compact

COMPUTER EN ACCOUNTANT

UIT DE INHOUD

- KANTOORAUTOMATISERING II
- GARBAGE IN, GARBAGE OUT
- TESTEN ALS CONTROLETECHNIEK
- CONTROLE VAN HET "BESTURINGSSYSTEEM"

Klynveld Kraayenhof & Co.
ACCOUNTANTS

Internationaal KMG Klynveld Main Goerdeler

NUMMER 28 9E JAARGANG ZOMER 1982

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

INHOUDSOPGAVE

NUMMER 28 9E JAARGANG ZOMER 1982

compact

Zomer 1982

VAN DE REDACTIE

In de hoofdstukken 3 en 4 van Kantoorautomatisering behandelen de schrijvers de aspecten van integratie en de gevolgen daarvan voor interne controle en continuïteit van de gegevensverwerking.
H. Veenman bespreekt de controle- en correctiemethoden van computerinvoer onder de titel Garbage in, garbage out.
Dat testen als controletechniek geen eenvoudige zaak is ingeval van automatisering kunt u lezen in het artikel van de hand van A.H.C. Koedijk.
H. Roos wijst in "Controle van het besturingssysteem" op mogelijke nieuwe wegen leidend tot een verantwoorde controleaanpak.
Een kijkje in de keuken verschaft ons A.W. Neisingh door het verslag van de 23e Guide.

Onder de rubrieken "Boeken", "Tijdschriften", "ABC-Nieuws" en "Onderwijs" kunt u het gebruikelijke verslag van de nieuwste ontwikkelingen lezen.

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.

Indien u belangstelling heeft voor meerdere exemplaren kunt u deze aanvragen bij de redactie-secretaris, evenwel zolang de voorraad strekt.

IN MEMORIAM

Op vrijdag 31 juli 1982 overleed onze collega Johan Philippo.

De redactie van Compact heeft er behoefte aan om in dit eerste nummer na zijn overlijden, zijn heengaan uit onze kring te herdenken.

Toen bij het zelfstandig worden van de AC-groep in 1974 het idee werd geboren om een soort huisorgaan het licht te doen zien was Johan mede vanuit zijn functie als beheerder van de AC-bibliotheek van stonde af aan enthousiast voor de verwezenlijking ervan. Vanaf het eerste nummer van Compact heeft hij vooral als de motor gefungeerd die er voor zorgde dat de afleveringen met een bijna niet aflatende regelmaat van één per kwartaal werden geproduceerd.

Na een langdurige ziekteperiode in het jaar 1979 moest hij zich noodgedwongen beperken in zijn werkzaamheden.
De overdracht van zijn taak aan Henk van der Wielen kostte hem destijds zeer veel moeite.
Johan Philippo was niet iemand die in "the foreground" opereerde maar in "the background" was hij altijd bereikbaar en bereid om zijn steentje bij te dragen.
Het gat dat hij achterlaat moge worden gevuld, het litteken blijft bestaan zeker in onze gedachten.

Namens de Redactie
Dick Steeman

compact

Zomer 1982

KANTOORAUTOMATISERING II

door: J. Balvert, A.v.d. Drift, drs. B.M. de Vries

Inleiding

De ontwikkelingen op het gebied van de elektronica hebben geleid tot het aanbod van een breed scala van hulpmiddelen, die bij uitstek inzetbaar zijn voor het verrichten van kantoorwerkzaamheden. De inzet van deze hulpmiddelen op een al dan niet planmatige wijze heeft het fenomeen kantoorautomatisering opgeleverd.
Kenmerkend voor kantoorautomatisering is de grote verscheidenheid van de hulpmiddelen of anders gezegd, van de ingrediënten van kantoorautomatisering.
In het eerste artikel van Kantoorautomatisering (hoofdstukken 1 en 2), gepubliceerd in Compact nummer 25, is een resumé gegeven van deze ingrediënten. In dit vervolgartikel zal ingegaan worden op de integratie, bereikt door de toepassing van meerdere ingrediënten in combinatie met elkaar, en op de met kantoorautomatisering samenhangende problemen betreffende interne controle en beveiliging.

3. Integratie binnen kantoorautomatisering

Integratie binnen kantoorautomatisering betekent het samenvoegen van zelfstandige functies in één ingrediënt of het koppelen van twee of meer ingrediënten.
Het samenvoegen van functies of wel functie-integratie wordt aangetroffen bij onder meer het fotocopieerstation, beschreven in het eerste artikel hoofdstuk 2.9. De functie "tekst-editing" wordt door deze integratievorm aangetroffen bij tekstverwerkende machines alsook bij sommige mini- en microcomputers en time-sharing.
In de volgende paragraaf worden de mogelijkheden van koppelingen besproken en wordt tevens een drietal voorbeelden van integratie toegelicht.

3.1 Koppelingen

Voor het tot stand brengen van koppelingen kan gebruik worden gemaakt van locale verbindingen, zoals bijvoorbeeld coax-kabels, light-links (infra-rood zie hoofdstuk 2.7) en glasvezels (zie hoofdstuk 2.6), maar ook van interlocale verbindingsnetten van de PTT, zoals het telex-, telefoon- en datanet.
Telex- en telefoonnetten worden onderscheiden in kieslijnen (dial-up-line) en vaste verbindingen.
Bij kieslijnen maken de stations (bijvoorbeeld een computer of een terminal) gebruik van het openbaar telex- of telefoonnet. De hieraan verbonden kosten worden door de PTT op basis van de normaal gangbare tarieven in rekening gebracht. Bij een geringe mate van gebruik verdient deze verbinding derhalve uit kostenoverweging voorkeur.
Een voordeel van deze verbinding is dat vanuit elke locatie, die beschikt over een aansluitmogelijkheid (telex of telefoon), gekozen kan worden voor een station, waarmee verbinding tot stand moet komen.

Nadelig is echter de hoge mate van storingsgevoeligheid en de lage transmissiesnelheid (de snelheid van gegevensoverdracht over het telexnet is niet meer dan 50 bits per seconde, het openbaar telefoonnet met een geringe kans op transmissiefouten gaat tot 2400 b.p.s.). Voor vaste verbindingen verzorgt de PTT een directe kabelaansluiting tussen twee stations. Deze verbinding, die van de PTT op maandbasis kan worden gehuurd, is minder storingsgevoelig en staat hogere transmissiesnelheden toe (vaste telexlijnen tot 200 b.p.s., vaste telefoonhuurlijnen tot 9600 b.p.s.). Een vaste verbinding is echter star, waardoor ingeval van storing, bijvoorbeeld ten gevolge van een kabelbreuk, speciale uitwijkmaatregelen wenselijk zijn. Dit kan resulteren in het huren van een extra vaste verbinding (backup-line).

Figuur 1 geeft een globale schets van totale integratie.

3.2 Voorbeelden van integratie

Een opsomming van alle integratievormen zal evenals de beschrijvingen van ingrediënten zelf niet of nauwelijks volledig zijn gezien de toename van technische ontwikkelingen op dit gebied.
Derhalve worden slechts drie ons inziens belangrijke vormen van integratie uiteen gezet, te weten:

1. Telexverkeer en tekstverwerking gekoppeld aan en bestuurd door een computer.
2. Time-sharing geïntegreerd binnen de geautomatiseerde gegevensverwerking.
3. Toepassing van microcomputers.

Ad 1.

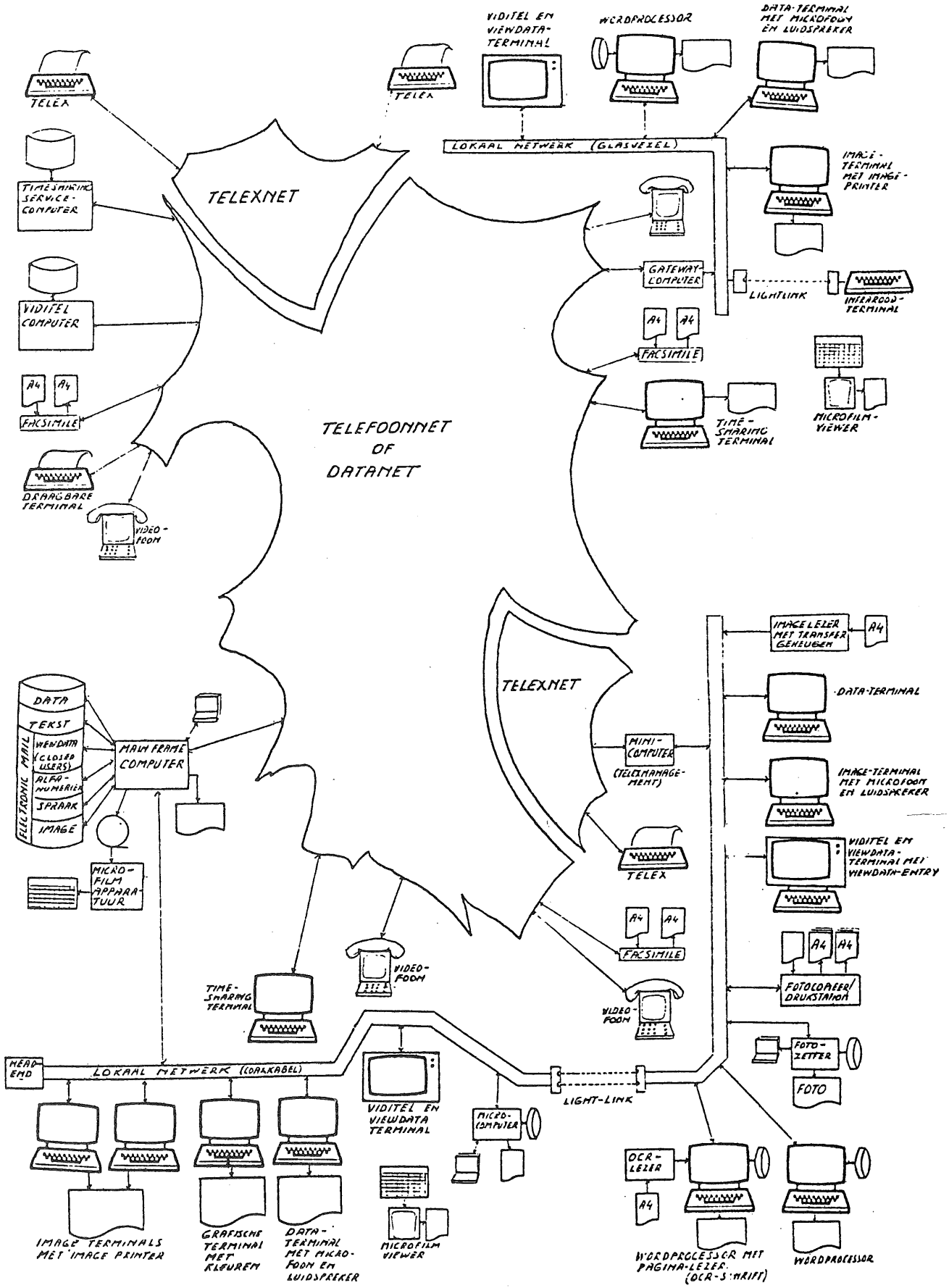
Tekstverwerkende apparatuur kan als terminal gekoppeld worden aan een computer, waardoor toegang kan worden verkregen tot computerbestanden. Een vereiste is, dat hiervoor programmatuur aanwezig is in de computer.

De tekstverwerkende apparatuur biedt een goede mogelijkheid voor de opmaak van boodschappen. Indien deze mogelijkheid in onvoldoende mate aanwezig is in de computer ten dienste van elektronic mail (zie hoofdstukken 2.3 en 2.4), kan een koppeling van deze computer met de tekstverwerkende apparatuur uitkomst bieden.

Een soortgelijke combinatie van voornoemde integraties wordt aangetroffen in een koppeling met het telexverkeer. Een special-purpose minicomputer is voor dit doel direct aangesloten op het telexnetwerk. Voor het telexnetwerk lijkt de minicomputer een normaal telexapparaat. Echter door de programmeerbaarheid van deze minicomputer worden mogelijkheden geboden, waardoor efficiënt en deels automatisch tekstontvangst, -verwerking, -opbouw en -verzending plaatsvinden. De opbouw van het telexbericht geschiedt met behulp van een gebruikersvriendelijke terminal, waardoor een groot deel van de tekst gedurende de opbouw zichtbaar en corrigeerbaar blijft. Het telexbericht komt voor verzending op een diskbestand te staan, waarbij nog steeds de mogelijkheid bestaat het bericht te wijzigen.

INTEGRATIE VAN DE KANTOORAUTOMATISERING

Zomer 1982



In het bericht wordt opgenomen naar wie en wanneer (datum en tijd) het bericht verzonden moet worden.
De minicomputer zal automatisch het bericht op het opgegeven tijdstip verzenden. De ontvangen berichten worden door de minicomputer automatisch op een ander diskbestand geplaatst.
Dit diskbestand kan via de terminal worden geraadpleegd en een of meerdere keren worden afgedrukt, waardoor gemakkelijk de beschikking wordt gekregen over kopieën van het telexbericht. Meerdere terminals kunnen worden aangesloten op deze minicomputer, waardoor het voor de organisatie lijkt alsof men de beschikking heeft over meerdere telexapparaten.
Een eenvoudig op het netwerk aangesloten telexapparaat kan zodoende als een soort terminal communiceren met deze special-purpose minicomputer.

Een verdere koppeling kan tot stand gebracht worden tussen deze minicomputer en de centrale computer ten behoeve van de gegevensverwerking.
Een telexapparaat, aangesloten op het openbaar telexnet, kan gegevens verzenden naar de minicomputer, die met behulp van een daarvoor ontwikkeld programma automatisch de gegevens doorzendt naar de centrale computer. De in de centrale computer aanwezige programmatuur zou de gegevens kunnen gebruiken voor het muteren en/of raadplegen van bestanden. Vervolgens is het ook mogelijk, dat programma's op de centrale computer gegevens uit bestanden doorgeven aan de special-purpose minicomputer, die op zijn beurt de gegevens over het telexnet verzendt naar het ontvangende telexapparaat. Dit gehele proces zou kunnen plaatsvinden zonder menselijke interventie. De benodigde telexadresgegevens van de ontvanger kunnen zijn vastgelegd in de programmatuur of bestanden op de centrale computer of special-purpose minicomputer.

Ad 2.
Time-sharing betekent in wezen niets meer dan dat beschikbare computertijd verdeeld wordt tussen gebruikers, die op een gegeven moment in verbinding staan met de computer. Aan elke gebruiker wordt vooraf een bepaalde hoeveelheid diskruimte toegekend. De gebruiker beschikt voor verwerking doorgaans over eigen programma's, die op zijn commando online kunnen worden uitgevoerd. Bovendien beschikt de gebruiker over eigen bestanden op de daarvoor toegekende diskruimte.
Doordat onder time-sharing meerdere gebruikers simultaan werkzaam zijn, is een afscherming van bestanden en programma's per gebruiker aangebracht door de time-sharing systeemsoftware.
Dit betekent dat een gebruiker uitsluitend kan beschikken over zijn eigen bestanden en programma's en niet over bestanden en programma's van andere time-sharing-gebruikers. Het is evenwel mogelijk dat een bepaalde gebruiker een andere gebruiker expliciet in staat stelt gebruik te maken van zijn bestanden en programma's, door deze te kopiëren en te verzenden (binnen de computer) naar de diskruimte van de andere gebruiker of de andere gebruiker te machtigen door bijvoorbeeld het aan hem bekend maken van een password waarmee tot de bestanden en programma's toegang verkregen kan worden.

Naast time-sharing-activiteiten worden binnen de computer ook operationele (of test) batch- en online-programma's met bijbehorende bestanden aangetroffen. Ook hierbij is een afscherming aangebracht tussen time-sharing-, batch- en online-activiteiten.
Deze afscherming, verwezenlijkt door de time-sharing systeemsoftware en/of het Operating System, kan doorbroken worden, waardoor time-sharing- gebruikers direct toegang verkrijgen tot operationele bestanden.
Deze toegangsmogelijkheid kan worden gezien als een vorm van integratie tussen het op zich zelf geïsoleerde time-sharing-gebruik en de operationele verwerking binnen de centrale computer. De integratievorm kan onder meer tot stand worden gebracht door aan de time-sharing systeemsoftware op te geven welke gebruikers toegang mogen hebben tot welke operationele bestanden. Binnen time-sharing is het mogelijk om op eenvoudige wijze bestanden, dus ook door deze integratievorm operationele bestanden, te raadplegen en/of te wijzigen. Zo ook kunnen delen van de onder time-sharing bereikbaar geworden operationele bestanden worden gekopieerd en doorgezonden naar andere (wellicht niet geautoriseerde) time-sharing-gebruikers.
Door deze vorm van integratie kunnen risico's ontstaan inzake het uitlekken van vertrouwelijke informatie en het ongeautoriseerd of zonder een adequate audit-trail wijzigen van informatie. Administratief organisatorische procedures dienen bij deze integratievorm dit risico te beperken.

