N. Ten Wolde.

compact

COMPUTER EN ACCOUNTANT

Klynveld Kraayenhof & co
ACCOUNTANTS

NUMMER 14 5E JAARGANG ZOMER 1978

compact

VAN DE REDACTIE

In dit nummer vindt U van de hand van Ackermans het artikel "De accountant en het computerservicebureau", terwijl De Jong en Neisingh het "gebruik van de computer" voor de beveiliging van computerprogramma's door middel van het bibliotheeksysteem PANEXEC bespreken.
Tot voor kort bestonden deze systemen slechts ter beveiliging van bronprogramma's tegen verlies, onrechtmatige inzage en wijziging en dergelijke. Voorbeelden hiervan waren de pakketten LIBRARIAN en PANVALET.
PANEXEC richt zich op het beheer en de beveiliging van objectprogramma's (dit is in machinetaal) en laadbare programma's.
In de beschrijving van PANEXEC is vertaling van "technische termen" achterwege gelaten, omdat wij meenden dat dit de leesbaarheid niet ten goede zou komen.

Dat gebruikte terminologie toch dikwijls de leesbaarheid van artikelen kan aantasten, blijkt uit "Lezers reageren": de redactie blijft echter vertrouwen op het doorzettingsvermogen van de lezers om de draad van het betoog te kunnen volgen.

De vaste rubrieken Computergebruik in de accountantscontrole, A.B.C.-Nieuws en Literatuuroverzicht vindt U ook in dit nummer.

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

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

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

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

Adres: Pr. Irenestraat 59 Amsterdam

DE ACCOUNTANT EN HET COMPUTERSERVICEBUREAU

door S.J.M. Ackermans

Bij de inschakeling van een computerservicebureau door een onderneming voor de verwerking van de gegevens dient door de accountant van de vennootschap aan de verwerking van de volgende aspecten aandacht te worden geschonken:

I Heeft de vennootschap in voldoende mate aandacht geschonken aan de keuze van het servicebureau, de voorbereiding van de uitbesteding, de invoering ervan en de follow-up.

II Welke zijn de invloeden van het uitbesteden op de administratieve organisatie en de interne controle van de onderneming.

III Welke zijn de invloeden voor de accountant op de door hem uit te voeren werkzaamheden in het kader van de controle van de jaarrekening.

Bij een nadere uitwerking van de hierboven genoemde aspecten zal aandacht geschonken dienen te worden aan de wijze waarop gebruik wordt gemaakt van de diensten van het servicebureau. De volgende mogelijkheden zijn hierbij te onderkennen:

1. De onderneming huurt computertijd bij het servicecentrum.
2. De onderneming maakt gebruik van het personeel van het servicebureau voor het verzorgen van alle gegevensverwerkingsfuncties.
3. De onderneming maakt gebruik van - door het servicebureau gemaakte - standaardpakketten.
4. De onderneming maakt gebruik van door het servicebureau speciaal voor hem ontworpen programma's, welke voldoen aan de specifieke eisen die de onderneming heeft gesteld.

In de eerste twee mogelijkheden zijn weinig elementen te herkennen die afwijken van de situatie waarin de cliënt een eigen computercentrum installeert. De verdere beschouwingen zijn dan ook met name van toepassing in de situatie zoals beschreven in de mogelijkheden 3 en 4.

Factoren met betrekking tot de keuze van het computerservicebureau

Hierna volgt een opsomming van een aantal factoren die een rol kunnen spelen bij de bepaling van de keuze van het servicebureau.

1. Reputatie van het centrum. Hierbij valt onder meer te denken aan de financiële positie van het centrum, de kwaliteit en de tijdige en correcte uitvoering van het werk, de mate waarin de werkelijke kosten van uitbesteding overeenkomen met hetgeen door het bureau werd geoffreerd.
   Hierbij kan mogelijk gebruik gemaakt worden van ervaringen van andere gebruikers; tevens kan eventueel een indruk worden verkregen van de omvang van de activiteiten van het servicebureau in het specifieke toepassingsgebied.
2. Welke ervaringen zijn er met betrekking tot soortgelijke problemen.

3. De beschikbaarheid van eventuele standaardpakketten.

4. De controle-inzichten en controletoepassingen in het computercentrum. Hierbij valt onder meer te denken aan de kwaliteit van de interne organisatie, zoals functie- en taakverdelingen, de maatregelen ter voorkoming van calamiteiten, de maateregelen ter verzekering van geheimhouding, de maatregelen voor de beveiliging van programma's en gegevensverzamelingen en de mogelijkheden van eventuele reconstructie van gegevensverzamelingen.

5. De bereidheid tot samenwerking ter zake van controleproblemen met de accountant van de onderneming en het toelaten van deze accountant voor een onderzoek.

6. Welke is de gebruikte apparatuur en welke uitwijkmogelijkheden zijn er in geval van calamiteiten. Zijn deze voldoende gezien in het kader van de aard en de wijze van de te verwerken gegevens van de onderneming. In dit kader is ook van belang het beoordelen van de mogelijkheden van het servicebureau om te voldoen aan eventuele toekomstige vereisten.

7. Hoe ligt de vestigingsplaats van het servicebureau ten opzichte van de plaats(en) van vestiging van de onderneming.

8. Hoe is de kwaliteit van de offerte en hoe verhouden de prijzen zich met andere offertes.

9. Wat is de inhoud van het modelcontract en welke zijn de algemene voorwaarden.
   Aan de mogelijke contractbepalingen zal hier verder geen aandacht worden geschonken.

Van belang is verder de aanwezigheid van een goede documentatie, zowel bij het servicebureau als bij de vennootschap.
De cliënt dient in elk geval te beschikken over: Probleembeschrijving en mogelijkheden van het systeem, systeem-flowcharts, record-indelingen en layout van overzichten, programma-listings, programma-flowcharts, operators-instructies, systeemconfiguratie, programmeertaal en conversieplan.
Bovendien dient de cliënt te beschikken over documentatie omtrent: Procedures voor input-voorbereiding en controle op input, correctieprocedures, procedures voor controle op output en distributie van output.

Heeft de vennootschap in voldoende mate aandacht geschonken aan de voorbereiding van de uitbesteding, de invoering ervan en de follow-up

De hieronder opgesomde punten kunnen voor de accountant als een leidraad dienen bij het onderzoek naar de haalbaarheid om bij de automatisering van de gegevensverwerking door de vennootschap gebruik te maken van de diensten van een computerservicebureau.
Bedacht dient te worden, dat eventuele adviezen van de accountant aan de leiding slechts zinvol kunnen zijn, als deze tijdig worden gegeven, dus vóór de invoering van de uitbesteding.

De volgende aspecten dienen onder meer in aanmerking te worden genomen:

1. Is de leiding voldoende bij het administratieve gebeuren betrokken en in staat aan organisatorische veranderingen leiding te geven.
2. Wat is de kwaliteit van de huidige organisatie en haar werkwijze.
3. Zijn de mogelijkheden tot mechanisering en automatisering in eigen beheer voldoende bezien.
4. Is het redelijkerwijze mogelijk, dat de organisatie op een tijdig moment juiste en volledige invoer aanlevert, zodat op tijd over goede computeroverzichten kan worden beschikt.
5. Is de personeelssituatie gunstig wat betreft kennisniveau, ervaring en inzet.
6. Zijn de huidige procedures in detail beschreven en kritisch geanalyseerd.
7. Welke functies en taken worden door de uitbesteding beïnvloed en op welke wijze.
8. In hoeverre zijn veranderingen in het interne controlesysteem vereist, onder andere voor samenvoeging van voorheen elkaar controlerende administraties.
9. Zijn de controle- en correctieprocedures ten aanzien van invoerverzorging en de computeruitvoer voldoende uitgewerkt en vastgelegd in instructies.
10. Zijn er aangepaste of nieuwe procedures voor beveiliging van informatie en is aan het aspect van de mogelijkheid tot reconstructie aandacht geschonken.
11. Is er een draaiboek opgesteld waarin de voorbereiding, invoering en follow-up worden gebaseerd en in detail gepland. Is er voorzien in een goede voortgangscontrole.
12. Is er een plan voor uitvoering en controle van de conversiewerkzaamheden.
13. Zijn er criteria opgesteld voor de evaluatie van het systeem en de werking ervan.

