COMPUTER CRIME: THINKING LIKE AN AUDITOR

Computer-assisted theft may be running 20 times as high as it was 10 years ago, says the cover story in Business Week (April 20, 1981). "If today's computer frauds are overestimated, the quantum leap being made in computer technology is creating a new potential for computer rip-offs that is hard to underestimate," the article says. Three computer industry developments currently enhance the risk of fraud: the spread of lowcost personal computers, the increasing number of students and others who are acquiring computer know-how and the vast number of employees who, using remote terminals, have access to central computers. The article notes that five years ago 1,500 personal computers had been sold. Today the number is over half a million, and projections are that by middecade 3 million will be in use.
Another development that encourages crime is the increasing number of computers which can be used via the telephone. The article cites, as an example, one New York bank which is said to be investigating someone with a personal computer who illegally accessed an expensive computer investment service. This type of theft, of course, threatens all the new on-line data based services being marketed to commercial and private users.

To help prevent computer crime, the article points out, the computer should be programmed to "think" like an auditor. "Security specialists say that programs typically do not have audit controls that will allow the computer to isolate frauds automatically."
And most security reviews reveal that even the traditional controls that were rigorously enforced in manual bookkeeping systems are either eliminated or not enforced once those systems are computerized, the writers say.
The article notes that some software vendors are now writing programs that allow an auditor, even one untrained in data processing, to make inquiries that would uncover fraud. The latest auditor software, for instance, permits an auditor to request information from a terminal in his own office, bypassing corporate data processing where the area he was auditing would be made known.
Most security experts believe that highly competent computer criminals, however, can still gain access to a mainframe's operating system and instruct it to perform any desired operation. But the article offers hope in the news that new systems soon to be marketed offer more sophisticated security measures, such as electronic analysis of a signature.

Een middel om "inbraak" in een computersysteem via een lijnverbinding te voorkomen zou, zo menen wij, het toepassen van versluiering van gegevens kunnen zijn. De Automatisering Gids van 6 januari 1982 meldt ons echter:

Versluiering data niet veel toegepast

Het versluieren van overgedragen gegevens, teneinde afluisteren door onbevoegden van het communicatiekanaal te voorkomen, neemt een minder hoge vlucht dan aanvankelijk werd gedacht. Dat is althans de conclusie van het marktonderzoekbureau International Resource Development. Genoemde conclusie werd getrokken na een uitvoerig onderzoek naar het gebruik van versluieringsapparatuur. Het blijkt, dat slechts een derde van de gebruikers inderdaad deze apparatuur toepast. Algemeen werd verwacht, dat na het vaststellen van een codeerstandaard door het Amerikaanse National Bureau of Standards de verkoop van versluieringsapparatuur sterk zou toenemen. Die standaard wordt aangeduid met de letters DES, een afkorting van Data Encryption Standard. Apparatuur, die volgens deze standaard werkt, wordt onder meer op de markt gebracht door IBM. Daarnaast zijn er enkele leveranciers van geïntegreerde schakelingen, die een speciale DES-chip in hun programma hebben. Het ontwikkelen van dergelijke gespecialiseerde chips wordt door de onderzoekers 'gekkenwerk' genoemd, voornamelijk vanwege het geringe aantal afzetmogelijkheden. Het is zeer onwaarschijnlijk dat de verkoopresultaten zullen opwegen tegen de ontwikkelingskosten. Indien alle versluieringsapparatuur over 10 jaar uitgerust zal zijn met een dergelijke DES-chip, dan zal het totaal aantal chips minder dan 10.000 stuks bedragen. Nauwelijks een rendabel aantal dus.