Time-sharing-gebruikers kunnen de mogelijkheid krijgen zelf telexboodschappen te verzenden en/of te ontvangen zonder interventie van derden. Deze mogelijkheid kan tot stand worden gebracht door de integratie van bovengenoemde met de special-purpose minicomputer ten behoeve van het telexverkeer. Hierdoor is het mogelijk telexberichten ongeautoriseerd te doen uitgaan. Ten einde de verzending van berichten via time-sharing en via telex te beheersen zijn aanvullende interne controlemaatregelen nodig (zie paragraaf 3).

Ad 3.
De microcomputer of microprocessor biedt door zijn programmeerbaarheid en omvang (geschikt voor inbouw en transport) een bijna onbegrensd aantal mogelijkheden voor integratie met andere ingrediënten. Een ervan wordt hier benadrukt; het gebruik van de microcomputer als terminal gekoppeld aan de centrale computer ten behoeve van de gegevensverwerking. Door deze integratievorm wordt de terminalfunctie (het invoeren en het representeren van uitvoer) programmeerbaar en programmatisch beïnvloedbaar met een relatief hoge snelheid.
Programmeerbaar, omdat menselijke handelingen zoals bijvoorbeeld het intoetsen van vaste gegevens maar ook van gebruikersidentificatie en password uitgevoerd kunnen worden door een programma, gestart op deze microcomputer.
Programmatisch beïnvloedbaar, omdat hetgeen ingetoetst wordt door het programma in de microcomputer veranderd kan worden voordat dit wordt doorgegeven aan de centrale computer, waarvoor de microcomputer dienst doet als terminal.

Ook boodschappen, die teruggestuurd worden naar deze microcomputer, kunnen door een programma op de microcomputer anders weergegeven worden. Door de hoge snelheid behoeft door de gebruiker van het veranderen van data niets of nauwelijks iets bemerkt te worden. Zo ook biedt deze toepassing de mogelijkheid volledige dialogen tussen de microcomputer en de centrale computer (bijna ongemerkt) te loggen. Vanuit het oogpunt van interne controle vereist deze vorm van integratie een bijzonder adequaat stelsel van technische en organisatorische maatregelen ten aanzien van programmabeheer voor deze microcomputer.

4. Interne controle en beveiliging van kantoorautomatisering

De interne controle- en beveiliginsaspecten van kantoorautomatisering hangen enerzijds nauw samen met de wijziging in de organisatie van het kantoor, anderzijds met de technische aspecten van kantoorautomatisering.
Bij kantoorautomatisering gaat het in belangrijke mate om de HANDELINGEN, die door mensen - op een kantoor werkzaam - worden verricht, geheel of gedeeltelijk te automatiseren. Deze HANDELINGEN bestaan uit o.a. creëren, produceren, reproduceren, opslaan, raadplegen, distribueren, presenteren en bewerken van informatie. Het automatiseren van deze handelingen en de daarbij ontstane integratie leiden steeds meer tot één totaal systeem van informatieverwerking. De gevolgen hiervan voor de interne controle en continuïteit van de informatieverwerking zijn niet gering en verdienen daarom de aandacht van de ondernemingsleiding en van de controlerende accountant.

4.1 Functiescheidingen

De koppeling van ingrediënten of het samenvoegen van zelfstandige functies (functie-integratie) kan doorbreking van de binnen de kantoororganisatie bestaande functiescheidingen betekenen. Functiescheidingen zijn uit hoofde van interne controle van betekenis, voor zover zij een belangentegenstelling bevatten, omdat in zo'n situatie controle op de taakuitoefening van elkaars functie het grootst is. Koppeling tussen de ingrediënten en de centrale computer met bijbehorende operationele bestanden is in dit verband een voor de interne controle vergaande vorm van integratie.
Een groot deel van de kantoorwerkzaamheden bestaat uit de verzorging van correspondentie, waaronder bijvoorbeeld het binnenkomen van telexberichten, facsimile vastleggingen, berichten via electronic mail. Het geautomatiseerd in gang zetten van verwerkingsgangen, waarbij voorbijgegaan wordt aan bestaande functiescheidingen, onderstreept de noodzaak van het treffen van aanvullende interne controlemaatregelen. Uitgangspunt zal moeten zijn, dat taakuitoefening slechts kan geschieden binnen de bestaande bevoegdheidsstructuur. Degene, die binnen deze (bevoegdheids)structuur bevoegd is tot het invoeren van bepaalde transacties, zal ook binnen een vergaande vorm van integratie op kantoorautomatiseringsgebied als enige deze bevoegdheid moeten hebben. Andere gebruikers, die technisch wel de mogelijkheid zouden moeten hebben tot invoeren van deze transacties zullen door maatregelen uitgesloten dienen te worden. Tot deze maatregelen kan worden gerekend het gebruikmaken van een geautomatiseerd autorisatiesysteem, dat iedere gebruiker dwingt tot het intoetsen van een identificatienummer en/of een password, waardoor afstemming met een bevoegdheidstabel uitsluitsel geeft of de gebruiker de gewenste transactie kan uitvoeren. Ook het tot stand brengen van fysieke koppelingen (bijvoorbeeld de koppeling van een terminal ten behoeve van electronic mailing) kan via een geautomatiseerd autorisatiesysteem geregeld worden.

In hoofdstuk 3 wordt als voorbeeld van integratie genoemd de koppeling van een special purpose minicomputer, die aangesloten is op het openbaar telexnet en op de centrale computer met bijbehorende applicatieprogrammatuur en operationele bestanden. In dit concept zou het zonder aanvullende maatregelen mogelijk zijn, dat programma's op de centrale computer gegevens uit operationele bestanden doorgeven aan de minicomputers, die de gegevens over het telexnet verzendt. Om in deze situatie het gebruik van gegevens uit operationele bestanden nog enigszins te kunnen beheren, zal in programmatuur toegangsbeperkende maatregelen moeten worden opgenomen, waardoor alleen daarvoor in aanmerking komende gegevens via het telexnet worden verzonden. Het gebruik van gegevens uit operationele bestanden zal vastgelegd moeten worden, zodat toezicht op het functioneren van het toegangsbeveiligingssysteem mogelijk is.

4.2 Interne controlemaatregelen voor juiste en volledige berichtenverzending

Binnen een geautomatiseerd kantoor, waarbij gebruik wordt gemaakt van op communicatie gerichte ingrediënten (bijvoorbeeld terminals voor electronic mailing, voor overbrengen van spraak, telexbeheersysteem) zal gezorgd moeten worden, dat maatregelen getroffen zijn die een juiste, volledige en tijdige geautoriseerde berichtenverzending waarborgen. Gedacht dient te worden onder meer aan verificatie van de verzending, terugmelding (bevestiging) van berichten, opname van controle-bits bij verzending van berichten, coderen van berichten (encryption), opnemen van controles in applicatieprogrammatuur of in de dedicated functie van microcomputer, logging van berichten ten behoeve van reconstructie.
Zoals in vorig hoofdstuk vermeld zijn de mogelijkheden van koppeling met microcomputers bijna onbegrensd. Menselijke handelingen, zoals bijvoorbeeld het intoetsen van vaste gegevens, gebruikersidentificatie en password kunnen worden uitgevoerd door een programma, gestart op een microcomputer.
In het algemeen is vanuit het gezichtpunt van interne controle het beheer van computerprogrammatuur belangrijk.
Voor wat betreft de programmatuur op de microcomputer zal het programmabeheer zich vooral moeten richten op de procedure inzake het muteren van programma's.
Het muteren van programma's op een microcomputer dient technisch alleen mogelijk te zijn voor bevoegden. Wijzigingen in programmatuur dienen een duidelijk spoor achter te laten door bijvoorbeeld wijziging van een programmaversienummer, afgedrukt op de mutatielijst. Wijziging in programmatuur behoort in principe alleen in opdracht van de gebruikers te worden uitgevoerd.

4.3 Continuïteitsaspecten

De continuïteit van kantoorwerkzaamheden vereist, dat maatregelen zijn getroffen om stagnatie (al dan niet tijdelijk) in de geautomatiseerde verwerking op te vangen.

Tot deze maatregelen behoren:

- het voorzien in de mogelijkheid tot het wijzigen van de koppelingen van beeldschermen, tekstverwerkende apparatuur etc., waardoor het uitvallen van een dezer apparaten opgevangen kan worden.
- het voorzien in een flexibele opvang in geval een deel of het gehele netwerk van verbindingen uitvalt (back-up van communicatielijnen). Belangrijk is: welke opvangfaciliteiten de leverancier van de geïnstalleerde apparatuur en datacommunicatielijnen biedt, de snelheid waarmee opvang gerealiseerd kan worden en het uittesten ervan.
- tijdens de ontwikkeling van kantoorautomatisering bij de apparatuurkeuze rekening houden met de compatibiliteit van de apparatuur, waardoor het mogelijk is bij uitval van een apparaat over te schakelen op een andere.
- het doen aanmaken en beveiligd opslaan van back-up-bestanden en back-up-programma's.
  Het loggen van berichten en van overige transacties.
- voorzien in de opvang van stroomuitval of van schommelingen in stroomsterkte.

4.4 Aanwezigheid van audittrail

Bepaalde vormen van kantoorautomatisering (ingrediënten) maken het mogelijk transacties te initiëren, zonder dat hiervan een schriftelijke vastlegging wordt gemaakt (electronic mailing, terminals voor overbrengen van spraak e.d.). Van een historisch overzicht van de verrichte transacties, waaraan vanuit controlegezichtspunt belang moet worden gehecht, (op eenvoudige wijze transacties volgen van begin tot eind en omgekeerd) is dan in het geheel geen sprake meer. Een dergelijke vorm van kantoorautomatisering zal de beheersbaarheid van de kantooractiviteiten niet ten goede komen. Het is niet meer mogelijk om achteraf inzicht te verkrijgen in de verrichte activiteiten, waardoor gemaakte fouten niet op juiste en controleerbare wijze kunnen worden gecorrigeerd. Ook op verzoeken om informatie omtrent verwerkte transacties zal niet ingegaan kunnen worden, hetgeen de bereikte servicegraad op grond van de verbeterde communicatiemogelijkheden teniet kan doen.
Duidelijk is, dat het aanwezig zijn en blijven van (liefst historisch traceerbare) vastleggingen van de verrichte transacties (lees kantooractiviteiten) zowel vanuit de beheersbaarheid van de kantoororganisatie als vanuit interne controlegezichtspunt eis is.

In dit hoofdstuk is ingegaan op enkele controle aspecten, die bij toepassing van kantoorautomatisering in een vergevorderd (integratie) stadium als belangrijk te onderkennen zijn. Daarmee zijn niet alle interne controle aspecten behandeld, met name niet de interne controle maatregelen, die ook bij andere vormen van automatisering kunnen worden aangetroffen.

5. Conclusie

Kantoorautomatisering is nog volop in beweging, waardoor de gedachtenvorming over kantoorautomatisering, over de integratievormen en over de interne controle en beveiliging ervan nog lang niet uitgekristalliseerd is.
Wel is duidelijk dat de gevolgen van kantoorautomatisering voor de interne controle en continuïteit van de informatieverwerking groot zijn en worden. Het tijdig onderkennen van deze gevolgen voor de ondernemingsleiding en de controlerende instanties (afdeling interne controle, interne accountant,externe accountant) is derhalve van groot belang.

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

compact

Zomer 1982

GARBAGE IN, GARBAGE OUT

door H. Veenman

Een verhandeling over controle- en correctiemethoden met betrekking tot computerinvoer ').

Steeds vaker ziet de accountant zich de laatste jaren genoodzaakt, de werking van een aantal geautomatiseerde systemen, zoals grootboek, facturering, e.d., te beoordelen in het kader van de jaarrekeningcontrole.

Een dergelijke systeembeoordeling houdt meestal in dat de tot het systeem behorende programmatuur geheel of gedeeltelijk wordt "gereviewed", terwijl ook (delen van) de output die gedurende een periode door het systeem is geproduceerd, wordt bekeken; dit alles om binnen het systeem een zo duidelijk en breed mogelijk controlepad of audit-trail te ontdekken.

Een ander onderdeel van een systeembeoordeling zou het bekijken van het zogenaamde invoerverzorgingsproces kunnen zijn, of wel door wie, waar en hoe worden gegevens in het systeem ingebracht, en wat zijn de mogelijkheden c.q. beperkingen tijdens die inbreng.

Het invoerverzorgingstraject is grofweg in drie delen te scheiden, nl. invoer, controle en correctie. De laatste twee stappen worden samen ook wel foutenbeheersing genoemd.
Wanneer de ingevoerde gegevens deze drie deeltrajecten, die meestal "voorin" in een systeem zijn gedefinieerd, zijn gepasseerd, wordt er door de gebruiker van uitgegaan dat ze "goed" zijn en tijdens de verdere verwerking als 100% betrouwbaar kunnen worden beschouwd. Dat dit zeker niet altijd terecht is, zal blijken uit het nu volgende betoog.

Invoercontrole op variabele gegevens

In de accountancy worden gegevens in twee categorieën ondergebracht, nl. vaste gegevens die reeds in een computersysteem bekend zijn, zoals NAW-bestanden, e.d. en variabele gegevens, de zgn. transactiegegevens, die worden ingevoerd. In dit stuk zal de aandacht op de tweede catagorie zijn gevestigd.
Computerinvoer bestaat voor 20 tot 40% uit variabele elementen, zoals prijs, hoeveelheid, temperatuur, e.d., terwijl het overige deel "vaste" gegevens genoemd wordt (artikelnummer, cliëntcode,etc.). Fouten in invoergegevens ontstaan tijdens de vastlegging. Dit vastleggen kan op verschillende manieren plaatsvinden:

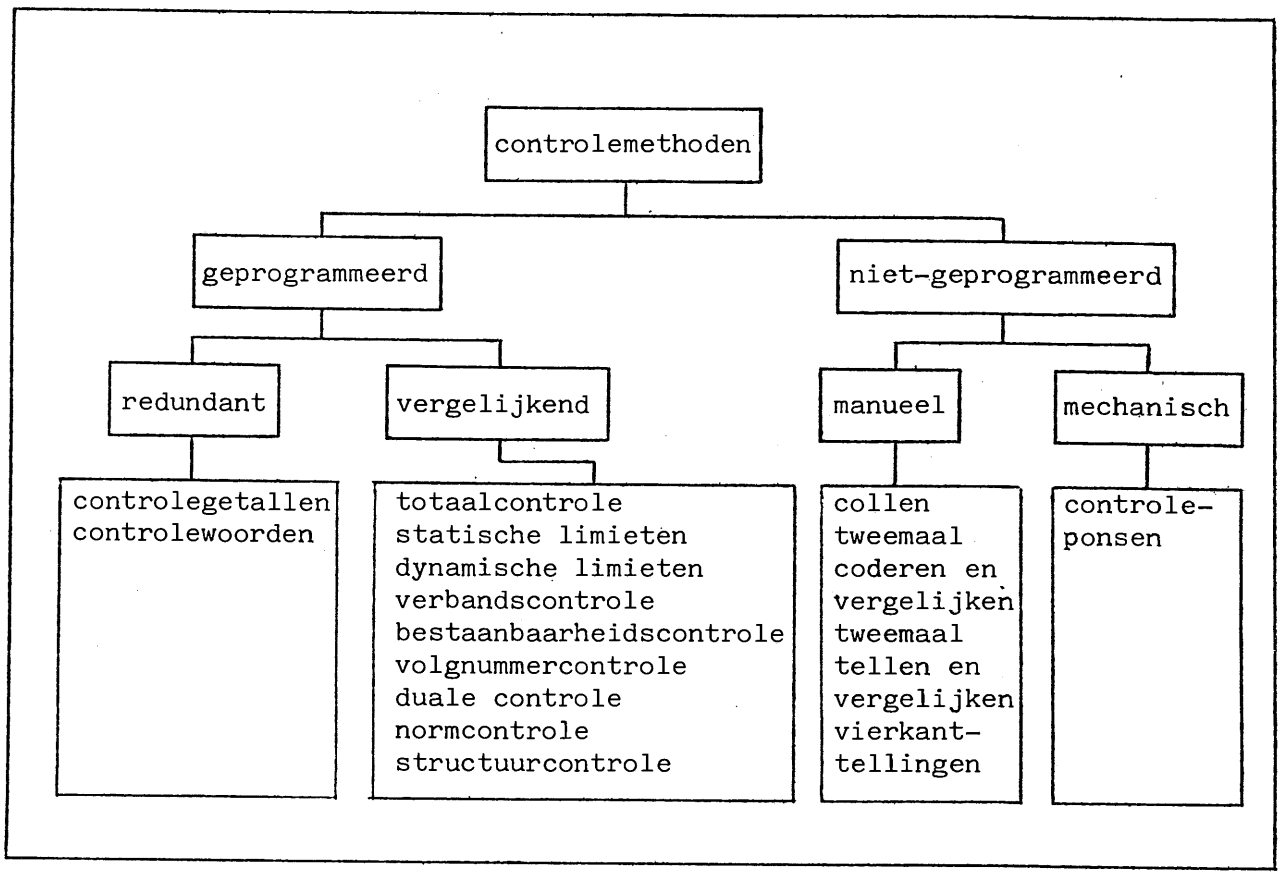
- via een data-entry-station; in beide gevallen worden de gegevens, voordat ze werkelijk in het betreffende systeem worden ingevoerd, op ponskaarten respectievelijk op schijf verzameld in groepen, zogenaamde batches;

') Tijdens het samenstellen is voornamelijk gebruik gemaakt van "Computerinvoer", van C. van Uitert.