De werkzaamheden - zoals een accountant die uitvoert- gericht op de controle van de jaarrekening van een vennootschap worden in zeer belangrijke mate beïnvloed door de aanwezige administratieve organisatie en interne controle bij de vennootschap. Uit dien hoofde zal het onderdeel: "Welke zijn de invloeden van het uitbesteden op de administratieve organisatie en de interne controle van de onderneming",
en het onderdeel: "Welke zijn de invloeden voor de accountant op de door hem uit te voeren werkzaamheden in het kader van de controle van de jaarrekening" verder in combinatie met elkaar bezien worden.

Gehele of gedeeltelijke uitbesteding van de verwerking van gegevens met betrekking tot de financiële administratie heeft geen invloed op de verantwoordelijkheid van de accountant ten aanzien van de verklaring bij de jaarrekening. Dit betekent, dat de accountant bij zijn oordeelsvorming over de kwaliteit van de organisatie, de wijze moet betrekken waarop uitbestede taken zijn georganiseerd en worden vervuld. De evaluatie van deze aspecten verschilt niet van de evaluatie van andere interne controle-aspecten en dient dan ook een wezenlijk onderdeel van de evaluatie van het gehele systeen van administratieve organisatie en interne controle te zijn.

De accountant zal bij de beoordeling van de controle-aspecten tevens dienen te betrekken de vraag in hoeverre het "Reviewen" van de controles bij het servicecentrum noodzakelijk is. Van belang hierbij is:

1. Het belang van de toepassing voor de financiële administratie.
2. Het oordeel van de accountant met betrekking tot de in punt I genoemde onderwerpen. Hierbij dien aan de aspecten - zoals beschreven - aandacht te worden besteed.
3. Komen in voldoende mate controleerbare vastleggingen beschikbaar en is hierbij de "audit-trail" van grootboekvastlegging tot brondocument en andersom gewaarborgd.
4. Zijn er voldoende totaalgegevens beschikbaar ter afstemming met controleregisters betreffende periodieke verwerking en volledigheid van de daarbij gebruikte bestanden.
   Ten aanzien van het vastleggen van controletellingen geldt, dat de noodzaak hiertoe in versterkte mate aanwezig is, omdat door het transport van gegevens extra aandacht dient te worden gegeven aan de controle op de volledige verwerking van gegevens. Het verdient de voorkeur om - indien mogelijk - de aansluitingen tussen controletotalen en de van het servicebureau terugontvangen output te laten uitvoeren door een functionaris, die niet belast is met het opmaken van de brondocumenten of andere gegevens welke naar het servicebureau gezonden zullen worden.

Naarmate de kennis over de verwerking van de gegevens bij het servicebureau belangrijker wordt bij de verkrijging van het eindoordeel zal de noodzaak gaan bestaan om het servicecentrum te bezoeken ten einde door directe waarneming tot een oordeel te komen over de organisatie aldaar. Niet meer kan worden volstaan met - zoals het geval was bij de beoordeling van de keuze van het computerservicebureau - de bestudering van de aanwezige documentatie.

Beoordeling van de controlemaatregelen op het computerservicebureau

De controlemaatregelen kunnen ingedeeld worden in:

A. Algemene controles: Controles die betrekking hebben op het gehele proces van gegevensverwerking.

B. Specifieke controles: Controles met betrekking tot de specifieke toepassingen.

A. Algemene controles

1. De administratieve organisatie.

2. Hardware-controles. Dit zijn ingebouwde controles waarover de machine van het computerservicecentrum beschikt. Bij de beoordeling hiervan kan de accountant eventueel gebruik maken van een lijst waarop de computer aangeeft welke hardware-fouten zich hebben voorgedaan. De accountant kan dan tevens een inzicht krijgen in de organisatie en de procedures van het centrum met betrekking tot het corrigeren van deze fouten.

3. Beveiligingsmaatregelen. Ten einde de programma's, gegevens, output van de gebruikers te verzekeren kunnen onder meer de volgende maatregelen worden genomen:

   - Toegangscontrole tot het centrum.
   - Het gebruik van codes in plaats van gedetailleerde beschrijvingen.
   - Verwerking confidentiële gegevens in aanwezigheid van employés van de gebruiker.
   - Het opbergen van documenten, output en bestanden, wanneer deze niet in gebruik zijn, in afgesloten ruimten.

4. Controles met betrekking tot gegevens en programma's. Hierbij valt onder andere te denken aan de aanwezigheid van een computerveiligheidsplan en een noodvoorzieningenplan. De accountant zal de inhoud hiervan dienen te beoordelen. Daarnaast is het noodzakelijk dat de accountant de organisatie rondom het wijzigen van stambestanden nauwkeurig beoordeelt en dat periodiek door het servicebureau de inhoud en de mutaties op de belangrijke bestanden wordt gegeven.

5. Controles met betrekking tot programmaveranderingen. Hierbij dient in beschouwing te worden genomen de autorisatieprocedure van programmawijzigingen, de documentatie van deze veranderingen en de aanwezige testprocedures.

B. Controles met betrekking tot de specifieke toepassingen

Controles welke gericht zijn op juistheid en volledigheid, zoals:

- Totalencontroles.
- Volgordecontroles.
- Gebruik van controlecijfers (check digits).
- Controle op volledigheid en juistheid van onder andere velden, labels, codes en combinaties van gegevens.
- Redelijkheidscontroles.

De accountant zal de noodzakelijke kennis verkrijgen door - naast zoals reeds eerder opgemerkt het bestuderen van de documentatie - het afnemen van interviews van het personeel van de onderneming en het servicecentrum. Vervolgens zal het steekproefsgewijze volgen van een aantal posten vanaf de eerste vastlegging tot de definitieve verwerking bijdragen tot het vergroten van de kennis van de opzet en de werking van het gehele systeem.

Na de aldus verkregen kennis over het systeem zal de accountant zich een oordeel willen vormen over de werking hiervan door middel van het testen van het systeem. Indien een duidelijke audit trail aanwezig is, kan de accountant dit doen door het checken van de brondocumenten met controlerapporten, foutlijsten, transactie-overzichten en rapporten aan het management.
Dit betekent in een aantal gevallen - met name bij batchgewijze verwerking van de gegevens - dat er geen verschil bestaat met de wijze van testen van een systeem waarbij geen computer gebruikt wordt.

Een andere manier van het testen van het systeem is het invoeren van "testgevallen". Hiermee kan de programmatuur getest worden; de aspecten van interne controle dienen hierbij dan nog betrokken te worden. Voor de mogelijkheden en de risico's met betrekking tot deze vorm van testen verwijs ik naar de artikelenserie van A.W. Neisingh: "Het gebruik van de computer in de accountantscontrole", zoals deze is verschenen in voorgaande uitgaven van Compact. Hierbij is ook aandacht geschonken aan het gebruik door de accountant van computercontroleprogramma's. De accountant zal nu - na het uitvoeren van de beschreven werkzaamheden - in staat dienen te zijn de kwaliteit van de administratieve organisatie en interne controle te evalueren en te beoordelen.
Ten einde te vermijden dat door verschillende accountants iedere keer weer de organisatie en de interne controle van een servicebureau moet worden onderzocht, is er een ontwikkeling gaande waarbij een onafhankelijke accountant het onderzoek verricht en hierover rapporteert aan de leiding van het computerservicebureau.
In dit rapport dient opgenomen te zijn:

- De omvang van het onderzoek waarbij begrepen een beschrijving van de uitgevoerde testwerkzaamheden en de resultaten hiervan.
- Een beschrijving van het systeem, inclusief de aanwezige interne controleprocedures.
- De periode waarover het onderzoek heeft plaatsgevonden.
- Een oordeel over het systeem.
- Een oordeelsonthouding met betrekking tot de controles ter zake van de specifieke toepassingen van cliënten van het computerservicebureau.
- Opmerkingen met betrekking tot onbevredigende situaties en aanbevelingen ten einde deze te verbeteren.

De accountant van de cliënt kan het rapport van de "derde" accountant ten behoeve van zijn onderzoek gebruiken. Daarnaast kan hij het controleprogramma en het dossier van de andere accountant raadplegen indien hij dit noodzakelijk vindt.
De accountant van een cliënt van het servicebureau die gebruik maakt van het rapport van de "andere" accountant blijft echter verantwoordelijk voor de evaluatie van de interne controle van het totale systeem van verwerking van de gegevens van de cliënt, zodat de mate waarin hij gebruik wil maken van dit rapport door hem zelf bepaald dient te worden.

Het artikel "Karakterisering van de autorisatieproblematiek" door H. Roos doet bij mij een paar overwegingen opborrelen, die ik U gaarne meedeel.