Twee jaar geleden hield IRD ook een onderzoek naar de mate waarin aan gegevensversluiering werd gedaan. Het bleek toen, dat bij eenderde van de gebruikers een studiegroep was geformeerd, om de wenselijkheid van versluiering vast te stellen. Nu blijkt, dat de gebruikers in de meeste gevallen niet de moeite hebben genomen hun communicatiekanalen door middel van een encryptie-apparaat te beveiligen.
De gebruikers, die hun gegevens wel versluieren bij transmissie, vallen meestal in de volgende categorieën: militair, oliemaatschappijen en regeringsinstanties. Veelal zijn dit gebruikers die 10 jaar geleden ook al gebruik maakten van gecodeerde gegevensoverdracht.
Er is een groeigebied aan te wijzen voor wat de versluiering betreft, en wel de financiële wereld. Hierbij wordt aangetekend, dat in het bankwezen de versluiering niet op de eerste plaats komt.
Vele banken vinden het afluisteren van overgedragen gegevens een minder grote bedreiging dan oplichting, fraude en gewapende overvallen. Zij zijn eerder bereid geld uit te geven om de laatstgenoemde gevallen te voorkomen, dan om afluistering van communicatiekanalen tegen te gaan. Geldautomaten en balieterminals zijn in de meeste gevallen wel van een zekere vorm van versluieringsapparatuur voorzien. Op die manier wil men rekeningnummers en de daarbij behorende toegangscodes geheim houden, zodat onbevoegden daar geen misbruik van kunnen maken.

THE FUTURE OF COMPUTER AUDITING, by Brian G. Jenkins

Brian G. Jenkins heeft zich in een artikel gewaagd aan een beschouwing inzake de toekomstige ontwikkeling van "Computer Auditing". Zijn conclusie luidt als volgt:

CONCLUSION

Over the next few years, external EDP audit will experience significant changes. At present the basic approach is sound, and it has involved considerable success in the use of computer audit software. However, this approach was heavily influenced by audit experience with manual systems and was designed to work with simpler computer systems.
Auditors must change their approach and expand or modify their techniques in order to conduct efficient and effective audits in a more complex computer environment.
The traditional manual influence must fade away. This is not to say that approach was wrong. Rather, it must be logically developed to adapt it to newer and more complex systems. The external audit staff that participates in this development will be a team of professionals from both auditing and data processing.

Uit deze conclusie spreekt een onmiskenbare behoefte aan het opnemen van "data processing know how" in de "external audit staff".
Hoe Jenkins tot voorgaande conclusie komt kunt u lezen in het volgende artikel.

Developments in the way computers process, record, and control accounting data will be significant enough to bring about substantial changes in audit methods. This article reviews these EDP developments and projects possible changes in auditing.

THE PRESENT SCENE

In the current environment, the external auditor is concerned with the computer as but one aspect of his objective of determining whether, in his opinion, the financial statements provide "a true and fair" view of the current financial position and operating results for an organization. If material financial or accounting applications are processed by the computer, the auditor will be concerned with the reliability of the records produced by such processing. Usually, the auditor will evaluate reliability by reviewing the system and placing reliance on day-to-day controls over operations.
The author feels that external auditors in the United Kingdom have fully implemented the audit techniques and documentation suggested 10 years ago in Documents U14 and U15, published by the Institute

of Chartered Accountants in England and Wales (ICAEW). These documents featured a marked influence by manual audit approaches. This manual influence is strongly evident in three areas:

Audit Approach

Manual audit approaches have had a major impact on computer audit. In manual systems, a chain of controls is applied to accounting data while it is being processed. Auditors attempt to satisfy themselves by verifying the operation of these controls. When working with EDP systems, auditors have looked for similar controls. Program controls were tested to form a basis for reaching audit conclusions.
Using this approach, external auditors tend to overlook organizational controls within EDP. These controls just did not fit within the traditional audit approach.

Documentation

Audit documentation for computer applications was a problem for many years. At first, EDP considerations were handled as an appendix to manual system documentation. This led to inefficient overlaps and gaps in documentation.
Gradually, documentation was integrated. Internal control questionnaires now contain alternate sets of questions for computer and non-computer processing. The auditor can select the appropriate mix of questions to evaluate controls in a given organization. However, EDP organizational controls are still given inadequate consideration. While integrated questionnaires are quite efficient, they are actually based on non-computer processing and control concepts.