- interactief, via een terminal; een gegeven wordt onmiddellijk na te zijn ingetikt, verwerkt. Het verzamelen in groepen vindt niet plaats.

De hierboven genoemde methoden betreffen alleen de mechanische vastlegging van gegevens. Hieraan vooraf gaat vaak nog de administratieve vastlegging, het overschrijven van de gegevens van een origineel formulier, strookje of iets dergelijks op een ponsdocument. Er dient echter naar te worden gestreefd de fase van administratieve vastlegging zoveel mogelijk uit het invoertraject te weren, daar ca. 2/3 van de invoerfouten tijdens deze fase tot stand komen (fouten door verkeerde interpretatie, verschrijving, omdraaiing, e.d.). De voorkeur gaat uit naar de zogenaamde gecombineerde vastlegging, waarbij de gegevens direct vanaf het originele document mechanisch worden vastgelegd. De eventuele codering van bepaalde gegevens (b.v. klantnaam naar klantcode) kan vooraf op dit document worden aangegeven.

Het controleren van gegevens, die als invoer voor een geautomatiseerd systeem dienen, kan globaal gezien in twee categorieën worden gescheiden, de manuele en de geprogrammeerde controles (zie figuur 1).



Figuur 1

Het accent komt de laatste jaren steeds meer op de tweede categorie te liggen omdat manuele controles, zoals tweemaal coderen of tellen, collen, controleponsen, enz. relatief gezien enorm duur, tijdrovend en onbetrouwbaar zijn geworden, omdat zij nu eenmaal door mensen moeten worden uitgevoerd. Het is daarom raadzaam zoveel mogelijk controles te programmeren en dus door de computer te laten uitvoeren. Door de behoefte is er in de loop der jaren een groot aantal te programmeren controletechnieken ontwikkeld, waarvan een deel als zeer efficiënt en betrouwbaar kan worden aangemerkt.

De categorie "redundante" controles kenmerkt zich voornamelijk door het feit dat, om een dergelijke controle uit te kunnen voeren, extra gegevens aan de invoer moeten worden toegevoegd, die voor de feitelijke verwerking geen functie hebben. De check-digit-controle is hiervan een bekend voorbeeld. Een redundante controle kan alleen op vaste gegevens worden uitgevoerd, omdat het aantal te verwachten ingevoerde waarden beperkt is.
Elk van deze controles, die gebruik maakt van controlegetallen (zie figuur 1), is in feite een check-digit-controle.
Aan ieder teken van een code (b.v. klantcode) wordt volgens een vast stramien een numerieke waarde toegekend. De som van deze waarden, vermeerderd met de waarde van het z.g. controlegetal of check-digit, dient een veelvoud te zijn van een andere vaste waarde, modulus genaamd; een veel voorkomende controle is de 11-proef, waarbij de waarde van de modulus gelijk is aan elf.
In figuur 2 is een overzicht weergegeven van een aantal van dergelijke controles met hun eigenschappen, waaruit blijkt dat een genuanceerde keuze, welke methode in een bepaald geval gehanteerd dient te worden, een noodzaak is.

Een tweede groep redundante controles maakt gebruik van een "natuurlijk woord" als toevoeging aan een code. Zo kan bijvoorbeeld in een orderadministratie als controlewoord van klant Pietersen (met klantcode 627047), diens telefoonnummer of een deel van zijn naam dienen: 627047 3445 of 627047 PIETE. Voorwaarde is wel dat het gegeven, dat als controlewoord wordt toegevoegd, tijdens het intoetsen duidelijk op hetzelfde document te lezen is als het klantnummer zelf, om praktische problemen te voorkomen.
Bij deze redundantiecontroles is het - tot op zekere hoogte - mogelijk autocorrectie te laten plaatsvinden, dus de computer met behulp van enkele formules een intoetsfout, hetgeen is ontdekt tijdens de controle, te laten corrigeren. Dit betekent echter niet dat de goedgekeurde of gecorrigeerde gegevens als "zeker goed" kunnen worden beschouwd. Er kan een "niet ontdekte" fout inzitten (zie figuur 2) of de fout kan verkeerd gecorrigeerd zijn.

proef		doeltreffendheid			redundantie	
modulo	gewichten, toegekend aan de tekens van een code (exclusief het controlegetal); de lengte van de code is 6 posities	niet ontdekte fouten (in %)	ontdekte fouten (in %)		benodigd aantal controletekens	
			enkelvoudige schrijffouten	verwisselingen	cijfers	letters
7	1.1.1.1.1.1	4,4	98		1	1
9	1.1.1.1.1.1	11,6	98		1	1
11	1.1.1.1.1.1	2,7	100	100	2	1
23	1.1.1.1.1.1	0,5	100	100	2	1
97	1.1.1.1.1.1	0,1	100	100	2	2
10	2.1.2.1.2.1	1,4	100	97,8	1	1
10	3.1.3.1.3.1	1,9	100	88,9	1	1
10	7.6.5.4.3.2	13,0	87	100	1	1
10	9.8.7.4.3.2	5,7	95	100	1	1
10	7.3.1.7.3.1	1,7	100	89	1	1
11	2.1.2.1.2.1	0,7	100	100	2	1
11	7.6.5.4.3.2	1,0	100	100	2	1

Figuur 2 Enkele foutendetectiemethoden en hun eigenschappen.

Naast de categorie van redundante controles zijn er ook de vergelijkende controles waarbij, zoals de term al doet vermoeden, ingevoerde gegevens vergeleken worden met vooraf berekende gegevens (b.v. hashtotalen), met waarschijnlijkheidgrenzen (b.v. het aantal besteleenheden dient tussen 1 en 100 te liggen), of met stamgegevens (in verband met bestaanbaarheid). In tegenstelling tot de redundantiecontroles hoeven ten behoeve van dezè categorie geen extra gegevens te worden ingevoerd. De meest bekende vergelijkende controles zijn:

- totaalcontrole, waarbij een voortelling van waarden van een groep in te voeren gegevens wordt vergeleken met een telling die door de computer is gemaakt; het doel is het ontdekken van intoetsfouten en het vaststellen van de volledigheid van het invoerrecord of van de complete batch.

  N.B. De volledigheidscontrole op batchniveau kan vanzelfsprekend alleen in een batch-omgeving plaatsvinden.

- controle met statische limieten, waarbij de ingevoerde gegevens (meestal numeriek) worden vergeleken met in het systeem vastliggende grenswaarden (b.v. bestelhoeveelheid mag niet kleiner zijn dan 20 en niet groter dan 400);

- controle met dynamische limieten, waarbij de ingevoerde gegevens (meestal numeriek) worden vergeleken met gedurende de controle berekende grenswaarden (b.v. bestelhoeveelheid mag niet meer dan 10% afwijken van de gemiddelde bestelhoeveelheid over de afgelopen 3 maanden).

Het doel van deze twee grenswaardecontroles is het nagaan van de waarschijnlijkheid van een gegeven; wanneer een controlegrens wordt overschreden zal de gegenereerde foutboodschap dan ook een waarschuwend karakter hebben.

- verbandscontrole; waarbij aan de hand van een vergelijking met andere gegevens wordt beoordeeld of een invoergegeven waarschijnlijk is;
- bestaanbaarheidscontrole; waarbij wordt vastgesteld of een ingevoerde code (b.v. klantnummer) bestaat of niet. De juistheid wordt echter niet gecontroleerd;
- volgnummercontrole; waarbij wordt vastgesteld of alle volgnummers, die op de invoerdocumenten staan, uniek aanwezig zijn. Dit is een volledigheidscontrole;
- duale controle; waarbij de gegevens tweemaal worden ingevoerd, waarna gelijkheid tussen de beide ingevoerde groepen gegevens dient te worden geconstateerd. Het invoeren kan geheel gescheiden plaatsvinden (andere locatie, persoon, tijd);
- normcontrole; waarbij de ingevoerde gegevens aan een bepaalde norm dienen te voldoen. In feite is dit een vereenvoudigde limietcontrole;
- structuurcontrole; waarbij de structuur van een gegeven wordt gecontroleerd, b.v. aantal in te voeren karakters, numeriek, alfabetisch, plaats van de komma, etc. Programmeertalen bieden vaak de mogelijkheid om een structuurcontrole te definiëren, zodat zij maar zelden expliciet behoeven te worden beschreven (bijv. in COBOL: wanneer een veld als PIC 9(2) is gedefinieerd, kunnen slechts numerieke tekens worden ingevoerd).

Als nadeel van de vergelijkende ten opzichte van de redundante controles moet worden vermeld dat bij vergelijkende controles slechts signalering en geen autocorrectie kan plaatsvinden.
Autocorrectie wordt reeds veelvuldig toegepast in de computer zelf en bij de transmissie van gegevens worden allerlei fouten automatisch hersteld, onder gebruikmaking van horizontale en verticale pariteitscontroles en bijzondere codestelsels.
Hoewel de noodzaak tot dergelijke methoden in de techniek groter is dan in de administratie en het binaire talstelsel zich er beter voor leent, is er toch al een aantal goede en bijzonder betrouwbare autocorrectiemethoden ontstaan.
Van Uitert laat zich in zijn boek zeer positief uit over autocorrectie zonder voldoende bij de beperkingen ervan stil te staan.

De in administratieve toepassingen met autocorrectie beoogde besparing op menselijke correctie is echter beperkt. Behalve dat deze procedures slechts bij enkele controlemethodieken kan worden toegepast en alleen op de vaste elementen in de invoer, is tevens het resultaat van een autocorrectie niet zonder meer betrouwbaar. Bij een doorsnee informatiesysteem vormen de vaste elementen (artikelnummer, cliëntcode, e.d.) 60 tot 80% van de totale invoer. Van de tijdens het invoeren van deze groep ontstane fouten, zijn 85 tot 90% enkelvoudige verschrijvingen of verwisselingen, de fouten die met behulp van autocorrectie kunnen worden verbeterd. Dit betekent dat grofweg 50 tot 75% van de totale invoer correct geautocorrigeerd kan worden. Of een op dergelijke wijze "verbeterd" gegeven tot die categorie behoort kan echter slechts door een manuele vergelijking met het brondocument worden vastgesteld!

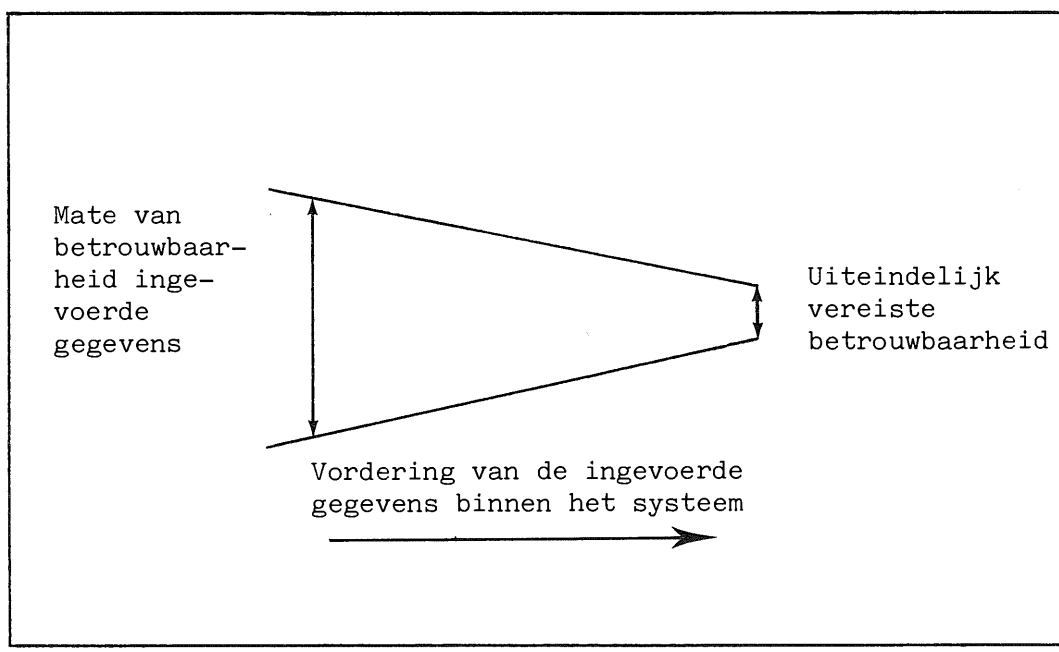
"Wanneer dient deze controle te worden uitgevoerd?", is een vraag die tijdens de ontwikkeling van een systeem aan de orde gesteld kan worden. Het meest eenvoudige is, om op het moment van invoer - dus tijdens het intikken bij online-realtime-applicaties en gedurende het inlezen van een batch in een batch-omgeving - per gegeven een aantal controles uit te voeren en aan de hand van de uitslag daarvan te bepalen of het gegeven "goed" of "fout" is. In het eerste geval is het gegeven voor verdere verwerking geaccepteerd, in het tweede wordt het uit het systeem geweerd.
Een nadeel van deze aanpak is echter dat er enerzijds te veel posten het predicaat "fout" meekrijgen, omdat door gebrek aan informatie, de controle te grof moet zijn, anderzijds kan een aantal "goede" posten nog foute informatie bevatten, doordat een bepaalde controle (b.v. een vergelijking) op dat moment eenvoudigweg nog niet uitgevoerd kan worden.

Voorbeeld
In een bestellingensysteem in de geneesmiddelenindustrie kunnen de aangesloten apothekers via een lokaal opgestelde microcomputer bestellingen invoeren op een cassettebandje. Tijdens de invoer worden controles uitgevoerd op onder meer de waarschijnlijkheid van het ingetoetste artikelnummer (check-digit-controle) en de bestelde hoeveelheid (structuurcontrole). Wanneer op dit punt een controle op bestaanbaarheid van het artikelnummer achterwege wordt gelaten, kan het voorkomen dat een niet bestaand artikelnummer, dat evenwel aan de check-digit-voorwaarde voldoet, op de cassette wordt geschreven; wordt er echter besloten wel een bestaanbaarheidscontrole uit te voeren (namelijk met behulp van een tabel waarin alle voorkomende nummers zijn opgenomen), dan is het mogelijk dat een nieuw artikelnummer niet wordt geaccepteerd omdat het nog niet in de tabel is opgenomen, hetgeen extra handelingen als telefoneren en opnieuw invoeren tot gevolg zal hebben.
Het al dan niet invoeren van een controle als hierboven beschreven, zal per toepassing overwogen moeten worden.

Aan het einde van iedere werkdag worden de bestellingen, die op cassettes zijn verzameld, via een telefoonverbinding overgeseind naar de computer, die centraal opgesteld staat bij de geneesmiddelenfabrikant; hier worden nog een aantal aanvullende controles op de binnengekomen bestellingen gedaan, zoals een controle op autorisatie: mag de betreffende cliënt dit geneesmiddel bestellen en zo ja, in welke hoeveelheden? Ook de controle op bestaanbaarheid van het artikelnummer zou hier, gebruik makend van het aanwezige artikelbestand, eenvoudig kunnen worden uitgevoerd.

Uit het bovenstaande voorbeeld moge blijken dat het pakket van controles, wanneer dit eenmaal voor een systeem is samengesteld, niet op één moment op de ingevoerde gegevens kan worden losgelaten maar dient te worden uitgesmeerd over een flink deel van het totale systeem.

Tijdens of pal na het invoeren zullen de eenvoudige controles worden gedaan, zoals structuurcontrole en check-digit-controle, terwijl de controles, naarmate de gegevens verder in een systeem doordringen, steeds genuanceerder en complexer zullen worden, doordat meer en meer neveninformatie voor zulke controles beschikbaar komt (zie figuur 3).



Figuur 3

Samenvattend kunnen wij stellen dat een "foutenbestrijdingssysteem" als onderdeel van een geautomatiseerd informatiesysteem als volgt kan worden opgebouwd:

- als eerste dient te worden besloten welke betrouwbaarheid van de betreffende invoergegevens in de verschillende stadia binnen het systeem moet worden geëist. De nadelige gevolgen van het niet of te laat ontdekken van fouten moeten worden afgewogen tegen het corrigeren ervan;
- aan de hand van deze eisen worden de verschillende controlemethoden gekozen, gebruik makend van statistische gegevens die over deze controlemethoden bekend zijn;
- men dient zich ervan te overtuigen dat verschillende gekozen controles elkaar niet overlappen, maar aanvullen om tot een optimale betrouwbaarheid te komen;
- er moet worden bepaald of de kosten en de remmende werking, die het foutenbestrijdingssysteem zonder meer zal hebben op de gegevensdoorvoer, redelijk zijn ten opzichte van de opgeleverde betrouwbaarheid.

Het is nuttig statistieken bij te houden van de gedurende de levensloop van een systeem optredende fouten, zodat van tijd tot tijd conclusies kunnen worden getrokken in hoeverre de tijdens de ontwikkeling verondersteld foutenverdeling overeenkomt met de praktijk.

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

compact

Zomer 1982

TESTEN ALS CONTROLETECHNIEK

door A.H.C. Koedijk

"We know that most people don't know what they are doing when they are testing." (State-of-the-art.)