Het komt vaak in sterk gespecialiseerde vakgebieden voor, dat het woordgebruik in de eigen vaktaal zeer specifieke betekenissen krijgt. Wanneer de specialist dan die specifieke betekenis als algemene betekenis gaat definiëren, ontstaat een spraakverwarring, die de specialist zeker niet heeft bedoeld, maar die de buitenstaander voor raadsels plaatst. Ik mag bij wijze van voorbeeld de vele betekenisverschuivingen noemen, die de sociologen in onze taal hebben gebracht en waarvan de omdraaiing van de betekenis van het woord motiveren de eerste was.

Daar moest ik aan denken bij de definitie van het begrip "autorisatie", die in dit artikel gegeven wordt. Daar staat: (kort samengevat) autorisatie is controle.
Dit nu kan niet juist zijn, tenzij we ons allemaal gaan aanpassen aan een specifiek taalgebruik.
Dit taalgebruik is waarschijnlijk op de volgende manier in de wereld gekomen:

Om bepaalde handelingen met data base gegevens te kunnen verrichten, moet men aantonen daartoe geautoriseerd te zijn, dit wil zeggen gemachtigd te zijn uit hoofde van functionele bevoegdheid.
Men kan dit echter niet aantonen door de computer een boterbriefje te laten zien en daarom is de idee ontstaan om in het systeem zelf vast te leggen welke functie bepaalde handelingen mag verrichten en bovendien te zorgen dat het systeem geblokkeerd is wanneer een andere functie zodanige handeling zou willen verrichten.
Waar Roos over spreekt is dus geen autorisatiesysteem, maar een systeem van controle op (on)geautoriseerd handelen. Het systeem stelt vast of men geautoriseerd is. Dit is niet hetzelfde als autorisatie.
In paragraaf 4 wordt dan ook terecht gesproken van autorisatiecontrole.
Is het dan niet beter door dit hele artikel heen (óók in de titel) voor "autorisatie" te lezen "autorisatiecontrole", dus ook "autorisatiecontrolesysteem", enz.?

In alle bescheidenheid denk ik dat gewone mensen er dan iets meer van zouden begrijpen en dat zou dit artikel, naar zijn inhoud gemeten, verdienen.

J.W. Pon

Reacties van de hand van H. Roos

1. Hetgeen de heer Pon opmerkt over het begrip autorisatie is zonder meer terecht. Juist in verband met data base toepassingen, of anders gezegd het toepassen van data bases is een zo zuiver mogelijk taalgebruik van essentieel belang. In het onderhavige geval betreft het een algemeen begrip als autorisatie. In een concrete situatie doet zich dit probleem echter voor bij de naamgeving en het definiëren van alle "objecten" waarover gegevens in de data base kunnen worden opgenomen. "Objecten" zeer ruim genomen, zodat daar ook immateriële zaken

onder vallen. De lezer zal opvallen, dat ook hier weer een onzuiver gebruik van een woord dreigt.
De reden van het min of meer forceren van betekenisveranderingen moet waarschijnlijk worden gezocht in de noodzaak waarvoor men (bijvoorbeeld de specialist) zich geplaatst ziet een "nieuw" verschijnsel van een naam te voorzien. Hiervoor kiest men dan een bestaand woord met een min of meer verwante betekenis en definieert vervolgens wat men in het kader van een mededeling met dat woord bedoelt. Eigenlijk het procédé dat ik ook heb toegepast.
Uit de opmerkingen van Pon blijkt, dat dit niet altijd nodig is. Ik zal ze dan ook zeker ter harte nemen.

2. Een fraai voorbeeld van begripsverwarring door onzuiver woordgebruik is de reactie van Bron in Compact nr. 13, voorjaar 1978, op het opstel van Gerritsen.
In dat geval gaat het echter niet om een bestaand woord waaraan een andere betekenis is gegeven, doch om een nieuw woord waarmee een nieuw begrip wordt aangeduid: het woord "data base".
Bij het gebruiken van het woord data base dient men zich af te vragen of men een "ding" bedoelt of een "begrip".
Door verschillende schrijvers is getracht dit onderscheid aan te geven door de term "fysieke data base" te gebruiken voor het "ding" en voor het "niet-ding" de term "logische data base" te reserveren.
In een praktische situatie zijn er echter meer dan twee verschijningsniveaus van een data base te onderkennen. Aldus wordt men genoodzaakt de term "logische data base" te gebruiken om verschillende zaken aan te duiden. Of dit niet reeds voldoende verwarring zaait, gebruikt Bron ook nog de constructie "gegevensverzamelingen die 'logisch' van elkaar gescheiden worden opgeslagen zijn conventionele gegevensbestanden". Hij bedoelt waarschijnlijk "fysiek" gescheiden opgeslagen.
Waarom hij juist "logisch" gebruikt in dit verband vindt, als ik mij niet vergis, zijn oorzaak in het feit dat hij hier een onderscheid wil maken tussen fysieke gegevensstructuren van eenvoudige en van gecompliceerde aard. Bij zo'n gecompliceerde gegevensstructuur worden gegevens over verschillende typen objecten op "fysieke" wijze gekoppeld, omdat ze voor één of meer toepassingen met elkaar verband houden. Met de nadruk op "fysiek". Het verband als zodanig is echter wel degelijk logisch van aard. Ziedaar de verwarring.
Hier is misschien alleen uit te komen door het begrip data base te reserveren voor het denken en praten over informatie- en communicatiesystemen in conceptuele zin, dit wil zeggen zonder daarbij te denken aan de technische realisatie.
De nadruk komt dan te liggen op het in hun verband met de activiteiten van de organisatie beschouwen van de informatie. Daarbij moeten informatiebegrippen die elkaar dekken met dezelfde term worden aangeduid en eenduidig worden gedefinieerd.
Of men een langs deze lijnen gedefinieerd informatie- en communicatiesysteem ("systeem" wegens de directe relatie met de organisatie en de bedrijfsprocessen) al dan niet automatiseert en of, zo men automatiseert, daarbij gebruik zal worden gemaakt van speciale standaardprogrammatuur is een technisch geaard probleem.
Wanneer men het begrip data base aldus interpreteert, hebben Gerritsen noch Bron het bij het rechte eind.

PANEXEC

door A.R. de Jong en A.W. Neisingh

Algemeen

Panexec is een programmapakket, dat op de markt wordt gebracht door Pansophic Systems Incorporated.
Het pakket is een zogenaamd library-bibliotheekpakket voor "Executable Program Libraries". (Dit zijn laadbare programma's; synoniemen hiervoor zijn: partitioned data sets, load libraries en core image libraries.)
Panexec is te gebruiken op IBM-computers onder de besturingssystemen DOS/VS, OS of OS/VS.
De literatuur, die de basis voor dit artikel vormt, is de brochure PANEXEC concepts and facilities voor auditing and security administration.

Programmabeveiliging

De beveiliging van programma's dient deel uit te maken van het gehele pakket van beveiligingsmaatregelen, dat genomen moet worden bij de automatisering van de gegevensverwerking.
De controlerend accountant dient bij zijn onderzoek naar de organisatie van de automatisering onder meer aandacht te besteden aan de maatregelen van beveiliging van operationele programmatuur.
Programmabeveiliging kan worden onderscheiden in:

1. de beveiliging van bronprogramma's,
2. de beveiliging van laadbare programma's.

Het belang van een georganiseerde beveiliging van bronprogramma's werd reeds vele jaren geleden onderkend. Hiervoor werden toen bibliotheekpakketten ontwikkeld, zoals Panvalet en Librarian.
De beveiliging van laadbare programma's werd echter niet in deze pakketten geregeld; zij waren zoals vermeld geheel gericht op de bewaring en beveiliging van bronprogramma's.
Laadbare programma's worden op dit moment voornamelijk beveiligd door een daaromheen gecreëerde organisatie, dat wil zeggen door toepassing van handmatige procedures. De bezwaren, die aan dergelijke procedures zijn verbonden, zijn alom bekend, zoals:

- de mogelijkheid van menselijke fouten is altijd aanwezig;
- de controleprocedures worden niet altijd strikt uitgevoerd;
- in een handmatig proces zijn grote hoeveelheden gegevens moeilijk te verzamelen;
- de papiermassa kan zo groot worden, dat ze redelijkerwijs niet meer toegankelijk is.

Het complexer en omvangrijker worden van de computersystemen had tot gevolg, dat de roep om beveiligingsmethoden op het niveau van de laadbare programma's, zowel vanuit accountantskringen als vanuit de automatisering zelf, steeds groter werden.