Staff

Most external audit firms selected suitable people from their staff and provided them with computer training with the intent of establishing an EDP audit staff. While there has been a lot of controversy about this approach, it was probably the right way to go during the early years of computer auditing. But, by failing to involve computer professionals, auditing lost some degree of technical experimentation and development.
Looking back, external auditors seem to have done a reasonable job of handling the computer challenge. File interrogation packages have been employed to utilize the computer as an audit tool. Applications that were developed for audit purposes have in some cases been adopted by management for its own use.

COMPUTER DEVELOPMENTS

Currently, developments at both ends of the computer-size spectrum are making it difficult for auditors to remain efficient while using their traditional approach to computer audit. At one extreme, the use of small computers is proliferating in an uncontrolled environment. On the other end of the scale, realtime processing and the use of sophisticated terminal devices tend to reduce visible evidence

and weaken user controls. Further, at all levels, the use of data base techniques changes the whole approach to processing master files. As a result, many traditional controls no longer apply.
Because of these developments, more and more of the controls within an EDP system are provided by the system software.

Although this software does not directly process any accounting or financial data, its correct functioning is becoming a matter of concern to the external auditor.
Viewed in this light, the traditional external audit approach of seeking controls on transactions begins to appear dated. In today's environment, controls must be provided via the system software, by the operational environment that surrounds a computer system.

DEVELOPING AUDIT TRENDS

New developments in EDP are likely to mean an extension, rather than replacement, of current audit strategies. Possibly, the external auditor's role in the assessment of internal control will increase. Perhaps there will also be improvements in the process of evaluating the effect of control weaknesses.

RECONSIDERATION OF CONTROLS

Auditors must begin to consider different types of controls and their interrelationships. As a first step, they must realize that they cannot rely upon program controls. Such controls are only lines of program code. Such code must also be subject to control to provide for their proper operation. In most systems, such controls are implemented as organizational controls.
Next, auditors will begin to realize that much of their audit satisfaction can be derived from and based upon the organizational controls that govern the quality of the operations, system design, and security environment. However, the auditor does not want to waste time reviewing unimportant controls or procedures. The kinds of organizational controls that are of interest to auditors can be called integrity controls and grouped into three major categories: implementation, program security, and computer operations. Many of these controls may be provided by system software.
Looking at controls in this way makes it easier to measure the effect of an absence of control; for example:

- Weaknesses in integrity controls may be offset by user controls.
- An uncompensated weakness in integrity controls creates a risk for all programmed procedures.
- Weaknesses in implementation controls and program security controls involve a risk for program content. Errors within programmed controls will tend to be permanent.

- Weaknesses in computer operations controls create a risk for the use of computer programs. Such risk may be temporary in nature.

- Program security controls are fraud-oriented. They can be evaluated in terms of the fraud risk that is involved.

An analysis of controls following the kind of approach outlined above leads to some general rules about controls:

1. When an auditor uncovers a breakdown in user controls, he should determine if it is an isolated incident. If it is not, the auditor must perform additional work to establish the extent of the breakdown.
2. If a breakdown in integrity controls is not isolated, the auditor must evaluate its impact on programmed procedures. This can be done by reviewing logs or by testing of programmed procedures.
3. A failure in programmed procedures means the auditor must find the reason for the failure. Usually it will be traced to a weakness in implementation, program security, or computer operations controls. In evaluating the effect of a breakdown in programmed procedures, the auditor should remember it is likely to be rather extensive. An error in a program will keep happening until it is corrected.

NEW AUDIT STRATEGIES

In some cases, the auditor may decide that the most efficient approach is to test user and integrity controls while placing appropriate limits on substantive tests.
He may also decide to test programmed procedures and system software. However, the auditor should look at some new approaches which may replace or supplement the testing of controls:

- Testing programmed procedures in order to establish that they were operating properly during a particular time period.
- Testing computer operations to determine that programmed procedures have been effective throughout the period.