1. Inleiding

Uitgangspunt van dit artikel is, dat testen van programmatuur een geaccepteerde controletechniek is voor de accountant (III). Het artikel richt zich op het niveau van de programmatest en is technisch van karakter; basiskennis omtrent de testtechniek en omtrent programmeren wordt bekend verondersteld. In de voorbeelden wordt de programmeertaal COBOL gehanteerd.

Testen is dan wel geaccepteerd als controletechniek, de state-of-the-art in de accountantsliteratuur gaat nog niet veel verder dan de "black-box" benadering (zie hoofdstuk 2). Dit artikel beoogt aan te geven, dat een meer fundamentele benadering, zeker als het gaat om gekwantificeerde, objectieve uitspraken omtrent de uitgevoerde tests (bij het gebruik van de techniek als controlemiddel), gewenst is.

In de automatiseringsliteratuur gesignaleerde "covering measures" (zie hoofdstuk 3) kunnen hierbij van nut zijn. Ze representeren echter nog niet een volgroeide oplossing voor de problematiek. De cijfers van Howden (zie hoofdstuk 3 onder Branch-testing) tonen dit aan. Onderzoek naar verdere verbeteringen is echter gaande.

Doelstellingen van het testen

Het doel van het testen van software kan in het kort worden aangeduid als het aantonen van:

1. de aanwezigheid en de juiste werking van de vereiste functies;
2. de juistheid van de structuur (de functies in hun onderlinge relaties);
3. de afwezigheid van ongewenste functies.

Onder functie wordt in dit artikel verder verstaan: een set instructies die alle tot uitvoering komen, zo gauw één ervan dat doet (dit wordt ook wel segment genoemd).

Probleemstelling

Gegeven de vermelde doelstellingen kan het vaststellen van de compleetheid van een uitgevoerde test als probleem worden genoemd; met andere woorden: hoe dekkend was de testset ten opzichte van het te testen programma?
Hierop wordt in dit artikel met name nader ingegaan.

2. Black-box testing

Het bij het testen benaderen van het programma als een "black-box" houdt in, dat uitsluitend wordt uitgegaan van de programmaspecificaties en dat de programmacode niet mede als basis dient voor het samenstellen van de testset en het beoordelen van de testresultaten. Wat zijn nu de uitspraken die op basis van de resultaten van zo'n test kunnen worden gedaan?

De aanwezigheid van de vereiste functies kan in principe worden vastgesteld.
De juiste werking van de functies is echter niet verzekerd: een juist verwerkingsresultaat van een bepaalde waarde voor een invoervariabele wil niet zeggen, dat dan ook alle mogelijke waarden voor die invoervariabele tot een juist resultaat zullen leiden. Overflow-fouten, bij voorbeeld, zullen soms moeilijk kunnen worden ontdekt. Dit is echter een probleem dat zich voordoet bij alle testtechnieken; slechts andere technieken (sourcecode review) kunnen hierin voorzien (er van uitgaande, dat de source-instructies juist worden vertaald door het vertaalprogramma en juist worden uitgevoerd door de machine).

Ten aanzien van eventueel aanwezige ongewenste functies kan worden opgemerkt, dat deze niet dan door toeval aan het licht zullen komen. Resteert nog het aantonen van de juistheid van de structuur. Indien het programma als een black-box wordt benaderd, dan is deze structuur onbekend; het aantonen van de juistheid ervan zal niet mogelijk zijn.

Bij het opstellen van de testset worden bepaalde aannames gedaan omtrent de geprogrammeerde oplossing. Er zijn voor een probleem echter vele programmeursoplossingen mogelijk.
De juistheid van de aannames zal door middel van onderzoek van de sourcecode moeten worden aangetoond.

Een voorbeeld moge dienen ter toelichting:

In de programmaspecificaties is opgenomen dat bij een waarde van VELDA tussen 10 en 20 ACTIE-1 moet worden uitgevoerd.
De test van een dergelijke functie zal zich normaliter richten op de grenswaarden van de conditie, derhalve testgevallen met waarden voor VELDA van

- 10 (ACTIE-1 dient niet te worden uitgevoerd)
- 11 (ACTIE-1 dient wel te worden uitgevoerd)
- 19 (ACTIE-1 dient wel te worden uitgevoerd)
- 20 (ACTIE-1 dient niet te worden uitgevoerd).

Een dergelijke test is gebaseerd op de geprogrammeerde oplossing:
IF VELDA > 10 AND < 20 .... (ACTIE-1).
De geprogrammeerde oplossing kan echter ook zijn:
IF VELDA = 11 OR 12 OR ..... OR 19 ..... (ACTIE-1).

Het risico bestaat dan, dat in de reeks 11-19 waarden ontbreken dan wel ten onrechte zijn opgenomen: indien in plaats van de waarde 14 abusievelijk de waarde 24 is opgenomen wordt dit bij een grenswaardentest niet ontdekt.

Hopelijk is hiermee in het kort aangeduid, dat de waarde van black-box testing beperkt is. De enige zekerheid die eraan kan worden ontleend is, dat de ingevoerde testgevallen (al of niet) juist werden verwerkt; hopelijk is de aanwezigheid van de vereiste functies aangetoond. Omtrent de juiste werking en een goede structuur van deze functies zal niet meer dan een (niet kwantificeerbare) indicatie zijn verkregen. Omtrent eventueel aanwezige ongewenste functies kan gewoonlijk niets worden gezegd.
De in de inleiding genoemde probleemstelling "hoe dekkend was de test" wordt hiermede nogal onbevredigend beantwoord.

3. Covering measures

Uit het bovenstaande vloeit voort, dat er behoefte bestaat aan een verder strekkende uitspraak, die bovendien in objectieve bewoordingen kan worden gegeven. In de automatiseringsliteratuur richt de aandacht zich hiertoe op "covering measures" (test evaluatie criteria, dekkingsmaatstaven) waarvan een reeks van verschillende niveaus is opgesteld (I, II).
Deze dekkingsmaatstaven hebben betrekking op alle in de inleiding genoemde doelstellingen, met uitzondering van de (mede) onder doelstelling 1 genoemde juiste werking van de functies; hierin kan, zoals in hoofdstuk 2 reeds is opgemerkt, sourcecode review voorzien (er van uitgaande, dat de source-instructies juist worden vertaald en uitgevoerd).
De dekkingsmaatstaven richten zich op de vraag: hoeveel van het programma is wel/niet getest (hoe dekkend was de testset ten opzichte van het te testen programma) en in eerste aanleg niet op andere aspecten van het testen (zoals het testen van speciale waarden:
- maximale waarde, -1, 0, +1, + maximale waarde; en dergelijke).

Doelstelling van de maatstaven is het bereiken van "100% dekking".

C0

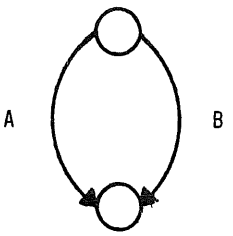
Het laagste niveau in de reeks covering measures is C0 (covering measure zero): "the percentage of statements exercised". Deze maatstaf, die in wezen de structuur van het programma buiten beschouwing laat, is bruikbaar indien sprake is van een programma dat alleen bestaat uit een "succession" (sequentie), met andere woorden: dus geen "alternations" (wissels) en geen "iterations" (herhalingen, loops). (Deze drie basisstructuren maken het mogelijk elke programmafunctie te bouwen.)

OVERZICHT BASISSTRUCTUREN

SUCCESSION

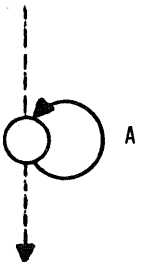
Voer A uit;
voer vervolgens
B uit.

ALTERNATION



Voer of A
of B uit.

ITERATION

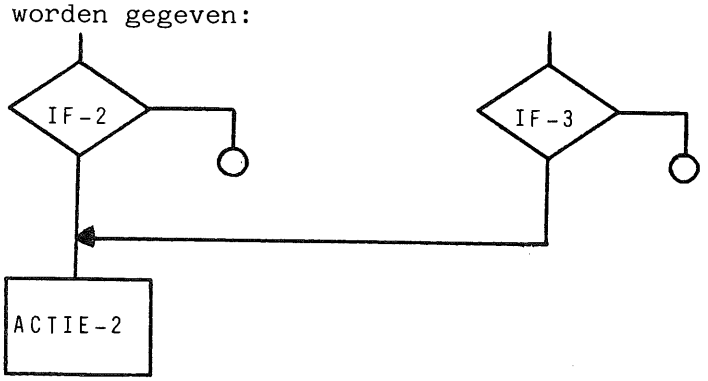


Voer A nul of
meer keer uit.

Programma's met een louter uit succession bestaande structuur komen in de data-processing praktijk nauwelijks voor. Sommige utilities (bij voorbeeld tape-to-print) benaderen een dergelijke simpelheid: denkbaar is, dat de end-of-file test de enige conditietest in zo'n programma vormt.

C1

Als "minimum coverage level" wordt genoemd C1: "the percentage of logical segments exercised". Onder segment wordt verstaan: een set instructies die alle tot uitvoering komen, zo gauw één ervan dat doet. Derhalve geeft 100% C1 aan, dat alle segmenten ten minste één keer zijn uitgevoerd. Als voorbeeld kan het volgende stukje programmalogica worden gegeven:



C1 vereist ten aanzien van ACTIE-2,
dat deze tenminste één keer wordt uit-
gevoerd (terwijl er twee ingangen zijn).

Ct1

Ct1 (de t staat voor "tree", boom) richt zich op minder goed gestructureerde programma's: segmenten moeten worden getest "in all their uses". Via de techniek van "hierarchical decomposition" (waarbij een hierarchische boomstructuur van het programma wordt vervaardigd, hetgeen geautomatiseerd kan geschieden; II, IV) komen deze boven water. Het uitvoeren van elk segment "in all its uses" verzekert dan dat elke "branch" (tak) in het programma minstens één keer is uitgevoerd. Ct1 geeft dus het percentage uitgevoerde takken in een programma; 100% Ct1 houdt in, dat alle takken ten minste één keer zijn uitgevoerd.
In het bovenstaande voorbeeld betekent dit, dat ACTIE-2 tweemaal moet worden uitgevoerd: zowel via IF-2 als IF-3.

Dit is wat algemeen wordt verstaan onder "branch-testing". Op deze techniek zijn geautomatiseerde hulpmiddelen als COMBI (VI) gericht. Een dergelijk hulpmiddel produceert naast de gewone programma-output tevens "coverage reports" (bij voorbeeld een overzicht van de niet-uitgevoerde takken).

Branch-testing: het doel bereikt?

Indien als testtechniek branch-testing wordt toegepast en een 100% dekking wordt behaald, is dan het doel bereikt?

Volgens de literatuur paste William Howden een aantal testtechnieken toe op een zestal programma's (V). Van de in totaal 28 fouten werden er met branch-testing 6 ontdekt, derhalve 21,5%. Van de 6 programma's waren er 2 bij die als normale data-processing programma's kunnen worden gekenschetst:

1. COBOL (450 regels): 3 fouten - 3 ontdekt. ')
2. PL/1 (175 regels): 20 fouten - 3 ontdekt.

(In de overige vier programma's, die niet als normale data-processing programma's kunnen worden gekenschetst, zaten 5 fouten waarvan er 0 werden ontdekt.)

Het percentage ontdekte fouten wordt dan 26%. Branch-testing lijkt derhalve nog niet een zeer betrouwbare techniek, zodat 100% Ct1 coverage nog steeds niet een zeer bevredigend antwoord geeft op de in de inleiding genoemde probleemstelling (hoe dekkend was de test).

') Ten onrechte kan hier de indruk ontstaan, dat ingeval sprake is van het gebruik van COBOL, branch-testing "the right technique" is, doch de 100% foutontdekking berust op toeval (geluk, zo u wilt).

Dit wordt onder meer veroorzaakt door AND- en OR-constructies. Om dit te verduidelijken diene als voorbeeld:

```
(1)     IF  VELDB > 6   OR    VELDC > 7   ... (ACTIE-2).
(2)     IF  VELDB > 6   AND   VELDC > 7   ... (ACTIE-2).
```

Dergelijke statements resulteren in twee logische takken:
de "true"-tak (er wordt aan de conditie voldaan) en de "false"-tak (er wordt niet aan de conditie voldaan, m.a.w. er wordt naar de ELSE-tak - achter de "punt" - gesprongen).
Verschillende waarden van VELDB en VELDC kunnen echter leiden naar de "true"- dan wel de "false"-tak:

(1) OR:

VELDB > 6	VELDC > 7	ACTIE-2	ELSE
nee	nee		X
ja	nee	X	
nee	ja	X	
ja	ja	X	

(2) AND:

VELDB > 6	VELDC > 7	ACTIE-2	ELSE
nee	nee		X
ja	nee		X
nee	ja		X
ja	ja	X	

Met het één keer uitvoeren van elk van de twee takken is derhalve nog geen fraaie "coverage" bereikt.

Overigens kunnen de fouten ook onontdekt zijn gebleven door de in hoofdstuk 2 vermelde problematiek bij het testen met betrekking tot het aantonen van de juiste werking van de aanwezige functies, waarin sourcecode review kan voorzien (aangenomen, dat de vertaling en uitvoering juist geschieden).

C-rel

Naar aanleiding van een paper van Howden voor de International Conference on Software Engineering 1981, is een nieuwe dekkingsmaatstaf opgesteld (II): de C-rel, rel staat voor reliability. Deze maatstaf is gebaseerd op "understanding the elementary functions within the statements that make up each logical segment in a candidate program". Deze maatstaf is een uitbreiding (en impliceert derhalve de eisen) van Ct1, doch kent nog een aantal aanvullende eisen, waarvan de volgende hier kort worden aangehaald:

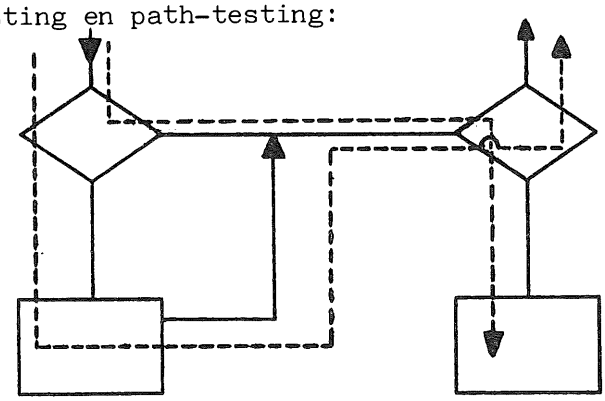
- and/or expressions: elk van de componenten van and- en or-constructies zodanig in de testgevallen verwerken, dat alle combinaties die leiden tot de "true"- dan wel de "false"-tak ten minste één keer voorkomen.

. data storage: elke waarde die resulteert uit een berekening dient te onderscheiden te zijn, zodat kan worden vastgesteld dat de inhoud van het machinegeheugen daadwerkelijk op de bedoelde wijze werd gewijzigd.

. Voorts wordt ondermeer het testen zo dicht mogelijk bij de grenswaarden van condities als regel gesteld.

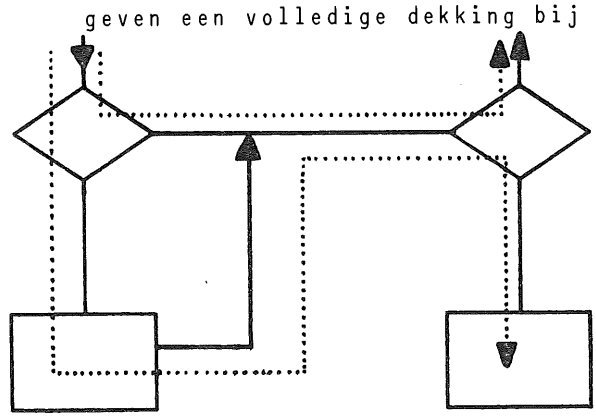
Path-testing

De eerder genoemde publicatie van Howden (V) vermeldt ook het resultaat van toepassing van path-testing op dezelfde programma's. Van de 28 fouten werden er 18 ontdekt. Voor de twee data-processing programma's (COBOL en PL/1) is het resultaat als volgt: 14/23, dat wil zeggen ± 60,8%.
Path-testing voldoet zo te zien dus beter dan branch-testing (over toepassing van C-rel bestaan helaas - nog? - geen cijfers).
Het volgende voorbeeld verduidelijkt het verschil tussen branch-testing en path-testing:



BRANCH-TESTING

De programmastroom wordt weergegeven door de ononderbroken lijn. De met ----- aangegeven testgevallen geven een volledige dekking bij branch-testing.



PATH-TESTING

Voor een zelfde resultaat bij path-testing zijn hiernaast nog de met ..... aangegeven testgevallen nodig.