Panexec is ontwikkeld met de bedoeling de beveiliging en beheersbaarheid van bibliotheken van laadbare programma's te verzekeren.
De programma's worden zowel in object als in laadbare vorm opgenomen in een centrale bibliotheek.

De belangrijkste mogelijkheden respectievelijk eigenschappen die het pakket biedt, zijn naar de mening van de leverancier:

1. De beschikbaarheid van een "sophisticated, multi-level password security system" ten behoeve van de beveiliging van de programmatuur op meerdere niveaus. (Zie hierna A.)
2. Een set utilities voor het beheer van de bibliotheek. (Zie B.)
3. De aanwezigheid van een report generator faciliteit (Easytrieve), die gegevens uit de Panexec-bibliotheek kan selecteren en verwerken.
4. Efficiënte opslag- en toegangstechnieken.
5. Onafhankelijk van opslagmedium en operating system.

Panexec-faciliteiten

A. Beveiliging programmabibliotheek

Een beveiliging van de programmabibliotheek kan worden bereikt door het invoeren van één of meer van de hierna te nemen beveiligingsmaatregelen:

1. Een password-beveiligingssysteem van maximaal vijf niveaus.
2. Het limiteren van het gebruik van kritische bibliotheekbeheerfuncties (zoals het verwijderen van modules en dergelijke) door middel van beveiligingscodes.
3. Het beschermen van produktieprogrammatuur tegen ongeautoriseerde wijzigingen en dergelijke door niet toegelaten plaatsing in een produktiestatus.
4. Het signaleren op de console van ongeautoriseerde benadering van de bibliotheek.
5. Het gebruik maken van de zogenaamde Security Administrator Control Code ten behoeve van het beheer van passwords en beveiligingscodes.

Toelichting op enige punten:

ad 1. In het password-systeem zijn vijf niveaus te onderkennen, te weten:

- Bibliotheekniveau (FAC = File Access Code)
  Deze code blokkeert de toegang tot de gehele bibliotheek. Gebruik van deze code is slechts doelmatig, indien het slechts enkele functionarissen is toegestaan de file te gebruiken.
- Groepniveau (GAC = Group Access Code)
  De programma's kunnen worden ingedeeld in groepen per functie, afdeling of andere logische eenheid. Aan dergelijke groepen kan een GAC worden toegekend.
- Elementniveau (EAC = Element Access Code)
  Programma's binnen een hiervoor genoemde groep kunnen worden beveiligd door een EAC. Alle versies van deze programmatuur worden vervolgens beschermd tegen ongeautoriseerde toegang.

- Element lezen (ERC = Element Read Code)
  Een programma kan met een ERC worden beveiligd tegen kennisname ervan. Hiermede kan worden bereikt, dat bijvoorbeeld kritische programma's niet ongeoorloofd worden verwerkt.
- Element schrijven (EWC = Element Write Code)
  Door gebruik van deze code kan het wijzigen van een programma slechts worden toegestaan aan hen, die daartoe gerechtigd zijn.

De beveiligingscode blijft aanwezig, ook in geval de library wordt gedumpt op (meerdere) archiefbestanden ten behoeve van back up en dergelijke.

ad 2. Programma's in de "produktiestatus" zijn door het bibliotheeksysteem beveiligd tegen modificeren of renamen.
Belangrijke informatie met betrekking tot het gebruik van de programmatuur worden automatisch verzameld gedurende de aanwezigheid van het programma in de bibliotheek. (Zoals datum laatste wijziging, datum laatste maal verwerkt.)

ad 3. Met behulp van de Security Administrator Control Code kunnen passwords en beveiligingscodes worden opgeroepen en gemodificeerd.
(N.B.: De passwords en de beveiligingscodes zijn vercijferd, zodat met behulp van een IBM dump utility geen kennis kan worden verkregen van passwords en dergelijke.)

B. Beheer van de bibliotheek

Ten behoeve van het beheer van de bibliotheek en de controle op het gebruik van de programmering en het onderhoud van programmatuur zijn gegevens benodigd over de programma's opgenomen in de bibliotheek. Panexec houdt ten behoeve van het beheer en met betrekking tot het gebruik van de bibliotheek meer dan 150 gegevens bij over de in de bibliotheek opgenomen laadbare programma's, alsmede zijn eigen activiteiten. Deze gegevens omvatten vier categorieën, te weten:

1. Library audit
   Van het gebruik van de bibliotheek wordt een informatiebestand bijgehouden, waarin voornamelijk statistische gegevens worden opgenomen, zoals het aantal elementen in de bibliotheek, het gebruik van de library (toegewezen aantal tracks, gebruikte tracks, tracks benodigd voor de directory, enz.) en "last date when inactive elements were removed to a protection file".

2. Library management
   Deze functie heeft betrekking op:
   - het onderhouden van back-up-bestanden,
   - het toewijzen van schijfruimte,
   - het verwijderen van niet meer benodigde programma's,
   - het kunnen restoren van een programma, zodra dat nodig is.

Panexec houdt de gegevens bij, die deze functie nodig heeft voor de uitvoering van zijn taak (zoals: Data set name, Volume serial number, datum en tijdstip van vervaardigen van de laatste twee back-up-bestanden; datum en tijd, waarop de laatste reorganisatie heeft plaatsgevonden, enz.).

3. Program information

Deze gegevens worden voornamelijk bijgehouden voor het onderhouden ter ondersteuning van de programmeurs bij het plegen van programma-onderhoudswerkzaamheden.
De gegevens, welke bijgehouden worden, zijn onder meer versienummer, status, namen van object-modules, datum en tijd van de meest recente wijziging, geheugenbeslag van het programma, enz.
Panexec heeft tevens de mogelijkheid een cross reference te vervaardigen van een laadbaar programma naar de corresponderende object- en source-programma's, die op PANVALET zijn opgenomen.

4. Management report generation

De opgebouwde gegevens kunnen naar allerlei gezichtspunten worden verzameld en afgedrukt, eventueel nadat bewerkingen op deze gegevens zijn uitgevoerd. Hiertoe zijn diverse Easytrieve-programma's in het Panexec-systeem opgenomen.
Daarnaast zijn in het Panexec-systeem reeds een aantal Easytrieve-routines opgenomen ten behoeve van het evalueren van gegevens en het verstrekken van informatie aan de functionarissen, die betrokken zijn bij het beheer van de bibliotheek.

C. Back-up- en recovery-maatregelen

Maatregelen ten behoeve van back-up en recovery zijn in het systeem opgenomen en eenvoudig uit te voeren.
De gegevens van de laatste twee back-up-bestanden (datum, tijd, tapenummer en data set name) worden op de Panexec-file opgenomen.
Het restoren van programma's kan selectief geschieden.

D. Het laten vervallen van programma's

Het verwijderen van programma's is een beheerfunctie. De uitvoeringsopdrachten ten behoeve van deze functie kunnen door een beveiligingscode worden beschermd tegen ongeautoriseerd gebruik.
De programma's kunnen door de voor die programma's verantwoordelijke personen van een indicatie worden voorzien, ten teken dat het programma kan worden verwijderd.
Periodiek kunnen de geïndiceerde programma's dan door de functionaris, verantwoordelijk voor het beheer van de bibliotheek worden verwijderd en op een beschermd bestand (inactive elements) dan wel op een back-up-bestand (disabled programs) worden geplaatst.

De te verwijderen programma's zijn derhalve te onderscheiden in niet-actieve programma's en vervallen verklaarde programma's.
Niet-actieve programma's zijn programma's, die niet direct nodig zijn, dan wel een lage verwerkingsfrequentie hebben en derhalve in de toekomst benodigd kunnen zijn.
Panexec registreert de datum waarop het programma voor de laatste keer is uitgevoerd.
Vervallen programma's zijn programma's, die nooit meer benodigd zullen zijn (bijvoorbeeld nieuwe programmaversie is aanwezig).
De verwijdering van de programma's geschiedt dus voor beide categorieën op een andere wijze. Dit ter beveiliging van de programma's tegen eventuele vergissingen bij de verwijdering van de programma's.

De uit de bibliotheek verwijderde niet-actieve programma's worden samengevoegd met andere reeds op een beschermd bestand vastgelegde programmatuur, zodat er een bestand niet-actieve programma's ontstaat waaruit met een eenvoudige opdracht een programma dat benodigd is kan worden opgehaald.

Vervallen programma's kunnen elke periode naar een back-up-bestand worden overgebracht, waarbij de back-up van de vorige periode wordt overschreven. Wil men uit oogpunt van beveiliging meerdere generaties bewaren, dan zullen bestanden uit verschillende perioden bewaard moeten worden. Dit is uiteraard mogelijk.