Picking an efficient audit strategy from among the available options requires careful consideration. A number of factors must be evaluated. Some general rules to be employed include:

1. Testing user and integrity controls is most appropriate when those controls are thought to be strong. It is also useful when the auditor is not skilled in EDP techniques because computer-assisted auditing applications are not required.
2. Testing user controls and programmed procedures is most appropriate when the programmed procedures are important, but few in number. This approach is also useful where testing the programmed procedures is easy and efficient.

3. Testing user controls and computer activity is most appropriate when there are a lot of programmed procedures or there are weaknesses in integrity controls. This approach requires an auditor who is technically skilled in data processing.

NEW TESTING TECHNIQUES

Over the next few years, existing EDP testing techniques will become a part of the standard audit approach. New strategies and techniques may also be required.
For example:

- Programs can be used to compare a production library with a control copy of that library to identify unauthorized or incorrect changes.
- Programs can be used to scan log files and report on items that are of interest to the auditors.

These kinds of techniques serve to validate data processing activity.

IMPACT OF MINIS

Minicomputers may create a more difficult audit environment than did conventional computer systems. To counter this problem, progress must be made in two areas:

- The question of controls must be carefully reviewed. Auditors should not assume that controls in the minicomputer environment cannot be relied upon. What is really needed is a control model that would be appropriate for minicomputer installations. The model would reflect an effective control environment for minis and could serve as a standard for evaluating client systems.
- File interrogation packages, a standard audit tool, will not run on most minicomputers. This problem will require a lot of development effort. It may be possible to alter some of the audit packages so they can be used to compile programs in RPGII or BASIC, but this may well prove to be inefficient. It may prove more effective to reformat files from minicomputer systems so they can be read by existing audit software. Another approach would be to have the auditor write interrogation programs in the native language of the minicomputer being audited.

TECHNICAL STAFF

As a wider range of EDP audit strategies is developed, there will be a need for a larger technical staff to support computer audit. External audit firms will recruit more computer professionals.

Privacy en Service Bureaus zijn twee gebieden die de laatste tijd de belangstelling van de accountant hebben. Echter als aparte interessegebieden. Joel T. Sothern heeft in het artikel "Information Privacy and Service Bureaus" de relatie tussen de twee gebieden gelegd. In het artikel - dat gedeeltelijk is weergegeven - gaat hij speciaal in op de privacy-aspecten die in het contract, dat met het service bureau wordt gesloten, dienen te worden geregeld.

INFORMATION PRIVACY AND SERVICE BUREAUS

by Joel T. Sothern
Security Pacific National Bank
EDP Auditor

Service bureaus, which have become very widely used, present special problems in the area of information privacy. The user of a service bureau has the responsibility to ensure, as completely as possible, the privacy of data processed by the service bureau. The user should make certain that inhouse controls are coordinated with those provided by the service bureau. A user should also be wary of standard form contracts offered by service bureaus if the contracts do not include proper data privacy provisions. A service bureau contract should include provisions explicitly covering at least 11 aspects of privacy and security.
Violations of privacy which may take place include four types of intrusions: 1) Intrusion upon a person's seclusion or solitude, or into his private affairs; 2) Public disclosure of embarrassing private facts about a person; 3) Publicity which places a person in a false light in the public eye; and 4) Appropriation, for someone else's advantage, of a person's name or likeness. Information privacy, especially in the context of service bureau processing, is most likely to involve the public disclosure of embarrassing private facts or libelous publicity. Information security, however, is very closely related, since a breach in security may lead to an invasion of privacy, the improper exploitation of a trade secret, or damage to a businessman's reputation or competitive position in his industry. There are two major ways in which a user can help protect against theft, misuse, misappropriation or disclosure of information: 1) Review the controls that remain in-house and attempt to integrate them with the service bureau's operating procedures, and 2) Negotiate a proper service bureau contract containing provisions protecting the user against misappropriation, misuse, disclosure, and loss of valuable data.