4. Nawoord

Zoals in hoofdstuk 1 werd gesteld en hopelijk met dit artikel werd gemotiveerd is een meer fundamentele benadering van het testen als controletechniek gewenst, zeker als het gaat om gekwantificeerde, objectieve uitspraken omtrent de uitgevoerde tests.
De gesignaleerde covering measures kunnen hierbij van nut zijn, doch zijn (nog?) niet volmaakt, zoals de cijfers van Howden aantoonden.
C-rel lijkt veelbelovend, hoewel een adequate set "aanvullende eisen" noodzakelijk is. Te denken valt bij voorbeeld aan regels met betrekking tot in het programma gedefinieerde constanten en aan mogelijkheden van programmeertalen als tabelverwerking (indexering) dat "ontduiking" van de drie in hoofdstuk 3 genoemde basisstructuren mogelijk maakt; hierbij is sprake van het implementeren van "functies" anders dan door het creëren van takken. Path-testing lijkt eveneens veelbelovend, doch vereist een zeer groot aantal testgevallen. Bovendien zijn mij hiervoor nog geen geautomatiseerde hulpmiddelen bekend, hetgeen voor branch-testing (waarop C-rel is gebaseerd) wel het geval is.

Hopelijk geeft dit artikel enig inzicht in met het testen verbonden problemen.

Literatuur

I Program Testing Techniques (seminarnotes 1977, Edward Miller/ Software Research Associates).

II Testing Techniques Newsletters (Software Research Associates).

III Het gebruik van de computer in de accountantscontrole, deel II, Handboek Accountancy (Samsom).

IV Technieken om te testen (RCC-Bulletin).

V An evaluation of the effectiveness of symbolic testing, William Howden/Software-Practice and experience 1978).

VI Combi (Compact 6e jaargang nummer 17, voorjaar 1979).

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

compact

Zomer 1982

CONTROLE VAN HET "BESTURINGSSYSTEEM" ')

door H. Roos

1. Inleidende opmerkingen

De ontwikkeling van de edp-audit staat niet stil. Geleidelijk is de aandacht zich gaan uitstrekken over alle facetten in de automatisering die de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking beïnvloeden. Zo is er de laatste jaren, mede door de toename van het gebruik van gegevensbanken en van computergebruik op afstand, een toenemende aandacht ontstaan voor de rol die besturingssystemen daarin spelen.
Onder een besturingssysteem wordt verstaan het geheel van computerprogramma's dat het verlengstuk vormt van de zg. hardware.
Het omvat besturingsprogramma's in enge zin - het operating system - en uitbreidingen daarop ten behoeve van datacommunicatie, gegevensbankbeheer, etc., alsmede de programma's die nodig zijn voor het maken en wijzigen van toepassingsprogramma's, zoals vertaalprogramma's, tekstverwerkingsprogramma's, etc.

In dit opstel wordt een - bij mijn weten eerste - poging gedaan het besturingssysteem als object van accountantscontrole te belichten. Ongetwijfeld zal het nog geruime tijd duren voordat zich hierover binnen het beroep een consensus zal hebben gevormd.
Geen poging zal daarom worden gedaan met stelligheid aan te geven in welke situaties een onderzoek naar een besturingssysteem noodzakelijk is. Volstaan wordt met het aangeven van tendensen en dan nog zo beknopt als geboden is door de aard van deze rubriek.

2. Onderzoek naar de interne controle

In de oordeelsvorming door de accountant over een financiële verantwoording zijn, conform NIVRA-geschrift nummer 13, te onderkennen het onderzoek van de kolommenbalans - het routineprodukt van de administratie - van de waarderingsgrondslagen en van de presentatie. De grondslag voor het oordeel over de kolommenbalans wordt gelegd door een onderzoek naar de administratieve organisatie onder welks vigeur zij tot stand komt en door een onderzoek naar het cijfermateriaal waaruit zij is opgebouwd.

Voor dit opstel is alleen het onderzoek naar de organisatie van belang. Een dergelijk onderzoek bestaat uit het verwerven van een zodanig inzicht als nodig is voor het beoordelen van het stelsel van interne controle, voor zover van invloed op de betrouwbaarheid van het routineprodukt.
Ieder stelsel omvat zowel preventieve als repressieve interne controles. Beide soorten worden verwezenlijkt door een combinatie van functiescheiding en van daarmede samenhangende administratieve procedures.

') Dit artikel zal binnenkort tevens in "de Accountant" verschijnen.

3. Invloed van de automatisering

De registraties die samenhangen met de administratieve procedures kunnen geheel of ten dele zijn geautomatiseerd.
Zolang er verband gelegd kan worden tussen gecontroleerde primaire vastleggingen en het routineprodukt, kunnen de geautomatiseerde administratief-organisatorische processen bij het onderzoek worden beschouwd als "zwarte dozen" met als eigenschap dat er gegevens worden ingestopt die er, al dan niet bewerkt, op een later tijdstip weer worden uitgehaald.
Indien een verband echter niet of niet doelmatig kan worden vastgesteld zonder kennis van de werking van het geautomatiseerde proces, zal die kennis moeten worden verworven. Onderzoek van het geautomatiseerde deel van het stelsel van interne controle zal dan moeten plaatsvinden.
In dat kader komt, wegens de onvervangbaarheid van vele maatregelen, ook de vraag naar het beheer van het geautomatiseerde proces aan de orde.
Met name de vraag naar, hetgeen in NIVRA-geschrift nummer 26 wordt aangeduid als "het voor alle informatiesystemen geldende stelsel van maatregelen en procedures voor zover gericht op de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking".

4. De automatiseringsfunctie

Het beheer van het geautomatiseerde proces vereist specialistische kennis en vaardigheden en is derhalve meestal ondergebracht in een verbijzonderde automatiseringsfunctie.
Interne controle op deze functie, die de geautomatiseerde administratiesystemen - en dus ook de uitkomsten daarvan - kan beïnvloeden, wordt primair gezocht in scheiding tussen programmering (d.w.z. het maken en wijzigen van de computerprogramma's voor de geautomatiseerde administratieve processen) en het besturen van het computersysteem waarop de processen plaatsvinden en de gegevens worden bewaard.

5. Functie en beheer van het besturingssysteem

Zowel programmering als besturing maken gebruik van speciale programma's die het mogelijk maken de computerapparatuur op doelmatige wijze te benutten. De besturingsprogramma's hebben o.m. tot taak het zodanig tot uitvoering brengen van de programma's, dat deze elkaar en elkaars gegevens niet op onbeheerste wijze beïnvloeden. De bij het programmeren gebruikte programma's hebben tot taak de toepassingsprogramma's in een zodanige vorm te brengen dat zij nauwkeurig zijn afgestemd op de besturingsprogramma's.
Een toepassingsprogramma wordt meestal geschreven in een hogere programmeertaal, bijvoorbeeld COBOL.
Een COBOL-programma kan pas worden uitgevoerd nadat het is vertaald in een "taal" die door de machine kan worden "begrepen".
Een taal wordt door de machine "begrepen" indien hij de afzonderlijke taalelementen kan herkennen en de daarin vervatte opdrachten kan uitvoeren.

Deze taal vormt de machine-interface taal; een voorbeeld is de assembler-taal voor een bepaald type machine.

Het besturingssysteem wordt op basis van een meestal door de leverancier van de centrale verwerkingseenheid van de computerinstallatie geleverde versie voor de specifieke installatie geschikt gemaakt en periodiek gewijzigd of vernieuwd op grond van door de leverancier verstrekte wijzigingen of nieuwe versies. Voor deze werkzaamheden is kennis nodig van de machine, van de betreffende programma's en van de machine-interface. Het eventueel aanbrengen van wijzigingen in een standaardversie van het besturingssysteem geschiedt met behulp van de machine-interface taal.

6. Doeltreffende functiescheiding bemoeilijkt

De mogelijkheid direct in de machine-interface taal te programmeren en de noodzaak tot het van tijd tot tijd vervangen van besturings- en programmeringsprogramma's impliceren de mogelijkheid tot het beïnvloeden van administratieve programma's en van in de installatie opgeslagen gegevens.
Mede hierdoor blijkt het verwezenlijken van een doeltreffende functiescheiding tussen programmering en besturing een moeilijke zaak.
Deze situatie, die wordt veroorzaakt door:

- het gemeenschappelijk gebruik van dezelfde machine en dezelfde besturingsprogrammatuur door programmering, besturing en de overige bedrijfsafdelingen wier programma's en gegevens zich op de machine bevinden
- het beschikbaar en toegankelijk zijn van de mogelijkheid om op machine-interface niveau te programmeren

wordt verder gecompliceerd door:

- toename van het gebruik van de computerinstallatie op afstand, waardoor het oogtoezicht op de besturing wegvalt
- gemeenschappelijk gebruik van gegevens en programma's door controletechnisch te scheiden bedrijfsafdelingen.

De functie van het besturingssysteem bij de handhaving van functiescheiding binnen het computersysteem neemt daarbij in gewicht toe. Het management is verantwoordelijk voor een adequate vervulling van ook die functie.
Indien voor de oordeelsvorming door de accountant over de doeltreffendheid van die functiescheiding een oordeel over de bijdrage daarin van het besturingssysteem niet kan worden gemist, is een onderzoek naar dat systeem nodig.
Dit kan zich bijvoorbeeld voordoen bij geautomatiseerde systemen voor het verrichten van grote hoeveelheden betalingen waarbij door middel van datacommunicatie of door middel van magneetbanden integratie plaatsvindt met de bank- of giro-instelling die de betalingen uitvoert.

7. Een parallel

Het onderzoek naar het besturingssysteem dient te geschieden met dezelfde invalshoek als het onderzoek naar een "normaal" geautomatiseerd administratief systeem.

Elk "systeem" bestaat uit één of meer programma's die, wanneer zij op de computerinstallatie tot uitvoering worden gebracht, gegevens van een bepaalde vorm accepteren, daarin bepaalde veranderingen aanbrengen of daaruit andere gegevens afleiden - al dan niet met behulp van reeds in het computersysteem aanwezige gegevens -, gegevens bewaren in bestanden en gegevens afgeven.
Een programma zal dan ook steeds bestaan uit een aantal procedures en een beschrijving van de vorm en de betekenis van de te accepteren en af te geven gegevens.
Dit geldt ook voor besturingsprogramma's.
Net zoals een administratief toepassingsprogramma kent een besturingsprogramma bepaalde in- en uitvoersoorten en bepaalde bestanden.
De invoer kan bestaan uit zogenaamde besturingscommando's en uit binnen het computersysteem gegenereerde gegevens, die betrekking hebben op het verloop van de in de machine in uitvoering zijnde (actieve) toepassingsprogramma's. Door middel van boodschappen geeft het besturingssysteem informatie aan de bediening van de installatie en aan de actieve toepassingsprogramma's. De door het besturingssysteem bijgehouden "bestanden" bevatten gegevens over de situatie van de verschillende machinedelen, de actieve toepassingsprogramma's en de op het computersysteem in z.g. bibliotheken beschikbare programma's en bestanden.

8. Onderzoek van een besturingssysteem

Voor een oordeel als bedoeld over een besturingsprogramma zal in de eerste plaats het verband tussen in- en uitvoer, bibliotheken en de verschillende besturingsfuncties moeten worden vastgesteld.
Op basis daarvan kan worden bepaald welke functies van invloed zijn op de doeltreffendheid van de interne controle en welke daaruit voortvloeiende eisen moeten worden gesteld betreffende het gebruik van die functies.
Vervolgens dient te worden vastgesteld of en op welke wijze aan die eisen is voldaan.
Dit wijkt niet af van een onderzoek naar een administratief systeem.
Het verschil zit in de benodigde kennis en inzicht voor het kunnen begrijpen van het besturingssysteem in een concrete situatie en in de benodigde vaardigheid om te kunnen vaststellen of de beoordeelde gebruiksprocedures ook werkelijk bestaan.
De verkregen resultaten dienen uiteraard te worden gerelateerd aan andere facetten van het beheer van de geautomatiseerde processen.

9. Struikelblokken

De voornaamste struikelblokken voor de accountant lijken:
- de diepgang van de benodigde kennis
- de omstandigheid dat er in de praktijk een groot aantal verschillende computertypes voorkomt met per type dikwijls verscheidene besturingssystemen en
- per besturingssysteem verscheidene versies waartussen soms aanmerkelijke verschillen bestaan.

In de praktijk heeft zich voor het onderzoek en de oordeelsvelling over geautomatiseerde informatiesystemen binnen de grote accountantskantoren en -diensten reeds specialisatie voorgedaan door verbijzondering in een edp-audit-functie.
Het is een logische weg te proberen de voor het onderzoek van besturingssystemen vereiste kennis, inzicht en vaardigheden binnen die edp-audit-functie op te bouwen.

10. Aanzet tot kennisverwerving

De kennisverwerving zal zich aanvankelijk concentreren op één of enkele combinaties van computer- en besturingssysteem.
Deze kennis kan worden verworven door het volgen van leverancierscursussen. De ervaring is echter tot nu toe dat daarin weinig of geen speciale aandacht wordt besteed aan typische interne controle-aspecten.
Een probleem is vast te stellen welke kennis nodig is om de werking van een besturingssysteem als stelsel te begrijpen en van welke onderdelen een diepgaande kennis nodig is in het kader van de oordeelsvorming over de betrouwbaarheid.
Meer in concreto de vraag: hoeveel moet de edp-auditor van de machine weten om een besturingssysteem te kunnen begrijpen en hoeveel moet hij van een besturingssysteem weten om zich een oordeel over de betrouwbaarheidsaspecten ervan te kunnen vormen?

11. Op peil houden en uitbreiden van kennis

Wanneer een eerste aanzet is gegeven en het eerste praktische onderzoek is verricht, zal blijken dat het op peil houden en vooral ook het uitbreiden van kennis een zware claim legt op de schaarse tijd van de specialist, op wie bovendien juist wegens zijn specialisme bij voortschrijdende invloed van de automatisering op de accountantscontrole steeds frequenter een beroep zal worden gedaan.
De oplossing dient mijns inziens te worden gezocht in het ontwikkelen van een algemeen inzicht van voldoende diepgang en breedte waarmee de specialist in hopelijk de meeste praktijkgevallen, zonder al te tijdrovende raadpleging van specifieke documentatie en in elk geval zonder de noodzaak voor elk nieuw geval een leverancierscursus te volgen, zijn controle zal kunnen uitvoeren.

Dat ook dit niet eenvoudig is wordt onder meer veroorzaakt door het ontbreken van daarvoor geschikte literatuur.
Er is weliswaar als algemeen bedoelde literatuur over besturingssystemen beschikbaar. Geen enkel mij bekend werk is echter vanuit de specifieke invalshoek van de edp-auditor geschreven. De typische interne controle-aspecten zijn meestal onduidelijk of onvoldoende beschreven.
De edp-audit specialisten zullen waarschijnlijk in belangrijke mate zelf in deze leemte moeten voorzien.

12. Huidige situatie: MVS workshop

Bij de huidige stand van zaken spelen opleidingen, gericht op specifieke besturingssystemen, die een ruime toepassing vinden binnen de cliëntenkring van de grotere accountantskantoren en -diensten, nog een onmisbare

rol. Het behoeft niemand te verbazen dat dit in elk geval geldt voor de voornaamste besturingssystemen van de marktleider voor grote computersystemen en met name voor het MVS besturingssysteem van IBM.
De reden daarvoor is onder meer dat dit systeem een grote rol speelt bij grote bedrijven in de financiële sector waar juist het onderzoek en de oordeelsvorming over de interne controle een belangrijke plaats innemen in het controleplan van de accountant.

Speciaal voor het MVS besturingssysteem is een op edp-audit gerichte cursus beschikbaar die reeds éénmaal in Nederland is gegeven.
De hierdoor opgedane kennis blijkt in de praktijk goed en doelmatig toepasbaar.
Besloten is dan ook deze cursus, die bestaat uit drie dagen beginselen (concepts) met aansluitend twee dagen toepassing (workshop) in november 1982 te herhalen.

13. De CAV-werkgroep

Voorts dient te worden vermeld dat dit onderwerp de aandacht heeft van de werkgroep Opleidingseisen edp-audit, die in opdracht van de CAV bezig is met de afbakening van benodigde en wenselijke kennis en vaardigheden op automatiseringsgebied van zowel de (algemeen) accountant als van de edp-auditor.

14. Besluit

Het in de accountantscontrole betrekken van het besturingssysteem, waaronder begrepen alle standaardprogrammatuur voor het beheer en het onderhoud van geautomatiseerde gegevensverwerkende systemen, gebeurt reeds. Gemeengoed is het nog niet. Mits op doelmatige wijze uitgevoerd kan het een positieve bijdrage aan de accountantscontrole zijn. Voorwaarde is dat hieraan in de opleiding tot edp-auditor gerichte aandacht wordt besteed.
Een belangrijke hinderpaal is het vooralsnog ontbreken van goed opleidingsmateriaal. De edp-auditors zullen waarschijnlijk zelf in deze leemte moeten voorzien.
Voorlopig zullen leverancierscursussen nog een belangrijk middel tot kennisverwerving vormen.

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

GUIDE HAMBURG

Verslag van de 23e Guide gehouden te Hamburg van 1 tot en met 4 juni 1982

De Guide bijeenkomst werd door ruim 800 personen uit alle landen van West Europa bijgewoond, alsmede door enkele vertegenwoordigers van IBM uit USA en Australië.
Tijdens de Guide bijeenkomsten wordt een groot aantal parallelcessies gehouden; van de door mij bijgewoonde cessies volgt hierna een korte samenvatting.