E. Panvalet interface

Een interface met een Panvalet Library is aanwezig, zodat een cross-reference tussen laadbare en source-programma's niet handmatig behoeft te worden bijgehouden.

De linkage editor voegt aan het laadbare programma onder meer de volgende (Panvalet-)gegevens toe:

1. source-naam,
2. status van het source-programma,
3. versienummer van het source-programma,
4. datum van de laatste wijziging in het source-programma.

Panexec heeft hierdoor gegevens beschikbaar omtrent het bronprogramma dat ten grondslag ligt aan het laadbare programma.
Indien de source-programma's niet van een Panvalet Library komen, bestaat de mogelijkheid gegevens door middel van een opdracht aan de programma's toe te voegen.
Of programma's in de laadbare bibliotheek langs geautoriseerde weg zijn opgenomen c.q. gewijzigd kan op deze wijze worden vastgesteld.

COMPUTERTOEPASSINGEN TEN BEHOEVE VAN DE ACCOUNTANTSCONTROLE

CA/EARL-toepassingen in samenwerking met Hurdman and Cranstoun

door A. Kamstra

Inleiding

In het kader van de samenwerking met Hurdman and Cranstoun heeft de A.C.-groep voor dit Amerikaans accountantskantoor ten behoeve van een Europese vestiging van een Amerikaans industrieel bedrijf enig A.C.-werk verricht. Een gedeelte van deze werkzaamheden bestond uit het uitwerken en programmeren van een door de EDP auditor van H + C geschreven wensenlijst.
De controlerend accountant heeft deze wensenlijst formeel goedgekeurd. Deze oorspronkelijke wensenlijst heeft tijdens het uitwerken en testen van de programmatuur forse wijzigingen ondergaan. Hierbij dient opgemerkt te worden, dat dit voor alle betrokkenen een nieuwe cliënt was, waardoor specifieke bedrijfskennis ontbrak.

Ontwikkeling van de toepassingen

Bij de wensenlijst was documentatie van de cliënt gevoegd betreffende de bij de controle te betrekken systemen. De omvang daarvan heeft ons extra tijd gekost, veelal ook doordat niet-relevante gegevens bestudeerd moesten worden voordat dit niet-relevant zijn vastgesteld kon worden.
Het belangrijkste gebrek aan de wensenlijst was, dat allerlei details ontbraken. Met name wensen met betrekking tot de af te drukken gegevens (rubrieken uit de bestanden) en de op te bouwen tellingen.

COBOL versus CA/EARL (IS/08)

In één van de volgende Compact-nummers zal ingegaan worden op de keuzecriteria tussen COBOL, CA/EARL en AUDITAPE.
Bij deze toepassing is oorspronkelijk voor COBOL gekozen omdat hiermee beter kon worden voldaan aan bepaalde layout-behoefte (dit is opmaak van de uitvoer in gedrukte vorm) van de gebruiker. Echter in de loop van de ontwikkeling en de diverse contacten bleek, dat de programmatuur zeker het eerste jaar forse wijzigingen zou ondergaan.
Als oorzaken kunnen onder meer worden genoemd:

- het betrof een nieuwe cliënt,
- de controlerend accountant bleek onervaren in het gebruik van de computer bij de controle,
- de verstrekte documentatie was niet altijd voldoende duidelijk.

In overleg met alle betrokkenen is dan ook overgegaan op het gebruik van CA/EARL, waarbij bleek, dat de gewenste layout ook bij gebruik van CA/EARL voor de controlerend accountant weinig bezwaren zou opleveren. Het voordeel van CA/EARL-programma's is, dat de programmeertijd belangrijk korter is en tevens zijn CA/EARL-programma's in de meeste gevallen aanmerkelijk sneller en eenvoudiger te wijzigen dan COBOL-programma's. Voorts is het testen met produktiebestanden bij gebruik van CA/EARL een acceptabeler methode dan bij gebruik van COBOL.

Problemen bij het testen van de programmatuur

Zoals veelal het geval is, bleken de meeste moeilijkheden bij het testen (in dit geval tevens proefproduktie) naar voren te komen. Genoemd kunnen worden:

- Computertijd was niet altijd beschikbaar. Steeds meer worden wij geconfronteerd met installaties, die een zodanig hoge bezettingsgraad hebben, dat wij er slechts op enkele dagen in de maand terecht kunnen. In dit geval konden wij er ook wel eens om zes uur 's morgens terecht. (Waarvan noodgedwongen gebruik is gemaakt.)
- Uit de registratie van de cliënt bleek niet altijd te kunnen worden afgeleid welke bestanden of versies van bestanden gebruikt moesten worden. In een aantal gevallen moest empirisch worden bepaald wat het juiste bestand was. (Door middel van aansluiting van controletotalen.)
- De verstrekte documentatie was niet altijd juist.
- Het aansluiten van totalen was soms een tijdrovend karwei.

Naast verkeerde interpretaties aan de zijde van de A.C.-groep en de altijd voorkomende programmeerfouten had het bovenstaande tot gevolg, dat de hele ontwikkeling een forse inspanning heeft vereist, hoewel de programma's op zich niet bovenmatig ingewikkeld waren.

Overzicht van de toepassingen

Gewenst werd de volgende informatie per systeem:

Accounts Payable (crediteuren)

- Totalen per valutacode.
- Een steekproef op de openstaande saldi.
- Selectie van posten op grond van specifieke criteria.

Inventory (voorraden)

- Totalen naar verschillende inzichten zowel voor de hoeveelheden als de waarde.
- Selectie van posten met specifieke kenmerken.
- Selectie van verouderde beschadigde goederen op grond van bepaalde codes.

Accounts Receivable (debiteuren)

- Selectie ten behoeve van saldobiljetten via de guldenrangnummermethode, met de bijbehorende tellingen. De geselecteerde posten werden op een lijst afgedrukt, de saldobiljetten werden van deze lijst gewoon overgetypt. Deze procedure lijkt omslachtig, maar is bij geringe hoeveelheden meestal goedkoper dan het ontwikkelen van een door de computer af te drukken saldobiljet met de daaraan verbonden extra programmeringskosten.
- Aging (rangschikking naar ouderdom, onder andere ouder dan 30, 60, 90 dagen). In bepaalde gevallen bleek, dat als vervaldatum een jaartal later dan 1980 was ingevuld!

- Een lijst van creditposten.
- Totalen per valutacode.
- Een lijst van posten met afwijkende inhoud (onder andere datum fout en jaar vóór 1975 en ná 1975).

Property (vaste activa)

- Tellingen per soort eigendommen.
- Selectie van posten ten behoeve van controle op de aanwezigheid.
- Nacalculatie van de afschrijvingen.
- Selectie van posten met een negatieve boekwaarde.
- Selectie van posten waarop niet wordt afgeschreven.

Sales (verkopen)

- Selectie van posten met een grote afwijking tussen boekingsdatum en afleveringsdatum.
- Totalen van de verkopen.

Slot

De samenwerking van de A.C.-groep en de controlestaf is in dit geval duidelijk anders geweest dan in een Nederlandse situatie het geval zou zijn. De formele scheiding tussen een EDP-auditor en een controlerend accountant, de moeilijke bereikbaarheid van de eerste (standplaats New York) en de volledig nieuwe cliënt zijn de voornaamste oorzaken geweest van de in dit geval ontstane problemen. Het voorkomen van deze problemen is iets waar uiteraard voortdurend naar gestreefd wordt. Echter het ontwikkelen van geautomatiseerde systemen en dus ook van accountantscontroleprogrammatuur gaat bijna altijd gepaard met enige aanloopmoeilijkheden.

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

door B.M. de Vries

Aanslag op privacy door fouten in computerprogramma's

Vele computerprogramma's zijn en blijven behept met fouten. Door de snelle toename van het aantal computers, zijn ook de fouten die ermee worden begaan, in aantal gegroeid. De consequenties daarvan, die onder meer betrekking hebben op de privacy, zijn onaanvaardbaar. Dit geldt niet alleen voor de manager bij een grote bank, of de gespecialiseerde wiskundige, maar ook voor iedereen die geregistreerd staat bij een postgiro, bank, hypotheekgever, overheid en dergelijke.
Aldus prof. dr. I.S. Herschberg, in zijn inaugurele rede als hoogleraar in de informatica aan de Technische Hogeschool Delft.