Coordinating in-house controls with those provided by the service bureau is important in avoiding any weakness in the chain of controls between the user's and service bureau's systems. A few areas which may require careful coordination of controls are:

1. The transmission of source documents and computer printouts between users and the service bureau.
2. The delineation of duties and responsibilities between a user's control group and the service bureau's control group.

3. The identification and authorization procedures for users to access and process data at the service bureau.

4. The procedures and responsibilities of both users and the service bureau for back-up and reconstruction of data and programs.

5. The identification of users' sensitive information and the establishment of the desired level of protection and security.

In negotiating a contract it is important to remember the two major functions of a contract: 1) To define legal rights and obligations, and 2) To serve as a means of communication to provide guidance to persons involved with contract performance. Good contracts are designed and planned to avoid problems and to give each party a fair bargain.
Most service bureaus have standard form contracts which are used unless the user insists upon additional provisions. Standard data processing contracts which may be offered to the user normally contain a simple definition of the services to be performed, without any mentioned concern for information privacy or the service bureau's responsibilities regarding such privacy. Most standard contracts do not even contain protections against the most obvious and common forms of privacy violation, such as preparing a mailing list from the names in a payroll file and selling this list to others. A few excerpts from standard form contracts should help to emphasize the seriousness of the problems with these contracts. For instance, take the following contract portion:

"Service Bureau assumes no responsibility for loss, destruction, alteration, or disclosure to any person of any physical media on which such program, data, or other information are stored, unless caused by willful default on the part of the Service Bureau."

This provision excuses the service bureau from almost any form of responsibility except in the unlikely, if not impossible, case in which the user can prove willful default.

Regarding the privacy of data processed by a service bureau, then, a number of areas should be specifically addressed in a contract. While the precise areas depend on the circumstances, there are 11 areas which should be included in all service bureau contracts.

1. File Access - All files, including files maintained by the system and intermediate or work files, should be accessible to and, if desired, removable by the user at any time, provided removal does not interfere with the service bureau's turnaround commitments.

2. File Ownership - Title to all files, including work files, should be explicitly given to the user.

3. File Confidentiality - The contract should state that the service bureau will protect the confidentiality of user files and use them only for the purpose for which they were supplied by the user. The agreement should also prohibit the service bureau from releasing the files to anyone without the permission of the user.

4. Destruction of Intermediate Files - The service bureau should be required to erase all confidential work files prior to their return to the data file library after the work has been completed.

5. Destruction of Print Media - If carbon paper is used in printing confidential, multiple-copy reports, the contract should state that the used carbon paper should be destroyed or delivered to the user for proper disposal.

6. Systems Controls - Controls to be included in a service bureau-designed system should be explicitly described in the contract so that the user can use these controls in determining compliance to and adequacy of controls in the systems.

7. Evidence of Proper Insurance - It is important for the service bureau to provide insurance against disaster, unauthorized entry, or destruction of valuable papers. The contract should require that such insurance be carried throughout the life of the contract.

8. Data Storage Facilities - The contract should contain a description of the data storage facilities used to retain user data in order to ensure proper back-up and retention of critical and/or sensitive files.

9. Privacy Violation Notification - The contract should include a requirement that all users be immediately notified in the event that the service bureau discovers an attempt to violate the information privacy of any user.

10. Identification of Third-Party Processors or Subcontractors - If actual processing of the user's data may not be performed by the service bureau named in the contract, the contract should include the names and locations of alternate processing centers.

11. Right to Audit - One very important aspect of ensuring the security and privacy of data processed by a service bureau is the ability to audit the service bureau. While this is a subject unto itself and is beyond the scope of this paper, suffice it to say that the contract should explicitly include provisions for an independent audit of the service bureau, either by the user or a third party chosen by the user. As mentioned at the beginning of this paper, responsibility for outside integrity cannot be delegated by management; however, neither can review of all significant operations of the organization, including those delegated to outside parties, be delegated by audit. Regardless of other contract provision, actually auditing the service bureau is the only way to ensure that the service bureau is adequately protecting the user's resources.