A. Small System Executive/VSE (SSX/VSE)

Het besturingsysteem SSX/VSE is bedoeld voor de IBM 4321 en 4331 model 1, 2 en 11 met een geheugen grootte van 1 tot 4 mb.
Bij gebruik van SSX/VSE is een systeemprogrammeur niet langer benodigd; terwijl een full-time operator evenmin nodig zal zijn.
Van SSX/VSE wordt gesteld dat het op eenvoudige wijze kan worden geïnstalleerd:
. het wordt toegezonden op één tape in object formaat;
. er zijn geen sysgen-options;
. er zijn slechts zeer weinig user decisions noodzakelijk; enz.

De zogenaamde pre-generated VSE-based components zijn:
VSE/POWER version 2, VSE/ICCF version 3, ACF/VTAME, DOS/VS COBOL release 3 en DL1/SSX/VSE.

IBM stelt zich voor dat binnen organisaties een zogenaamde system administrator function aanwezig is.
Voor deze functie dient men een basiskennis automatisering te hebben en daarnaast kennis van het SSX die ca. 2 weken in beslag zal nemen.
Ten behoeve van betrokkenen bij SSX is een documentatie beschikbaar die ongeveer 2.000 pagina's beslaat.

Het SSX/VSE bevat zogenaamde DDP (Distributed Dataprocessing Functions).
Ook voor operators is het systeem eenvoudig te gebruiken: dit wordt gerealiseerd door het beschikbaar zijn van een automatische IPL en een automatische recovery ingeval van een emergency restart.

Met betrekking tot onderhoud werd uitdrukkelijk gesteld dat er van preventieve service geen sprake zal zijn. Er vindt uitsluitend zogenaamde corrective service on request plaats. Dit betekent dat op verzoek PTF (Protect Temporary Fixes) worden toegezonden; uitdrukkelijk werd daarbij opgemerkt dat er geen sprake zal zijn van prerequisite en evenmin van co-requisite PTF's.
Af en toe zal een zogenaamde refresh tape worden toegezonden, waarop zijn opgenomen:
. New system libraries in restore format
. Self Running jobs to update non-library data.

B. 8100 - an update on recent developments

Aangekondigd werd het model 8140 model c, met als bijzonderheden
. DPPX support in FEP 6;
. Dualprocessing elements;
. realstorage van 1, 1 1/2 of 2 mb (with ECC):
. Logical storage of 16 mb.

Verder werden genoemd DPPX/Base command facility extentions; DPPX/Interactive productivity facility en DPPX/Problem determination application requirements.
Van HCF (Host Command Facility) werd van versie 2 melding gemaakt:
. nieuwe functies: interface to the terminal access facility of the network communication control facility;
. device support for both 3270 (Display station) en 3767 (communication terminals).

C. Building flexible systems that anticipate unpredictable change

Spreker besteedde aandacht aan de filosofie van aanpak om een hoge flexibiliteit van systemen te verkrijgen. Hiertoe werd overgegaan tot een "table-approach", waarvoor een general purpose parameter management system werd ontwikkeld. De toegang tot de parameter data base is beperkt tot bepaalde functionarissen op grond van functie en niveau.

D. Application Development with IMS/ADF (Application Development Facility)

Als voordelen van het gebruik van ADF werden genoemd dat betrekkelijk geringe IMS en programmeringskennis nodig zijn; dat de "Datenschutz und Datensicherung" wordt ondersteund door middel van het moeten gebruiken van zogenaamde user profiles en tenslotte dat de beeldscherm lay out automatisch wordt ondersteund.

E. Experience in data administration using data structure analysis

De spreker over dit onderwerp lichtte uitgebreid de stappen data analysis, data base architecture en data base toe. Met nadruk wees hij op de noodzaak voldoende tijd uit te trekken voor de data-analyse, omdat wijzigingen later veel problemen en ongemak met zich meebrengen.

F. Report on the EDP-auditing function (Italië)

Een interessante voordracht op basis van een rapport dat door een Italiaanse werkgroep "Auditing EDP" is opgesteld. Het rapport kan bij Guide worden aangevraagd.

G. VM/SP in large MVS installation

De ervaringen met VM/SP waren opgedaan op een IBM 3033 en 3081 ieder 16 MB en 16 kanalen. Software-kenmerken van de machines waren: VM/SP release 1, MVS/SP, YES release 3, TSO, IMS, RACF, enz.

Als praktijkproblemen die tot nu toe nog niet waren opgelost werden genoemd:

* VM/SAVE functioneert niet goed wanneer de machine groter is dan 8 MB;
* Error recovery is incompleet.

H. RACF: from planning to realization; statement of experience

Bij de betrokken bank was een reeks apparatuur zoals 3081, 10x IBM 8100, enz. in gebruik alsmede voor wat betreft software MVS, VM/370, DOS, IMS, enz.
RACF was pas na een calamiteit geïnstalleerd; fouten in het rekening-courantsysteem van aangesloten banken bleken op eenvoudige wijze gecorrigeerd te worden met behulp van TSO.
De gehele beveiligingsoperatie had 41 mandagen gekost. Onder druk der omstandigheden was men ondermeer gekomen tot het opstellen van een Datensicherheits konzept.

I. Interface between EDP production en EDP development

In het onderhavige geval was sprake van een grote organisatie in Zwitserland (hardware: 3033 MB, 3x 3081, 2x 168 MP).
Het was noodzakelijk de relatie tussen ontwikkeling en produktie in deze ingewikkelde omgeving goed te structureren.
Daartoe werd een coördinatieteam ingesteld dat planning en voortgangscontrole in de gaten hield, alsmede de tijdige inschakeling van andere disciplines, zoals bijvoorbeeld produktie in verband met de produktiedocumentatie. Verder werden standaarden ontwikkeld en vastgesteld en werd het testcentrum gereorganiseerd (in het testcentrum was een 168 MP beschikbaar).
Benadrukt werd de invoering van een EDV Inspectorat d.w.z. interne EDP-audit.
De conclusie van spreker was dat de procedures en voorschriften over en weer waren geaccepteerd (d.w.z. ontwikkeling en produktie ieder afzonderlijk als in relatie tot elkaar);
De samenwerking was gerealiseerd en de rol van EDP-audit werd gewaardeerd.

J. Automation in planning and control of batch workload; experience with OPC

OPC staat voor Operations Planning and Control; blijkens de mededelingen van de spreker een uiterst doelmatig middel om automatisering te automatiseren. In het kort werd aandacht besteed aan het kalenderbestand, workload gegevens, e.d. op grond waarvan de computer een dagplanning kan maken. Met de uit de verwerking komende gegevens voor wat betreft CPU-capaciteit, kanalenbezetting, e.d. wordt het OPC-bestand bijgewerkt zodat de meest recente informatie beschikbaar is.

K. Early user experience with SQL/DS

Door een medewerkster van IBM werd de loftrompet gestoken over SQL/DS dat op een vijftal installaties in de wereld was geïnstalleerd om uit te proberen. De conclusies die hierna zijn weergegeven moeten dan ook met enige voorzichtigheid worden gehanteerd:

* cliënten waren tevreden;
* documentatie is uitstekend;
* uitgebreide gebruiksmogelijkheden;
* noodzakelijke opleiding voor DP-personeel slechts een halve dag;
* kwaliteit en stabiliteit verzekerd;
* performance: geen problemen;
* verbeteringen worden mogelijk geacht o.m. uitbreiden van commando's, gebruik nog eenvoudiger maken en toevoegen van data-types.

Zoals gezegd voorzichtigheid bij de uitleg van voornoemde punten is geboden.

L. An approach to information systems security

Door een medewerker van Arthur Anderson & Co. België werd een inleiding gehouden over hun wijze van aanpak van systeemonderzoek.
Alhoewel in principe hun aanpak niet afwijkt van die van KKC, was opvallend dat zeer de nadruk werd gelegd op autorisatie-controle-aspecten.
Verder werd nogal wat aandacht besteed aan het beleid ten aanzien van gegevensbeveiliging en de keuze van accesscontrol software.

Tot slot een sessie inzake "quality assurance in program development"

Een bijzonder interessante voordracht op grond van praktijkervaringen bij de ontwikkeling van een omvangrijk systeem.
Gebruikte trefwoorden/doeleinden:

* correctness of processing
* reliability
* simplicity for the user
* extandability
* maintainability
* testability
* auditability.

De betekenis van zgn. walk-thrumeetings werd onderstreept. Deelneners daaraan o.m. teamleider, db-spec., operations spec. en gebruikers.

De heer Cassani, president van IBM Europe gaf een overzicht van de strategische produkten, te weten series 1, S/34, S/38, 8100 en 43xx en voor wat betreft textprocessing 8100, 5520 e.d. Verder noemde hij het streven naar beperking van de ingewikkeldheid van HW en SW.

BOEKEN

CICA. "Symposium on Computers and Auditing". Toronto November 15-18, 1981.
AC 399.
De inhoudsopgave van dit symposiumboek is opgenomen als bijlage bij dit artikel.
Ter toelichting/handreiking op dit werk volgt een summiere bespreking.

I Lijst sprekers en deelnemers.

II Future systems.

A. The Uniform Communication System (U.C.S.)

Op pag. 19 wordt de conclusie weergegeven over wat het U.C.S. behelst en wat het niet is. U.C.S. definieert de algemene regels uit hoofde van controle van transacties tussen bedrijven. Een aantal aanbevelingen wordt gedaan; duidelijk is dat de gedachtenvorming nog niet ten einde is.

B. Auditor's Concerns with Electronic Funds transfer Systems

Op pag. 32 worden de tot nog toe onopgeloste controleproblemen beschreven (voldoende getrainde controleurs, verhouding controlekosten en de aanwezige risico's, "the switched systems problems").

III Accounting Control evaluation model.
Een pleidooi om te komen tot een systematiek om risico's te kwantificeren.

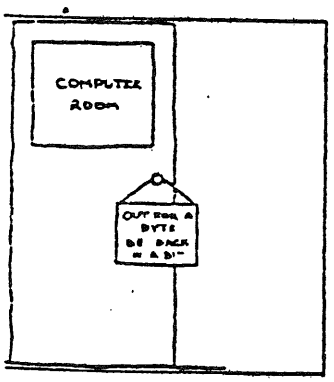
IV Audit documentation of complex systems.
Bestaan er wel goede richtlijnen om complexe systemen te documenteren? Zij worden immers gekenmerkt door de voortdurende stroom van veranderingen. In een aantal schema's tracht de spreker de weg aan te geven, hoe dit tot stand kan komen. Het is duidelijk dat wij nog aan het begin van een ontwikkeling staan (aldus H. Wiegers R.A.). Aan de hand van "Happy wholesale Hardware ltd" CICA-cursus Computer Audit Guidelines, toont een andere discussiant aan dat het Canadian Institute al enigszins gevorderd is met het documenteren van ingewikkelde systemen.

V Computers & The Law.
Dit onderwerp verdient grote aandacht, speciaal de onverwachte uitspraak van de rechters, die in deze geconstrueerde case zowel de eigen accountant als de accountant van het computercentrum veroordeelden. Bog afgezien van de controleproblematiek, was de onvoldoend zorgvuldig geredigeerde mededeling mede aanleiding tot de veroordeling (zie NIvRA 26).
Een bespreking van dit onderwerp staat in "De Accountant" van mei 1982, geschreven door H. Wiegers.

VIa Disaster recovery plans - To audit or not to audit ("The lack of adequate back-up planning is a significant audit Issue.").
Is een oordeel over het disaster recovery plan mogelijk?
Wordt het van de accountant gevraagd of moet hij het ook ongevraagd beoordelen?

VIb An Approach of the Audit of a Disaster Recovery Plan.
Overwegingen van een externe accountant wat nu wel of niet onder het plan zou moeten vallen.

VII Security Systems.
De ervaringen opgedaan bij het Amerikaanse leger zowel ten aanzien van computer security als software security, komen beschikbaar voor de private sector. Het is duidelijk dat betere resultaten worden bereikt ingeval van een ramp indien gewerkt wordt met nieuwe software dan met oude opgelapte. Het belangrijkste probleem blijft echter bestaan namelijk dat er geen standaardlijst bestaat met alle mogelijk voorkomende problemen; integendeel deze lijsten variëren sterk van installatie tot installatie.



Bijlage

TABLE OF CONTENTS

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

Tijdschriften

Zomer 1982

SPECIFICATION MODELLING

Software World vol. 12, no. 4
AC-Documentatie S819
Trefwoorden A40, A23

Tom DeMarco

door D. Jansen Heytmajer

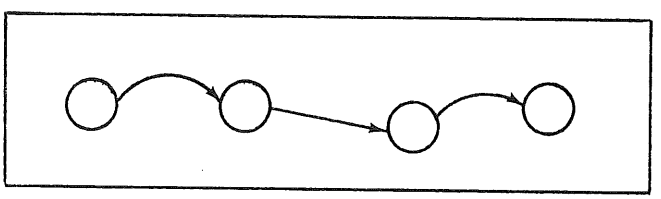
The most expensive failing of present day development methods is the inability to achieve early and meaningful understanding between users and developers on the key question: "What system shall we build?".
We need some new way to specify systems in advance of construction. The resulting specifications have to be:

- concise
- comprehensible to users and developers alike
- a natural lay-product of the user-developer negotiation
- easy and cheap to update
- such a graphic description of the new system that eventual installation brings no surprises about key system characteristics

Our solution to the problem is:

- build models to specify future systems
- show the modules to end-users of the system so that they will understand what they'll be receiving
- use the models to elicit user compliance
- when the user finds the proposed system wanting, make such alterations directly into the model and give him another chance to judge the result
- use the same modelling techniques to specify the rebuilding of systems (maintenance and enhancements)

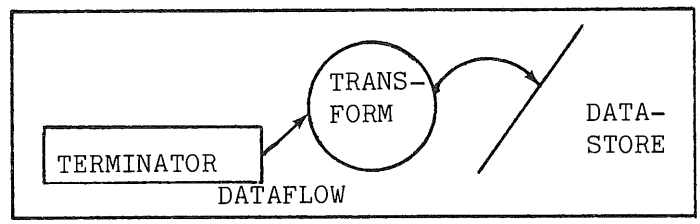
A system is a connected set of procedures used to carry out business policy. Some of the procedures may be automated and others manual.
A graphic portrayal of a system might look like this:



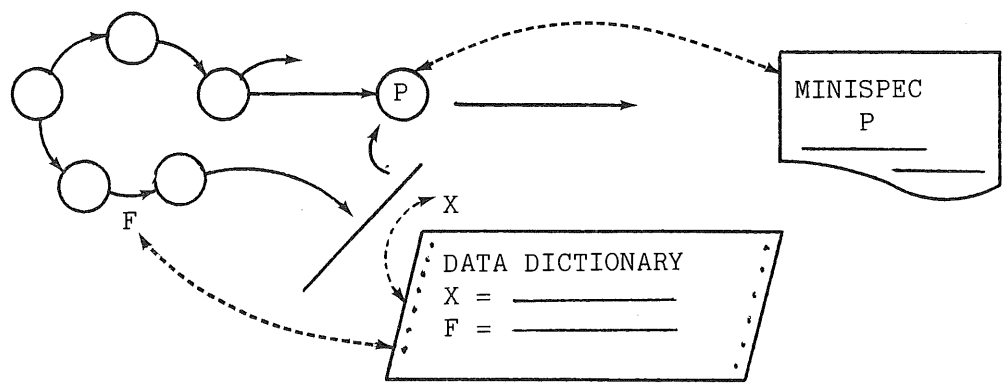
where the nodes represent procedures and the vectors represent connections.
Connections among component procedures are, for the most part, data streams carrying information of known composition.

Concept of the system model

A model of a system calls attention to the component procedures and to connections among them.
A Data Flow Diagram is a network representation of a system.
The elements that make up a DFD are: the dataflow (vector, indicating well-defined information flow), the transform (node, where incoming dataflow is transformed into outgoing dataflow) and terminators (outside sources or destinations of system data).



We do need a complementary tool, the Data Dictionary. This is the set of formal definitions of all dataflows and datastores declared on the Data Flow Diagram.
Formal definitions of a data item can be accomplished by declaring the component data elements that make it up and the relationships that apply among them.
All that is lacking to complete the model is a set of user-level specifications of the component procedures. They are called "minispecs". A minispec is a concise statement of user policy governing transformation of data at one mode of the DFD. The completed model and relationships among its components are described by the following graphic.



The DFD ties the elements together. For each dataflow or data store declared in the DFD, there is a complete definition in the Data Dictionary. For each primitive node on the DFD, there is a minispec stating user policy for data transformation at that node.

Evaluation of the Model

1. The three-part model avoids a major pitfall of alternate specification techniques by not concentrating on the machine.
2. The modelling costs are small.
3. By using DFDs we gain the advantage of a multidimensional tool, a picture, to represent the multidimensional nature of the system.

Large systems require the concept of levelling to allow top-down treatment. Levelled Data Flow Diagrams imply that a single figure is used to portray the whole system. The node of this top-level DFD might be thought of as "subsystems". This process of successive partitioning continues down to the primitive level, where nodes can not be further partitioned, or are judged small enough to specify via minispec.