In fouten die met computerprogramma's worden gemaakt, zijn twee soorten te onderscheiden. In de eerste plaats fouten die ontstaan omdat niet ondubbelzinnig vastligt wat het programma moet doen. In vakjargon heet dit onvoldoende specificatie. Daarnaast zijn er fouten die ontstaan omdat er bij de programmering iets misgaat. Een derde soort fout, die wordt veroorzaakt door mankementen aan de computerapparatuur, laat prof. Herschberg buiten beschouwing. Deze komen volgens hem zelden voor, terwijl de systemen zo zijn opgebouwd, dat zij vrijwel altijd alarm slaan als zich zo'n fout voordoet.

Programmeringsfouten

Om fouten in het programmeren op te sporen worden de programma's van tevoren getetst en net zo lang gewijzigd, tot de programma's ogenschijnlijk naar behoren werken. Een nadeel van het testen is, dat het wel de aanwezigheid van fouten kan aantonen, maar nooit de afwezigheid daarvan kan bewijzen. Testen alleen, is dus onvoldoende. Bovendien vindt prof. dr. Herschberg testen een verspilling van machinetijd en intellect en brengt het zijns inziens de testende programmeur vaak tot wanhoop. Volgens prof. Herschberg gaat de testende programmeur in zijn wanhoop daardoor geloven in onverklaarbare duistere machten, die het op hem en zijn programma hebben gemunt. Het gebeurt dan dat er te hooi en te gras wordt gewijzigd zonder enige systematiek en meestal op die plaatsen van het programma, waarvan duidelijk zou moeten zijn dat ze niets met de fout te maken kunnen hebben. De programmeur weet vaak letterlijk niet meer waar hij het zoeken moet. "Wij hebben", aldus prof. Herschberg, "slecht geprogrammeerd, we hebben met name het doel van onze programma's vaak slecht geformuleerd en we zijn maar al te vaak gevangen in een testpraktijk die verkwistend is."

De onbetrouwbare programma's opereren op iedere gegevensverzameling, iedereen is wel eens ergens geregistreerd en dan nog vaak op verschillende plaatsen tegelijk. Daardoor is volgens prof. Herschberg eigenlijk iedereen een gebruiker. Al deze gebruikers worden bedroevend slecht bediend. De leveranciers kunnen door fouten de veiligheid niet garanderen, dat wil zeggen, niet voorkomen dat onbevoegden kennis nemen van de gegevens en programma's van anderen. Door programmafouten is het ook niet mogelijk te garanderen, dat alleen bevoegden de persoonsgegevens raadplegen.

De programmeur wordt zo het slachtoffer van een ingewikkeldheid die hij niet meer kan overzien en de gebruiker wordt in zijn val meegesleept. Onder deze omstandigheden wordt privacy, zelfs als men allerwege de beste bedoelingen veronderstelt, een dubieuze zaak. Men bewijst in feite lippendienst aan de beschermende persoonlijke levenssfeer zonder zelfs maar te kunnen garanderen dat aan de eisen van de wet en reglement is voldaan.

Als oplossing tegen het hierboven geschetste kwaad stelt prof. Herschberg een defensieve stijl van programmeren voor, te vergelijken met het defensief autorijden. In feite bedoelt prof. Herschberg daarmee niets nieuws, maar een consequente toepassing van alle bekende methoden en middelen om bij het programmeren het maken van fouten te voorkomen. Verdeel en heers is daarbij een belangrijk uitgangspunt. Ontleed elk ingewikkeld probleem net zo lang in iets minder ingewikkelde stukken, tot ieders probleem afzonderlijk en overzichtelijk is. Ook binnen zo'n deelprogramma moet men nooit meer dan één doel tegelijkertijd zien te bereiken. Het bereiken van een eventueel iets snellere doorgangstijd is daaraan volgens prof. Herschberg ondergeschikt.

De correctheid van ieder programma-onderdeel moet dan nog worden bewezen. Onder de geboden, die de defensieve programmeur verder in acht moet nemen, vindt men volgens prof. Herschberg allerlei bepalingen van een vrijwillig reglement van orde. Hij moet zich verplichten tot een ruim gebruik van commentaar, zonder daarbij in breedsprakigheid te vervallen. De defensief programmerende programmeur documenteert zijn programma voor zijn afnemer en voor zichzelf volledig maar bondig, hij geeft verslag van het aantal weinige testen, die om schrijffoutjes te verwijderen misschien nodig zijn en dergelijke, kortom hij moet zijn programma ordelijk en gewetensvol beheren, gelijk een goed huisvader betaamt. De defensieve programmeur neemt daarnaast aldus prof. Herschberg één gebod in acht: "hij bezwijkt niet voor de verleiding van trucage, hij mijdt, hij schuwt elke poging zijn taal, dialect of machine te bewegen tot oneigenlijk gebruik. Zijn programma's bevatten geen woordspelingen, geen dubbelzinnige constructies, die zijn afgestemd op zijn dialect of zijn machine, geen bespeling van de barokke eigenschappen van zijn instrument. Noch gebrek aan kennis, noch gebrek aan esprit staan het gebruik van trucages in de weg, alleen zijn defensieve houding legt hem deze beperking op".

Prof. Herschberg besloot zijn rede door op de volgende wijze zowel de programmeur als de gebruiker duidelijk te maken hoe zij uit de ban van hun fout kunnen worden bevrijd, waarmee zij nu zijn geslagen: "En gij allen in mijn gehoor, zowel programmeurs als gebruikers" - en gebruikers zijt gij allen - ik zou u willen toeroepen, al was het alleen maar in het belang van de bescherming van uw persoonlijke levenssfeer, past deze werkwijzen toe of bevordert hun toepassing. De werkwijzen zijn beschikbaar, de utopie kan een feit zijn: "zo gij het wilt, is het geen sprookje".

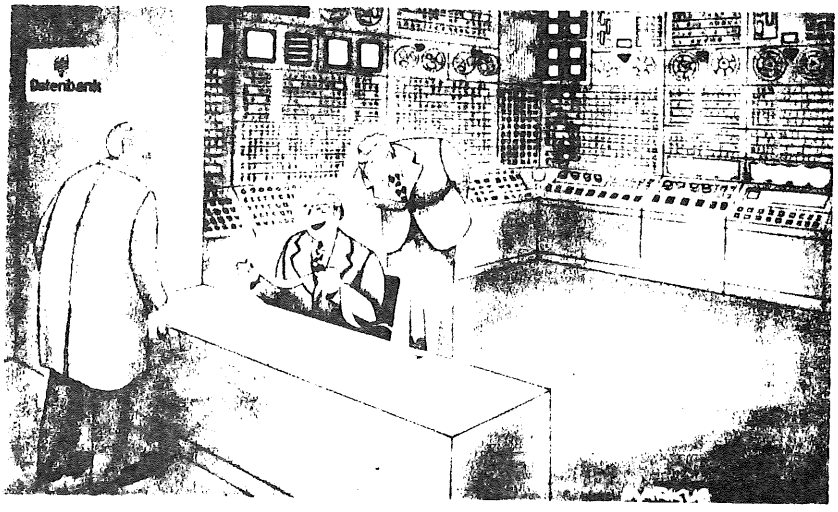
De Automatiseringsgids, 6 april 1978

Het privacy-probleem nader bekeken

Auskunftsersuchen

Wie einer Meldung des Westdeutschen Rundfunks zu entnehmen war, betrat kurz nach Beginn des neuen Jahrs ein leicht angeheiterter jüngerer Mann die Räumlichkeiten der Polizeiwache einer mittleren Stadt im Westen Deutschlands. Er lallte etwas von Datenschutzgesetz und verlangte Auskunft, ob personenbezogene Daten über ihn bei der Polizei gespeichert seien.

Das System wurde fündig. Der Bildschirm von INTERPOL wies nämlich einen Haftbefehl aus. (Im übrigen kein Aprilscherz, sondern wahr.)



"Aber natürlich treiben wir mit Ihren persönlichen Daten keinen Missbrauch, Sie altes Ferkel, Sie!"

Datenschutzberater, nr. 2, 1978

Waarom computerfraudes in zo geringe mate door bedrijven gesignaleerd worden?

"... A gunman walks into a bank and pulls off a $ 10,000 robbery and the bank officials have no hesitation about calling in the police. Nobody blames the bank for the robbery. But a slick white collar criminal manipulates that same bank's computers and steals $ 500,000-and all too often the bank officials have nothing to say. They would rather absorb the loss than call in the police. They are fearful of the bad publicity. It is one thing to be robbed at gunpoint. All of us can sympathize with the victim in that kind of crime. But to be tricked by a crooked computer expert is to admit vulnerability and a weak set of controls-and, under those circumstances, it is human nature to wish to avoid the embarrassment.