In conclusion, service bureaus, although widely used, should not be taken for granted, and data should not be blindly entrusted to them. A user has the responsibility to ensure as completely as possible the privacy of the data processed by the service bureau. The user should make certain that in-house controls are coordinated with those provided by the service bureau. Finally, the user should not accept a service bureau contract which does not include proper data privacy provisions. At least 11 aspects of privacy and security should be explicitly covered in the contract.

KMG
Klynveld Main Goerdeler
Accountants-international

Momenteel heeft KMG de beschikking over de volgende audit-software.

1. AVAILABLE RELEASES CULPRIT/EDP-AUDITOR

REL. 4.3.B
REL. 5.0.B
REL. 6.0.

2. AVAILABLE CARS RELEASE 4.0 SYSTEMS

COMPUTER HARDWARE	OPERATING SYSTEM	LATEST RELEASE	DATABASE INTERFACES	COBOL COMPILER
BURROUGHS-LARGE	STANDARD MCP	4.0B BETA		ANSI'68
BURROUGHS-MED. SYS.	STANDARD MCPXRAM	4.0B	RUFF-FINE	ANSI'68
BURROUGHS-MED. SYS.	STANDARD MCP	4.0A	THRIFT W/MIF	ANSI'68
BURROUGHS-SMALL SYS.	STANDARD MCP	4.0B BETA		ANSI'74
DEC/VAX	VAX	4.0B		ANSI'74
DATA GENERAL ECLIPSE	AOS	4.0A	INPOS	ANSI'74
FACOM	OSIV/F4	4.0A BETA		ANSI'68
HEWLETT PACKARD 3000	MPE	4.0B BETA		ANSI'68
HONEYWELL-BULL LEVEL 64	GCOS	4.0A		ANSI'74
HONEYWELL-2000	GCOS	4.0		ANSI'68
HONEYWELL-6000	GCOS	4.0B		ANSI'74

KMG
Klynveld Main Goerdeler
Accountants-international

2. AVAILABLE CARS RELEASE 4.0 SYSTEMS

COMPUTER HARDWARE	OPERATING SYSTEM	LATEST RELEASE	DATABASE INTERFACES	COBOL COMPILER
IBM SYSTEM/34	SSP	4.0A BETA		ANSI'74
IBM 360/370	OS/VS	4.0B		ANSI'68
IBM 360/370	OS/IMS	4.0B	IMS	ANSI'68
IBM 360/370	DOS/VS	4.0B		ANSI'68
NCR CENTURY/ CRITERION	B.C SERIES VRX	4.0B	CIF	STAGE 2 STAGE 3
PRIME	PRIMOS	4.0B		ANSI'74
UNIVAC 1100	EXEC 8-12	4.0B BETA	DMS-LEVEL-6 DMS-LEVEL-8 TIP	ANSI'74
UNIVAC 90	OS3	4.0B BETA		ANSI'74
WANG 2200	VS	4.0B		LEVEL 1 ANSI

Note:
1. Unless otherwise noted, all release tapes are the final version of CARS release 4.0.

2. 4.0A tapes contain PTF's CA40*001 through CA40*027

3. 4.0B tapes contain PTF's CA40*001 through CA40*058

Voor verdere inlichtingen over CULPRIT/EDP-AUDITOR alsmede CARS kunt u contact opnemen met J.E. Huizenga.

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

EXTERNE CURSUSSEN; ONDERWIJS

Controle bij geïntegreerde gegevensverwerking.

Achtergrond van de cursus

In de administratieve organisatie en de accountantscontrole worden gebruikers en accountants steeds meer geconfronteerd met on-line gegevensverwerking met gebruikmaking van geïntegreerde gegevensverzamelingen. De interne controlevoorzieningen worden daarbij steeds meer afhankelijk van de mogelijkheden van de software op het gebied van data communicatie en data base management. Deze volkomen nieuwe materie dient doorzichtig te worden gemaakt voor niet software-technisch onderlegde gebruikers en accountants. Deze dienen zich de gevaren en de mogelijkheden te realiseren. Op dit gebied is nog nauwelijks opleidingsmateriaal ontwikkeld.