Use of the model

The principal use of system models as described has been for specification of systems.
The same modelling techniques have been used succesfully for negotiations and specifications of changes to delivered systems.

compact

Zomer 1982

STANDARD COSTING IN DATA PROCESSING

AC-Documentatie 0363

door drs. B.M. de Vries

EDP Performance Review; june 1981

Er is geen algemeen aanvaarde methode voor de doorberekening van automatiseringskosten aan gebruikers. Dit administratieve gegeven is voor vele organisaties een probleem. Gebruikers zijn vaak ontevreden over de manier waarop hun kosten zijn gecalculeerd. Dit artikel is gebaseerd op een reële toepassing van de standaardkostenmethode.

De huidige situatie

Het computercentrum gebruikt een algoritme waarin de diverse gebruiksfactoren worden vermenigvuldigd met vaste tarieven. De uitkomsten daarvan worden doorbelast.
Deze benadering was niet altijd juist. Vaak vond doorbelasting voor niet-gebruikte diensten plaats.
Datacommunicatiekosten werden beschouwd als onderdeel van de kosten van de centrale verwerkingseenheid. Gebruikers van alleen stapelverwerking betaalden zodoende mee aan de datacommunicatie waarvan zij geen afnemer waren. Hierdoor was het computercentrum niet in staat de kosten voor de gebruikers juist te begroten.

Standaardkosten

In een poging een aantal van de boekhoudkundige en communicatieve problemen op te lossen werd besloten een standaardkostensysteem in te voeren. De gevolgde benadering was die van "Management Control of EDP Performance" door Barry Stevens en Phil Howard.
Deze benadering omvat negen stappen.

1. De bepaling van de produktie-eenheden

Een fysieke groep van mensen en produktiemiddelen wordt beschouwd als een produktie-eenheid. Ieder eenheid verricht produktieve functies die gemeten kunnen worden in werkeenheden.
Bijvoorbeeld kan het opzetten van magneetbanden gezien worden als een produktieve functie. De centrale verwerkingseenheid heeft slechts één functie; namelijk verwerken.
De prestatie wordt gemeten in "busy" tijd als werkeenheden.
Binnen één produktie-eenheid moet voor ieder produktiemiddel een maatstaf voor de capaciteit ervan worden toegewezen. Hardware-capaciteit kan worden gemeten in invoer/uitvoerbewerkingen of gedrukte regels.
Het identificeren van produktie-eenheden is doorgaans niet moeilijk, maar het beslissen over de maatstaf is vaak een moeilijker opgave. Het interviewen van de betrokken medewerkers ten aanzien van hun ideeën met betrekking tot de maatstaven is als nuttig ervaren. De werkzaamheden in deze stap resulteren in een totaal budget van mensen en middelen voor iedere produktie-eenheid.

6. Voorspel de hoeveelheid werkeenheden (= normale produktie)

De bepaling van deze grootheid kan geschieden door analyse van historisch materiaal in combinatie met discussies met gebruikers. De gebruikers kunnen gegevens aandragen die, zo nodig, als wijziging op de historische gegevens worden aangemerkt. Idealiter echter dient de taxaties van de transactievolumes volledig door de gebruikers te geschieden. In een aanvangsfase kan dit echter op praktische problemen stuiten.

7. Becijfer "voorlopige" dekking

Alle gegevens zijn nu voorhanden om de standaardkosten om te zetten in doorbelastingen. Eerst wordt een voorlopige berekening gemaakt. De uitkomsten daarvan zijn doorgaans niet zonder meer bruikbaar. Met name de berekende beschikbaarheid kan arbitrair zijn.

8. Bereken dekkingsconstanten

Om de voorlopige dekking af te stemmen op de totale budgetten van de produktie-eenheden wordt een dekkingsconstante gebruikt. Deze wordt berekend uit de formule:

$$\frac{\text{budget produktie-eenheid}}{\text{(hoeveelheid werkeenheden x standaardkosten per werkeenheid)}}$$

De berekend constante zal doorgaans groter zijn dan één. Alle tarieven berekend in stap 8 moeten ermee worden vermenigvuldigd om de kosten van de produktie-eenheid te dekken.

9. Bepaal de definitieve tarieven

Tenslotte worden de tarieven vastgesteld. Alle tarieven zijn op basis van werkeenheden. Het moeilijkste deel van de berekening van de doorbelasting is het uitzoeken van de werkeenheden waarvan een bepaalde toepassing gebruik maakt.

Nevenvoordelen van de standaardkostenbenadering

De standaardkostenbenadering heeft een aantal nevenvoordelen afgeleid van het oorspronkelijke doel.
De voordelen zijn:

- Het wordt gemakkelijker met de gezamenlijke gebruikers voorspellingen en budgetten op te stellen. Vooral wanneer deze in begrijpbare termen worden uitgedrukt (bijvoorbeeld aantal inkooporders).
- Het bepalen van de tijd nodig om een werkeenheid uit te voeren verschaft bruikbare informatie om de arbeidsproduktiviteit te meten en de samenstelling van takenpakketten te analyseren.
- De bezetting van produktie-eenheden kan worden gevolgd.

2. Beschikbaarheid

Deze is gedefinieerd als de totale capaciteit van iedere produktie-eenheid.
Als bijvoorbeeld een persoon per jaar 1.760 direct produktieve uren kan maken, is de beschikbaarheid voor een produktie-eenheid van 10 medewerkers 17.600 uren. Leiding gevende taken worden daarbij als niet-produktief aangemerkt en niet in de beschikbaarheid meegeteld.
De beschikbaarheid van de hardware wordt berekend met de formule:

gemiddelde bezettingspercentage
(maximale capaciteit -/- gemiddelde tijdverlies)

Het gemiddelde bezettingspercentage is het bezettingsniveau over een langere periode.(= normale produktie). Voor de centrale verwerkingseenheid kan 50% normaal zijn. De vaststelling van het percentage is arbitrair. Het juiste evenwicht wordt gevonden door "trial and error".

3. Bereken standaardkosten

De standaardkosten van een produktie-eenheid worden gevonden door het totale budget te delen door de beschikbaarheid.

4. Bepaal de tijd nodig om de werkeenheid uit te voeren

Elke produktie-eenheid verwerkt een aantal te onderscheiden werkeenheden. Van iedere werkeenheid moet de benodigde tijd worden vastgesteld. Voor "machinale" werkeenheden kan het Job accounting systeem een goed informatiemiddel zijn.
CPU-tijd besteed aan een specifieke transactie gedeeld door het aantal transacties geeft inzicht in de tijd benodigd voor de verwerking van een transactie van dat type.
Voor menselijke handelingen en voor hulpapparatuur zoals decollators zal op een of andere manier een administratie moeten worden bijgehouden om de relatie tussen tijd en werkeenheid te kunnen leggen.
(Het originele artikel bevat een voorbeeld van de hierbedoelde berekening ten aanzien van de produktie-eenheid operators.)

5. Bepaal de standaardkosten per werkeenheid

De standaardkosten per werkeenheid worden gevonden door de in stap 3 becijferde standaardkosten te vermenigvuldigen met de in stap 4 berekende benodigde tijd.

Samenvatting

Het gebruik van standaardkosten biedt een aantal voordelen voor de automatiseringsafdelingen zowel als voor de gebruikers. Het voornaamste voordeel is, het gebruik van direct aan een toepassing gerelateerde tarieven voor de gebruikers. Indirecte voordelen zijn een beter inzicht in de produktiviteit en bezetting. Tenslotte zal door de standaardkostenbenadering een eind komen aan de verwarring tussen gebruikers en computercentrum ten aanzien van de kostendoorbelasting. Hieruit zal vaak een verbeterde relatie resulteren.

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

Automatisering Beveiliging Controle NIEUWS

door drs. H.C. Kocks

Automatisering

Het volgende had ook onder het hoofd "Controle" van ABC-nieuws kunnen worden opgenomen.
De schrijver gaat in op de "audit problems" bij laser printers, die echter het gevolg zijn van nieuwe technologische ontwikkelingen.

LASER PRINTER PROBLEMS (Carl R. Wolf)

While laser printers offer new opportunities for significant time and cost savings, they also create control problems.
At Transamerica Corporation we have seen the time required for long print runs of negotiable instruments (checks, drafts, bonds, stock certificates, etc.) reduced dramatically. For example, the printing of 22,000 checks formerly took 12 to 14 hours on the impact printer, plus several more hours on the signature-bursting equipment. On a laser printer, it takes only four hours.
Many of the laser printers can complete the entire printing of a form on blank, or near blank, stock paper as well as imprint the data on the completed form. At Transamerica, for one application we use stock paper with only our logo and the MICR (Magnetic Ink Character Recognition) bank routing codes preprinted. The rest of the form, including the signature, has been digitized (converted into electrical signals) and stored on a removable disk. This disk is loaded onto the laser printer for each print run. A magnetic tape created by an application production program provides input of payee and check amount information.
Since we are using nearly blank stock, we avoid the enormous physical security problems involved in storing preprinted negotiable instruments. In addition, the control problems associated with signature plates have been eliminated. However, we now have new security problems involving the removable disk and its magnetic tape backup. We have addressed these problems by storing both in secure environments.
The removable disk, for example, is stored in a safe-deposit-box-type metal cabinet requiring two keys to open. Data Processing Operations has one key and the user the other.
But what about the equipment used to scan the original document that created the digitized form and, more importantly, the digitized signature? What are the vendor's controls over this equipment? We now have the technology to recreate any signature on any document that can be produced on a laser printer and do it without the knowledge of the owner of that signature. This is not a forged signature. It appears to be an identical printed signature without any noticeable differences from a handwritten signature.

In May 1982, while visiting a vendor display area at a conference, I was offered scanning equipment that could be used to digitize forms and signatures. I was assured that the equipment would create a magnetic tape which could be used to load the removable disk associated with laser printers. The supplier of this equipment did not manufacture laser printers!
Large laser printers are not the only security and control problem that has recently appeared. A new line of word processing equipment has been added to the office automation field. One manufacturer is offering a smaller laser printer which also serves as a copy machine. It can store digitized forms and signatures.
This printer is designed to be used with floppy disk input from word processing stations in non-data processing departments.
The new laser word processing printer uses a permanent disk. Digitized forms and signatures can be indexed for permanent storage or just loaded for temporary use by each application. The word processing operator calls up the proper form and the appropriate signature by typing the correct codes when a letter or document is transcribed upon the floppy disk. Whatever information is transcribed upon the floppy (advertisement, interoffice memo, procedures, etc.) is then produced on the proper form with the appropriate signature. Either blank copy paper or special paper can be used.
If the index numbers for all the signatures permanently stored on the laser printer are compromised, or the floppy disk with a signature code falls into the wrong hands, everyone in the department may be given salary increases or extra vacation authorized by letters to the Payroll Department with the appropriate manager's signature on them. Further, if the digitized form permanently stored on this printer unit is a negotiable instrument, a massive fraud could easily take place.
We have entered a new era of rapidly developing technology. Simply by dialing the appropriate telephone number, we can communicate across the country from one word processing station to another or from a word processor to big mainframe computers. Controls for computers and computer-related equipment are mandatory, but it appears that technology is ahead of the auditor. It is occasionally lonely to be on the leading edge, or "bleeding" edge, as it has been called. We at Transamerica Corporation would like to share ideas and thoughts with other companies which have similar control problems.

EDPACS, juli 1982

De eerste stormen met betrekking tot de privacy-wetgeving zijn wat geluwd. Het leek ons echter goed onder uw aandacht te brengen dat ondanks de kritische beschouwingen inzake het wetsontwerp de eerste contouren van een echte wetgeving zichtbaar worden. Het volgende artikeltje geeft enige inhoudelijke informatie met betrekking tot het "aanmeldingswetje".

AANMELDINGSWETJE MOET DIENEN ALS WEGBEREIDER VOOR WET OP PRIVACY

DEN HAAG - Bij de momenteel op zomerreces zijnde Tweede Kamer is een wetsontwerp ingediend dat betrekking heeft op de aanmelding van geautomatiseerde persoonsregistraties.

Het wetsontwerp, dat is opgesteld onder verantwoordelijkheid van Minister J. de Ruiter en Staatssecretaris M. Scheltema van Justitie en van de Minister van Binnenlandse Zaken, M.G. Rood, is bedoeld als voorloper van het in november van het vorige jaar ingediende wetsontwerp op de persoonsregistraties. Deze wet is zo omvangrijk dat de invoering ervan gefaseerd zal geschieden en enkele jaren in beslag zal nemen.
De aanmelding, die nu in de "Tijdelijke wet aanmelding geautomatiseerde persoonsrehistraties" geregeld gaat worden, maakt deel uit van de maatregelen in de uiteindelijke wet. De tijdelijke wet voorziet in een aanmeldingsplicht van bestaande en nieuw te vormen bestanden bij een op te richten register, dat wordt gevestigd bij het Ministerie van Justitie en een voorloper is van de in de uiteindelijke wet genoemde registratiekamer.
In de tijdelijke wet wordt niet zoals in de uiteindelijke, onderscheid gemaakt tussen meldingsplichtige, reglementsplichtige en vergunningsplichtige persoonsregistraties, drie categorieën met een oplopende "gevoeligheid" van de vastgestelde persoonsgegevens. Het gaat bij de voorlopige aanmeldingswet vooral om een inventarisatie, die de behandeling van het "grote" wetsontwerp in de Tweede Kamer moet ondersteunen.
Maar van bijna even groot belang wordt een stimulerende werking geacht: de aanmeldingswet zou een stootje in de rug zijn op de weg naar een zekere zelfregulering, vooruitlopend op de uiteindelijke wet. Voor deze zelfregulering zal de rijksoverheid overigens het goede voorbeeld geven door de eigen bestanden met persoonsgegevens systematisch te gaan doorlichten. De behandeling van het nieuwe aanmeldingswetsontwerp in de Tweede Kamer zal nog wel enkele maanden op zich laten wachten.

Computable, 6.8.1982

NIEUWE RELEASE Jasper/JA

Computer Associates heeft release 2.0 van Jasper/JA uitgebracht, die is ontworpen voor de OS/VS1- enMVS-gebruikers waarmede de produktiviteit van de hardware als van de software kan worden verbeterd door het constant bijhouden en meten van de systeemprestatie. Het nieuwe release is uitgebreid op het gebied van systeemmetingen met dagelijkse, wekelijkse, maandelijkse en jaarlijkse rapporteringen van alle hardware- en software-activiteiten van het OS/VS1- en MVS-besturingssysteem.
CA-Jasper/JA biedt analyse met betrekking tot de actieve tijd (cpu-plus i/o-tijden) en abends, vastlegging van gebruik van de verschillende resources, mogelijkheden om de kosten door te boeken, uitgebreide overzichten ten behoeve van het management, het vastleggen van TSO-, VM- en SMF-gegevens en een interface naar CICS performance analyzer van IBM.

Zomer 1982

De CICS PAII interface van Computer Associates voorziet in de mogelijkheid om CICS-data te combineren met VM, TSO en batch-gegevens, waardoor nu voor de eerste keer een complete verslaggeving van systeem- en gebruikersactiviteiten wordt geboden. De report-generator van CA-Jasper/JA, Wizard genaamd, levert specifieke bedrijfsgerichte analytische overzichten van elke gewenste informatie.

Het gaat hierbij om een in de accountantswereld aangeduid "accounting-systeem", een registratiesysteem waarmee het gebruik van de computer kan worden vastgelegd, onder andere voor doorberekeningsdoeleinden.

Beveiliging

In Computers & Security van januari 1982 (first issue of a new journal) vonden wij een artikel met de kop:
"International Computer Crime: Where Terrorism and Transborder Data Flow Meet" van J. BloomBecker.

Steeds meer krijgt transborder data flow betekenis. De security-aspecten van de automatisering worden in een internationaal kader geplaatst met alle problemen van dien. De conclusie uit bovenvermeld artikel willen wij u niet onthouden.

CONCLUSION
In light of the serious concern for the sovereignty of nations, and the security of individuals, which permeates the talk about transborder data flow, it is rather puzzling that so little attention has been paid to the threat both to nations and individuals posed by the computer criminal. Whether they are terrorists, would-be instant multimillionaires, or corrupt multinationals, it seems unrealistic to expect their ardor, resources, or persistence to be less than those of the would-be privacy invaders whose threat the transborder data flow talks take so seriously. Though certainly not without sin, the corporations and the governments most feared as agents of privacy invasion do have primarily valid purposes for their existence. By definition the data processing efforts of computer criminals do not fall in this catagory.
What one author said about terrorism applies, I suggest, to the whole of international computer crime. *"A determined response to international terrorism is not a matter of choice - it is a question of survival".*

TDF zal wellicht steeds meer hinder ondervinden van nationale wetgevingen.

Uit het volgende stuk uit Transnational Data Report blijkt dat die nationale wetgevingen beperkingen kunnen opleggen aan de "remote support centres" van computerleveranciers.
Is dit misschien het begin van het einde van die centers?

DOES REMOTE COMPUTER FAULT DIAGNOSIS INVOLVE TDF?
(Transborder Data Flow)

IBM, Burroughs, Digital and other mainframe and minicomputer manufacturers have developed remote support centres to monitor and diagnose problems in computers operated by their customers. TDR has been asked whether remote diagnosis may involve the transmission of data from a customer's computer in one country to a service centre in another; thereby, TDF?