Citaat Senator Abe Ribicoff's (Democraat Conn. U.S.A.) in Computer Security, nr. 22, mei/juni 1978

Senator A. Ribicoff is van plan een wet tegen computermisbruik uit te vaardigen, zoals blijkt uit een artikel in de New York Times d.d. 23 juni 1978:

Computer Crime Assailed

Washington, June 21 (AP) - Federal law enforcement officials called today for speedy passage of legislation aimed at stopping criminals who steal millions of dollars each year by using computers.
The bill, written by Senator Abraham A. Ribicoff, Democrat of Connecticut, is intended to fill a gap in the Federal criminal code by catching up with the electronic era. It would impose prison terms of up to 15 years and fines up to $50,000 for criminal misuse of a computer. It also would prohibit the theft, destruction or fraudulent use of data from computers owned or used by the Government.
The legislation was endorsed by John C. Keeney, Acting Assistant Attorney General in charge of the criminal division, and by Joseph F. Henehan, chief of the Federal Bureau of Investigation's white-collar crimes section.
Senator Joseph R. Biden Jr., Democrat of Delaware, chairman of a judiciary subcommittee holding hearings on the Ribicoff bill, said that computer crime was causing an annual loss of $ 100 million and was growing rapidly.

Wat te doen om microfilm tegen waterschade te beschermen?

In Edpacs van februari 1978 lazen wij het volgende:

Recovery of microfilm from water damage

The 1977 Johnstown flood damaged the records of numerous businesses. Many of the valuable records of several banks and an electric utility were salvaged because they had been put on microfilm.
Eastman Kodak provided free reclamation service for its customers. They suggest that anyone who must recover water-soaked microfilm should follow these guidelines:

- Keep the film wet at all times after its first exposure to water. For example, put the film in clean garbage cans and fill them with clean water.
- Do not attempt to remove the film from its original package.
- Cover the garbage cans and ship them immediately to the nearest commercial microfilm processing center.

At the center, the film will be washed, dried, and put into new boxes. It is then returned to its owner ready for use.
Remember, once the film gets wet, keep it that way.

De oplossing van Burroughs voor het probleem van het vervalsen van bankcheques

Zelfbeschermde cheques van Burroughs

Ook het vervalsen van bankcheques neemt hand over hand toe. Met de vergevorderde techniek van het kleur-kopiëren, zo stelt Burroughs, is het zelfs mogelijk dat er vervalsing wordt toegepast door bankemployees, die ongestoord een aanslag op iemands rekening zouden kunnen plegen zonder dat daar direct enige vorm van controle aan vooraf gaat.
Burroughs heeft een bankcheque ontworpen die onzichtbaar voor het oog het woord "ongeldig" draagt, dat zichtbaar wordt op een kopie of andere reproduktie. Voor de zekerheid verschijnt het woord in drie talen.

De Automatiseringsgids, nr. 15, 1 juni 1978

Euronet-tarieven zijn aangekondigd

Provisional tariffs have now been announced for the Euronet packet-switched network being implemented by European PTT's on behalf of the EEC.
The most significant feature of the proposed tariffs, which will not be altered by more than 10% before the service becomes operational next year, is that they are distant independent. This means that the cost will be the same whether a user is accessing a data base in London or Italy.

Three elements will make up the cost of using Euronet: a usage charge, an annual rental and a connection charge.
The usage charge will be £1.15 per thousand 64 byte data segments, plus a duration charge depending on the data rate. Those working at up to 1200 bps via the public network will pay £1.35 an hour, and via private line £1.00 an hour. The private circuit rate rises to £1.35 an hour for transmission at up to 9600 bps, and to £3.60 for transmission at 48 Kbps.
Over the dial-up network, the Datel service will be used, requiring payment for the call to the London packet-switching exchange, £25 for installation of the modem and £20 a year rental. Rates for private circuits range from £300 for a 300 bps link to £ 3,000 for a 48 Kbps link.

Euronet initially will be a private network providing Europe-wide access to data bases held on computers installed all over the EEC. The intention is to expand it to the point where it becomes an international data communication facility, interfacing with national networks. Italy has considered making its own national packet-switched network an extension of Euronet.
The technology for the switches is microprocessor-based, and was first developed for the French Transpac network. It consists of a complex of Intel 8010 microcomputers, and the switches are controlled by French SEMS Mitra 125 minicomputers (CW, August 25, 1977).
As exclusively revealed in Computer Weekly, the switching technology is under consideration for the Post Office's successor to EPSS (CW, July 21, 1977).

Informatie (f)

Met Secure kunnen zowel "batch" als "TSO" bestanden worden beveiligd

The European Software Company heeft aan haar leveringsprogramma van door het Amerikaanse Boole & Babbage ontwikkelde pakketten een systeem voor gegevensbeveiliging toegevoegd. Met behulp van dit zogeheten "Secure" pakket kan het IBM-verificatiesysteem binnen de besturingssystemen OS, VS en MVS worden vervangen. Hiermee kunnen dan bestanden, vastgelegd op schijf of magneetband, voor zowel groepsgewijze gegevensverwerking als bestanden gebruikt voor interactieve toepassing (TSO = time sharing option) worden beveiligd.
De operateur of timesharing-gebruiker wordt niet betrokken bij de beveiligingsprocedure: bij de opzet van Secure wordt er namelijk van uitgegaan dat slechts één persoon verantwoordelijk is voor de beveiliging, de zogeheten Security Manager. Toegang tot bepaalde gegevensgroepen kan verder worden toegekend aan bepaalde stukken programmatuur. Het aantal benaderingspogingen kan worden beperkt of alleen worden toegestaan binnen een bepaalde tijdsduur. Zowel de geslaagde als de mislukte benaderingspogingen kunnen worden vastgelegd. Via diverse aaneengeschakelde verwerkingseenheden kan het bestand, waarin de bevoegdheidsleutels zijn vastgelegd - de zogenaamde "Security Data" - worden benaderd.

Computable, 23 juni 1978

Computer Audit Tests of Employee Benefit Records = $5,436 Recovery

An audit of employee benefits disclosed that the company was paying medical benefit premiums for 15 former employees. This was uncovered by matching the social security numbers of terminated employees in the Personnel Department's master file of current employees.
Premium overpayments of $5,436 were deducted from the next payment to the insurance carrier. Moreover, improved procedures were initiated for notifying Employee Benefits of terminations.

Computer Tape Management System Evaluation

An audit was performed on the Computer Tape Management System (CTMS) to evaluate its effectiveness in controlling tape utilization and storage. A physical inventory disclosed that approximately one-third (4,200) of the data processing tapes were not listed in the CTMS and approximately one-fourth (3,600) of open shop tapes within control of CTMS were either obsolete of duplicate tapes. The Data Processing Department took action to improve the effectiveness of CTMS and was able to avoid ordering $10,000 in new tapes by reusing the obsolete and duplicate tapes.

Nieuwe versie van CA-EARL

CA-EARL, versie 2.2

Het aantal mogelijkheden dat deze snelle en eenvoudig te gebruiken report generator de gebruiker biedt, werd door CA regelmatig uitgebreid. Met de nieuwste versie is CA-EARL nu dermate flexibel geworden, dat het in een doorsnee commercieel rekencentrum tot aan 90% van alle rapporten kan verzorgen.

De in september uitgebrachte versie 2.2 van CA-EARL bevat onder meer de volgende uitbreidingen:

a. Alle versies van het DL/1 Data Base systeem zijn nu toegankelijk door middel van een interface-routine, waarmee de gebruiker de noodzakelijke bewerkingsparameters kan ingeven.

b. Door middel van een meegeleverde interface is nu ook VSAM (Virtual Storage Access Method) support beschikbaar.

c. Het drukken van zelfklevende etiketten, voorbedrukte formulieren, enz. is nu mogelijk.

d. Door middel van een "print exit" kan de gebruiker, indien gewenst, bepaalde routines voor verwerking van de afzonderlijke regels zelf schrijven, hetgeen bijvoorbeeld nuttig kan zijn voor overdracht op microfilm en dergelijke.