Door de AC-groep van Klynveld Kraayenhof & Co. is een cursus ontwikkeld waarin deze problematiek is verwerkt. Hiervoor is een - thans operationele - data base gebouwd waarbij tevens gebruik wordt gemaakt van een Data Dictionary Directory System (DD/DS) en een Tele Processing monitor (TP-monitor).

Thema en doel

Het accent van de cursus ligt op het wegen van de invloeden van geïntegreerde gegevensverwerking op de interne controle en daarmede op de accountantscontrole.

Met nadruk dient te worden vermeld dat de cursus zich niet beperkt tot alleen een data base omgeving. Aan de controle-aspecten in situaties met geïntegreerde gegevensverwerking doch zonder een data base management systeem en/of Data Dictionary Directory System wordt ruim aandacht besteed.

Bestemd voor

De cursus is bestemd voor hen die werkzaam zijn in de in- of externe accountantscontrole, als ook voor systeemontwerpers en -analisten, die betrokken zijn bij alsmede medeverantwoordelijkheid dragen voor de kwaliteit van de interne controle en de beheersbaarheid van mede door hen ontwikkelde geavanceerde gegevensverwerkende systemen. Als ingangskennis is enige bekendheid met COBOL vereist waartoe wij verwijzen naar onze 1-daagse cursus inleiding COBOL.

Wijze van kennisoverdracht

Kennis wordt overgedragen door middel van inleidingen en het uitwerken van opdrachten. Rondom een casus "Widget Nederland", welke een niet bestaand produkt fabriceert en verkoopt, is een aantal modules gebouwd.