Digital, for example, has invested several million dollars in remote diagnosis centres in the US and Europe. On the Continent, thousands of minis are connected through a network to the Digital centre at Valbonne in Southern France.

At this regional service centre a special microprocessor and communications interface with the customer's system enables service engineers to determine what is faulty. It may be necessary to have access to data in the customer's computer; and bring some data to the diagnosis centre.

There has been at least one well publicized case where TDF was involved and use of the diagnosis service refused. A Burroughs computer, used by the Canadian Government to process unemployment insurance records, was to be serviced by the company's remote diagnosis centre in California. Because of strict restrictions on access to these records in Canadian law, Burroughs was refused permission to monitor or diagnose the computer, except in Canada under the supervision of government officials.

W. Michael Blumenthal, Chairman of Burroughs, told the National Computing Conference in May 1981 that this Canadian case typifies the increased hampering of efficient use of computers, and constitutes a form of protectionism.

Blumenthal said: "Recently, Canada denied a Burroughs petition to dial into a government computing system in order to service our hardware. That's a very good case in point. And how, I ask you, will it affect the financial community in which so much of the work of my company is being done? How will it affect electronic funds transfers? We operate the Society for Worldwide Interbank Financial Telecommunications (SWIFT). How will we efficiently be able to operate the SWIFT system in the face of these kinds of restriction?

"These are the kinds of practical issue that occur to us in our company, and I'm sure they can be duplicated over and over again in the case of other companies in the same field."

Toegangsbeveiliging houdt de computerwereld bezig.
Naast de fysieke beveiliging is dat tevens de software-matige beveiliging van de toegang tot gegevens via terminals. Steeds nieuwe vindingen worden onder de aandacht gebracht.
In Edpacs van februari 1982 vonden wij het volgende:

Access Control Hardware

The Computer Security Institute's recent conference in New York City included a number of vendor exhibits of security-related products. Four access control devices were particularly interesting. A fifth device, under development, is also described.

FINGERPRINT CONTROL
Fingermatrix Inc. offers what appears to be a practical method of using fingerprints as an access control key. Their device can be utilized to control physical access to a facility or to secure a terminal device against unauthorized use.

Authorized user verification takes less than five seconds, and the device is insensitive to finger skin condition. Since control is based upon something the individual always has with him, the human interface is quite simple.

Physical Access Control. Each Fingermatrix System 201 can support a maximum of 64 terminals or access units and store about 100,000 individual identifications. The access units may be directly connected to the host computer or linked by standard telephone lines for remote data communications. A system printer may be used to prepare a log of all access activity.

The System 201 is provided with a complete software package to manage files, set up terminal operations, and transmit messages/files to the terminals.

To request access, an individual keys in an ID number and places his finger on the INPUT PLATEN of the terminal. The fingerprint is scanned, and the unique characteristics or minutiae are automatically extracted, converted to digital information, and compared to the reference file associated with the ID number that has been entered. The MATCHER section of the terminal receives both these files and completes the comparison. If both files represent the same fingerprint, the access terminal displays "ID VERIFIED" and initiates positive action such as opening a door or bank vault.

Personal Touch Verification. With FINX 401, the CRT terminal uses its own microprocessor to perform matching and extraction, so the terminal itself performs both verification and ID enrollment. As an online terminal, the 401 provides standard interfaces to most computer and data networks. Block, protected, line, character, or full-screen transmission are supported.

When power is turned on, the FINX 401 comes up in verification mode. In this mode, only the Automatic Personal-Touch Verification and Control (APVC) subsection of the terminal is capable of limited communication with the host computer. The APVC transmits a request for a particular operator's data file corresponding to the ID number entered via the terminal keyboard. The reference file is received from the host and buffered for the MATCHER program of the APVC. To complete the verification process, the operator must place his finger on the INPUT PLATEN. The matching is performed, and, of the identification is verified, the message "ID VERIFIED" will appear on the CRT screen. When this happens, the connection between the terminal and the host computer is completed and the operator can then make full use of the CRT terminal.

After completion of a set of operator tasks, a set time interval, or a defined period of inactivity, the host computer can send a command to the terminal which will cause the FINX 401 to go into verification mode. An authorized security officer can go through a verification process which places the terminal in a mode which permits enrollment of new individuals and other security functions.

PALMPRINT IDENTIFICATION CONTROL

Palmguard Inc. is selling an access control system that uses palmprints as the identifier. The user enters an ID number on a keyboard and places his right hand in a jig on the palmprint reader. The jig controls the placement of the spaces between the thumb and index finger and the ring and little fingers.
The terminal reads the palmprint and compares it to the data stored for the ID number entered. As a result of the comparison, five possible steps may be performed:

1. The door will be opened.
2. Information is not conclusive, so the user will be asked to put his hand back into the jig.
3. A second match attempt is successful.
4. The match will fail for the second time, so entry is rejected.
5. Entry of three invalid ID numbers will cause an alarm to sound.

Access can be limited to particular work shifts or days of the week. Each access is logged. Lighted prompt messages guide the user through the access process. By use of a special key and acceptance of his own palmprint, the security officer can place the terminal in a mode to accept new palmprints into the system. The basic system can store 256 palmprints. The vendor claims a very low identification error rate.

SIGNATURE VERIFICATION CONTROL

Based on concepts developed by SRI International (formerly Stanford Research Institute), SYCON Inc. is manufacturing two signature verification products, the SD-10 Signature Verifier Terminal and the DT20 Signature Verifier Pad. Both devices use signature dynamics to verify identity. This method measures pressure, velocity, acceleration, total signing time, number of pen ups-and-downs, and other selected parameters to identify signatures.
While no one person signs his name exactly the same way every time, certain parameters for each individual are consistently similar. By analyzing signatures over a period of time, these fixed traits can be identified for each individual.
Significantly, less than 1% of the population does not have a repetitive dynamic pattern.
The devices can be used to control physical access to an area, access to a computer system or to control financial transactions, such as through use of automated teller machines. Enrollment procedure requires two authorized people. The enrollee signs several times. Ten to fifteen of the best parameters are automatically selected and become part of a profile stored in a computer or on a magnetic stripe of an identification card.
A user identifies himself to the system by using an encoded plastic card or by keying-in an ID number. A standard ballpoint pen is then used to write a signature in the "signature" window. The signature is compared, using the selected parameters, with the stored profile. Each profile contains 40 bytes of information. If required, communication between the terminal and the host computer may be coded.

Further, the signature profile may be encrypted prior to being written on the magnetic stripe. The signature window paper is automatically advanced after each transaction. An error rate of less than 1.5 percent is reported.
The SD-10 is a self-contained terminal unit with its own display, keyboard, and magnetic card reader. It can perform all data capture, analysis, verification, and enrollment functions. The DT-20 is a verification-only terminal. In most applications it would be used in conjunction with a CRT terminal.

HAND GEOMETRY CONTROL
Stellar Systems offers an access control system that uses hand geometry to identify and authenticate users. The user inserts a magnetic card in the reader or enters an identification number. He then places his hand on the reader. If the geometry of his hand matches, he will be given access.
In its simplest version, the system consists of a single reader and encoder. It is used in conjunction with a magnetic card that contains the individual's hand geometry data and identification number.
The encoder is used to enroll an individual on the system. It measures the individual's hand and records the data on a magnetic card.
More sophisticated systems that can handle a number of terminals are available. These store hand geometry data at a central controller or host computer site and can provide an interface to other access control devices. Access can be controlled by individual and location. A printer provides a permanent record of all activity.

EYE BLOOD VESSEL CONTROL
There are other physical characteristics than those described above which might be utilized for access control. There has long been research in voice recognition, which has occasionally been used for identification in legal proceedings.
Another approach is based on the uniqueness of the human eye. There is a great variety of blood vessels in the eye and some characteristics, such as their positions, remain unchanged throughout life. They cannot be altered or eliminated.
Medical research going back at least to 1935 indicates that it is a mathematical certainty that no two retinal formations are identical.
Not displayed at the CSI Conference, but described in a recent issue of Computer Decisions, is the EyeDentifier, a device based on recognition of eye blood vessels. The developer is a small firm in Portland, Oregon, called Eyedentify, Inc. A working prototype of this machine has been undergoing final testing and was to be tried at a local bank.

Controle

Een discussie die in vakkringen steeds meer aandacht begint te krijgen is de kennis die een accountant dient te hebben met betrekking tot de automatisering om zijn/haar functie adequaat te kunnen vervullen. De heer C. Judson Howard Jr. gaat in het artikel "EDP-izing the Internal Audit Staff" in the Internal Auditor/april 1982 in op de kennis die een intern accountant behoort te hebben.
Dient de extern accountant deze kennis ook te hebben?
Als bijdrage aan de discussie zijn delen van het artikel hieronder opgenomen. Centraal in het artikel staat dat

AUDITORS NEED TO ACQUIRE KNOWLEDGE IN FIVE AREAS TO COMPETENTLY INTERACT WITH THE DATA PROCESSING ENVIRONMENT ON THE POSTIMPLEMENTATION LEVEL

Computers in their many and varied forms are all around us. One would be hard pressed to name an industry that does not employ them in some capacity. Certainly, it is difficult to name a company with a large internal audit staff that does not use computers extensively.
Companies will employ more computers that work faster and require far less manual intervention. Evaluating the controls for these future systems will require that every internal auditor have a basic understanding of computer auditing.
Because not all audits require extensive EDP expertise, it is not practical to tie up technical computer audit experts (typically known as EDP auditors) when a limited EDP knowledge would suffice. Audit management needs a method for attaining a staff level of data processing knowledge that can be utilized in performing nontechnical EDP reviews.
Currently, EDP proficiency exists in a normal audit department on two levels.
On one level, the EDP auditors are technically competent computer professionals. They can communicate in EDP terminology, independently review and appraise EDP systems, write, test, and run those computer programs that the audit department requires.
On the other level are the non-EDP auditors. These individuals typically perform financial, operational, and/or field audits that do not require EDP expertise. They can neither program nor read programs and are generally not EDP oriented.
There are two levels of EDP audits typically performed. On a technical level are the audits of the computer operation and its environment. This includes the operating system, tape/disk management, hardware and data security, job accounting, and physical security. It is not reasonable that an auditor without an EDP background of at least moderate depth perform these audits. These technical audits are the exclusive realm of the EDP audit specialist.

On the other level is the application environment. Here are the audits of the controls that exist within application systems (i.e., payroll and billing). These controls cover data input, interpretation, manipulation, alteration, and output.
Application system reviews may be broken down into preimplementation (undergoing development) and postimplementation (actively operating) reviews. Preimplementation reviews generally require an active, long-term involvement on the part of the auditor. They also require a high degree of EDP communication as the auditor interacts directly with data processing personnel. EDP audit specialists should be directly involved in preimplementation audits.
Postimplementation reviews are examinations of active information systems to ensure that they are performing specific tasks as intended and with adequate controls. All internal auditors should be able to perform these audits.
A program to attain the required levels of EDP competence includes five areas. The auditors need to acquire knowledge in these areas to competently interact with the data processing environment on the postimplementation level.

1. Hardware.
The auditor must be taught to recognize the purpose of the various pieces of hardware (CPU, I/O devices, etc.) that are in use at the computer installation. A tour of the facility is beneficial and provides a familiarity that takes away the mystique of the environment. The auditor is able to associate a mental image and physical purpose with a piece of hardware when that piece is referenced during an audit.

2. Operating system, tape-management system, etc.
The auditor should be taught the basic purpose and functions of the various major elements of operating systems' software that make up the processing environment.

This training should be as nontechnical as possible. This will permit a general understanding of how the operating systems controls affect overall security and control of application systems and production data files.

3. Computerese.
While an ability to program is unnecessary, the ability to communicate with programmers is essential. This requires a recognition and understanding of programming terms, program organization, and common elements of computer language. A basic communication course should include the following:
- Basic program structure for the languages most frequently encountered by the auditors.
- Basic programming terms including those terms and acronyms that are typical to the local environment.
- An introduction and general familiarization with the various manuals available that auditors may use for reference when unfamiliar terms or concepts are encountered.

4. Flowcharts.
Auditors must be instructed in reading and interpreting systems and program flowcharts. This ability will prove invaluable for their understanding and determining control points.

5. Computer controls.
Finally, auditors must be taught the fundamentals of control in application programs. Reference material is available in the form of textbooks and professional publications.
While these five steps provide an internal audit staff that is functionally trained to engage in EDP, there are three more that are necessary to ensure that the training is not wasted.
Motivation. Audit-department management must motivate auditors to utilize their news skills by requiring that they review information systems supporting the area being audited. Audit management should review documentation for proof of the review and sufficiency of findings. Good reviews should be recognized and encouraged.
Continuation. Refresher training should be regular and mandatory for all staff auditors (other than EDP audit specialists). The objectives are to keep skills fresh, to update information that may be of use, and to emphasize the importance placed by management upon the EDP aspects of the audits.
Indoctrination. All new staff additions should receive basic EDP training as part of their indoctrination into the internal audit department.

Summary

Internal audit managements need staffs that can audit all aspects of the operation under review. They must, therefore, be committed to providing the necessary training so that staffs can acquire and use the skills required in the EDP environment. The result will be a fully qualified staff that can perform complete audits and render informed opinions and recommendations. EDP-izing the internal audit staff, thus, creates an effective team of EDP audit generalists and specialists.

ONDERWIJS

Zomer 1982

CURSUS ON-LINE DATA ENTRY IN DE BATCH-OMGEVING

door H. Sliedrecht

Inleiding

Medio 1980 vond in aanwezigheid van vertegenwoordigers van tal van KKC-kantoren de proefpresentatie plaats van de eerste in KMG-verband ontwikkelde cursus. Het lag in de bedoeling dat het materiaal van deze cursus door zo veel mogelijk KMG-leden zou worden gebruikt voor het geven van interne en mogelijk ook externe cursussen.

Door KKC zijn vanuit het daar gepresenteerde materiaal een tweetal cursussen ontwikkeld:

1. Kleinschalige Automatisering die inmiddels zowel intern als in Vera-verband wordt gebruikt.
2. On-line data entry in de batch-omgeving die in het najaar van 1981 als interne cursus is gepresenteerd en met ingang van 1982 ook is opgenomen in de brochure Externe cursussen van KKC.

Over de cursus Kleinschalige Automatisering verscheen reeds eerder een bijdrage in Compact, zodat deze bijdrage zich kan beperken tot On-line data entry in de Batch-omgeving een wat lange naam die echter de beste weergave vormt van de casussituatie die in deze cursus wordt behandeld.

In het interne opleidingsprogramma van KKC dient de cursus als vervanging voor de aloude Batch-module waarvan de casus voor wat de automatiseringsomgeving betreft, steeds minder aansloot met de praktijk van de tachtiger jaren.

Doel van de cursus

De cursus heeft tot doel om de cursisten kennis bij te brengen om

- de kwaliteit van de interne controle van een (ten dele) geautomatiseerd systeem van gegevensverwerking te kunnen beoordelen;
- de accountantscontrole, al dan niet met behulp van de computer, op basis van het verrichte systeemonderzoek doelmatig te kunnen aanpakken.

Zoals reeds uit de doelstelling duidelijk zal zijn moeten de toekomstige cursisten vooral worden gezocht onder hen die werkzaam zijn in de interne en externe accountantscontrole. Enige basiskennis op het gebied van automatisering en op het gebied van accountantscontrole is wel vereist.

Inhoud en wijze van kennisoverdracht

Aan de hand van een casus van een verkoop-/debiteurensysteem, waarbij gebruik wordt gemaakt van geautomatiseerde verwerking met behulp van on-line data entry en batch-verwerking, worden de volgende onderwerpen behandeld:

- begrijpen en beoordelen van een systeemontwerp;
- evalueren van het effect op de interne controle van de voorgestelde geautomatiseerde toepassing;
- het doen van aanbevelingen om leemten in de interne controle op te heffen;
- het onderkennen van foutgebieden die bij geautomatiseerde gegevensverwerking in deze vorm kunnen ontstaan;
- de aanpak van de accountantscontrole en het onderkennen van de mogelijkheden tot gebruik van de computer daarbij.

De cursisten moeten in kleine groepen een aantal opdrachten uitwerken die daarna uitgebreid worden besproken aan de hand van voorbeelden van uitwerking. De opdrachten worden afgewisseld met inleidingen over automatisering en controle als aanvulling op de aanwezige kennis en ter ondersteuning van de uitvoering van de opdrachten.

Naast drie theoretische dagen wordt een aparte praktijkdag gegeven. De cursisten gaan dan zelfstandig aan het werk met een audit-pakket en zien ook de resultaten van hun werk terug in de vorm van computeroutput op basis van de door hen geschreven instructies.

Voorstudie en cursusduur

De behandelde casus bevat onder meer vrij uitgebreide documentatie over een verkoop-/debiteurensysteem, die vooraf ter bestudering wordt toegestuurd. Tevens moet vooraf reeds een opdracht worden uitgevoerd. De benodigde voorstudietijd bedraagt circa 8 uur. De cursus zelf duurt inclusief de praktijkdag 4 dagen.

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