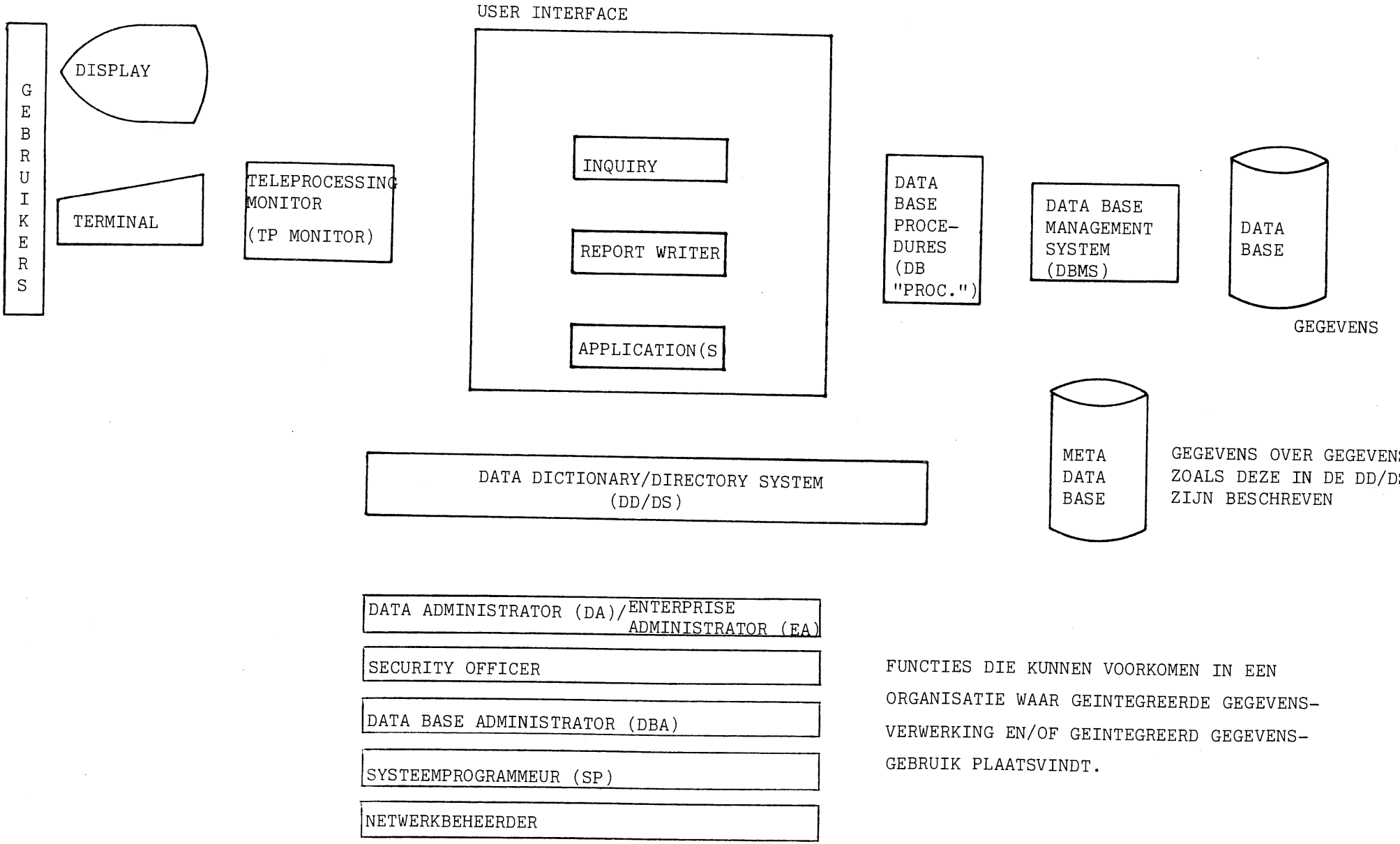
Inhoud

1. Inleiding (data sharing, computer sharing, program sharing).
2. Introductie van de casus "Widget Nederland".
3. Principes van data base en data dictionary/ directory system (DD/DS).
4. IDMS/DB en de geïntegreerde data dictionary/ directory IDD.
5. Interactieve transactieverwerking en data communicatie monitor-functies, waaronder de monitor IDMS/DC.
6. Bepaling data sharing en de consequenties daarvan voor de interne controle.
7. Geïntegreerde "ideaalsituatie" en de controleproblemen, welke zich kunnen voordoen bij afwijking van die ideaalsituatie.

Cursusstructuur

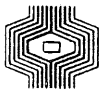
De cursus heeft enigszins het karakter van een workshop en bestaat uit een zevental modules. Elke module bestaat uit één of meerdere inleidingen welke al dan niet gevolgd worden door een opdracht. Deze opdrachten worden in groepen uitgewerkt waarna behandeling en evaluatie in pleno plaatsvindt. Bij de uitwerking van de opdrachten wordt tevens direct of indirect (reële output) gebruik gemaakt van het operationele data base systeem dat geïmplementeerd is op de KKC-computer te Amsterdam. De cursus locatie is daarvoor online met de KKC-computer te Amsterdam verbonden. De opdrachten in de modules hebben hoofdzakelijk ten doel te toetsen of men de stof uit de inleidingen en kernbegrippen heeft begrepen.

Bij de start van de laatste module wordt - nadat alle daarvoor benodigde kernbegrippen in de vorige modules zijn behandeld - een uit interne controle-oogpunt gewenste ideale situatie gegeven bij geïntegreerde gegevensverwerking (zie bijgaande tekening).



FUNCTIES DIE KUNNEN VOORKOMEN IN EEN ORGANISATIE WAAR GEINTEGREERDE GEGEVENS-VERWERKING EN/OF GEINTEGREERD GEGEVENS-GEBRUIK PLAATSVINDT.

Aangezien dié situatie meestal niet in overeenstemming is met de praktijk wordt ingegaan op vele mogelijke afwijkingen van de ideaalsituatie en wat de invloed daarvan kan zijn op de interne controle en daarmee op de accountantscontrole. Tevens wordt ingegaan op de wijze hoe dergelijke situaties in de praktijk dienen te worden benaderd.

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