CA LINK, oktober 1977

Inmiddels is de bovengenoemde DL/1 interface door de A.C.-kern beproefd op een IMS data base, draaiend onder OS/VS2.
Met deze interface kan de IMS data base op segmentniveau in grote lijnen op twee manieren worden benaderd, namelijk:

1. met een zogenaamd "unqualified segment search argument"; dit wil zeggen, dat er geen sleutelgegevens beschikbaar gesteld worden. Alle segmenten in de data base kunnen fysiek sequentieel worden doorlopen. Selectie kan met behulp van het EARL Select Statement plaatsvinden.
2. met een zogenaamd "qualified segment search argument"; dit wil zeggen, dat er een sleutelgegeven moet worden gedefinieerd. Op grond van deze sleutel worden de gegevens direct uit de data base geselecteerd.

LITERATUUROVERZICHT

door B.M. de Vries

In de A.C.-bibliotheek opgenomen boeken

AC 167 Data security aspecten van data base toepassingen - Werkgroep data security van de Nederlandse IMS-GUIDE 1978 (6)

Het rapport bevat het resultaat van het werk van twee van de drie subgroepen, te weten de autorisatie-subgroep en de integrity-subgroep.
De kern van het rapport bestaat uit de hoofdstukken 3, 4 en 5, achtereenvolgens gewijd aan:

- autorisatie,
- integriteitsaspecten,
- praktijkgevallen.

Hoofdstuk 3 is onderverdeeld in drie secties. De eerste sectie bevat een algemene benadering van de autorisatieproblematiek (waarover reeds in Compact een artikel werd opgenomen), de tweede een aantal met IMS-gebruik samenhangende softwaretechnieken en de derde een aantal bijzondere onderwerpen.

In hoofdstuk 4 worden de volgende integriteitsaspecten behandeld: recovery-factoren, detectie van transmissiefouten en de detectie van data base fouten.

Door middel van dit rapport wordt een raamwerk van security-aspecten voor een data base toepassing gegeven, waarbij het accent ligt op de autorisatie- en integriteitsaspecten.

AC 168 Auditor's study and evaluation of internal control in EDP systems - Lilly e.a. (Engels, 67 blz.) 1977

Het zogenaamde "Lilly-rapport" heeft ten doel de accountant ten aanzien van het onderzoek en de evaluatie van de interne controle van geautomatiseerde systemen enige richtlijnen te verschaffen. De hoofddoelstellingen worden als volgt in het rapport omschreven:

- To describe and recommend procedures to be performed by an independent auditor (conducting an examination of financial statements) in the auditor's study and evaluation of electronic data processing (EDP) accounting controls as a part of the overall review of the accounting control system. This study and evaluation will be used to determine the nature, timing, and extent of audit procedures to be applied in the examination of financial statements.
- To provide the auditor with information useful for meeting the requirements of Statement on Auditing Standards No. 3, "The Effects of EDP on the Auditor's Study and Evaluation of Internal Control", through illustration and description of various control techniques and related auditing procedures.

- To outline some examples of the typical tests of compliance that can be applied to EDP accounting controls.
- To discuss, in general terms, the possible effect of a weakness in EDP accounting control.

Substantive testing and the use of the computer as an audit tool are not covered in this guide.

AC 171 Management, control and audit of advanced EDP systems - Johnson Task Group AICPA 1978 (Engels, 38 blz.)

Het onderhavige rapport wijst op de zorg van de leiding en van de accountant ten aanzien van de turbulente ontwikkelingen op het gebied van de geautomatiseerde informatieverzorging. De invloed van deze ontwikkeling op de te hanteren controlemiddelen en controletechnieken wordt besproken. Een aantal controlemiddelen worden meer in detail behandeld. Een overzicht van de besproken controlemiddelen en hun doelstellingen wordt weergegeven in de "techniques matrix".
De leesbaarheid en duidelijkheid van het rapport is groot vanwege de toelichtingen in de appendices en vanwege de goede begripsomschrijvingen in de verklarende woordenlijst.

AC 174 Documentation of computer-based systems - British Standards Institution (Engels, 11 blz.) 1978

Het rapport geeft het raamwerk van een documentatiesysteem weer. Dit raamwerk is bedoeld als hulpmiddel om een eigen, op een specifieke situatie toegespitst, documentatiesysteem op te bouwen.

AC 169 Basic computer concepts & control - Cursusboek van AICPA (Engels, 200 blz.) 1977

AC 170 COBOL - Drs. F. Remmen 1977

Dit boek is ontstaan als een poging om het leerproces bij een cursus COBOL niet te laten verstikken door omvangrijke en ondoorzichtige taalspecificaties. Bij experimenten is namelijk gebleken, dat de leerstof het beste beperkt kan blijven tot de essentiële taalelementen. Dit bevordert het opbouwen van een helder taalbegrip. Vanuit dit begrip kan men dan verder voor allerlei details zijn weg vinden in het manual, waarop men is aangewezen voor het verwerken van programma's.
De voor deze syllabus benodigde taalelementen gebaseerd op ANSI-COBOL 1974 zijn in een aparte taalbeschrijving (bijlage 1) opgenomen.

Uit de tijdschriftenliteratuur

The internal audit mandate in EDP - W.E. Perry
C.A. Magazine (September 1977) - S 133

Perry bespreekt het rapport "Systems Auditability and Control" (SAC) van het Institute of Internal Auditors. Een soortgelijk artikel heeft Perry geschreven in Edpacs van maart 1978.
De twee artikelen vullen elkaar grotendeels aan en geven te zamen een goede aanvulling op het SAC-rapport, hetgeen het inzicht in het "hoe" en "waarom" van de EDP-audit ten goede komt.

Volgens Perry bestaat er een discrepantie tussen de technologische ontwikkelingen op automatiseringsgebied en het daarop passende netwerk van controlemiddelen en controletechnieken. De in het SAC-rapport en de in het artikel opgenomen tabel "EDP audit practices" zijn middelen om de bestaande kloof te overbruggen. Helaas zijn over het algemeen deze controletechnieken bij de accountants te weinig bekend. Perry roept op de werkprogramma's van de interne accountant te actualiseren, opdat hij een passend antwoord heeft op het mandaat, dat hij van de directie heeft verkregen.

Perry signaleert bij de accountants een tekort aan automatiseringskennis. Besproken wordt op welke wijze dit probleem valt op te lossen.
Voor wat betreft de aard van de controlewerkzaamheden wordt een verschuiving voorzien van de beoordeling en het toetsen van de verwerkingsresultaten (data files, records en reports) naar de beoordeling en de toetsing van de interne controles, die een blijvende betrouwbaarheid en nauwkeurigheid van de verwerkingsresultaten moeten waarborgen.

Interessant is de door Perry gegeven beschouwing over de onderlinge relaties tussen de drie thans bestaande standaardwerken op het gebied van automatisering en controle, namelijk:

- Control Guidelines and Computer Audit Guidelines (CICA)
- Computer Control & Audit (Mair, Wood and Davis)
- SAC study (IIA).

De CICA-publikaties leggen de nadruk op de relatie tussen interne controle en de daarop afgestemde accountantscontrole.
Computer Control & Audit stelt dat het doel van maatregelen van Interne Controle is een vermindering van risico's en accentueert daarom de rol van de accountant in de systeemontwikkelingsfase en bij de beoordeling van de organisatie van geautomatiseerde infoverwerking en van de geautomatiseerde toepassingen.
Het SAC-rapport geeft de meer feitelijke informatie omtrent de thans bestaande vormen van interne controle- en toetsingstechnieken bij geautomatiseerde gegevensverwerking.

The auditor's role in systems development - A.R.G. Parker
C.A. Magazine (September 1977) - S 134

Vaak zijn accountants niet betrokken bij de ontwikkeling van geautomatiseerde systemen, maar worden zij pas ingeschakeld na installatie van de apparatuur, na gereedkoming van het geautomatiseerde systeem of na het afsluiten van het contract met een servicebureau.

Ingegaan wordt op de volgende aspecten:

- De rol van de accountant:
  - beoordeling van de maatregelen van interne controle in in ontwikkeling zijnde systemen,
  - beoordeling van de "management trail",
  - beoordeling van de juistheid van de toegepaste waarderingsregels (accounting principles),
  - voorzien in een aanvullende link tussen de leiding en het rekencentrum,
  - het volgen van de conversie naar een nieuw geautomatiseerd systeem.
- De ontwikkelingsfasen van een geautomatiseerd systeem en de betrokkenheid van de accountant.
- De gevolgen, die de betrokkenheid van de accountant in de systeemontwikkeling voor de onafhankelijkheid van de accountant met zich meebrengt (collissiegevaar).

Conclusie: Noch de ondernemingsleiding, noch de automatiseringsdeskundigen zijn zich bewust van de belangrijke inbreng, die de accountant tijdens de ontwikkeling van een informatiesysteem kan hebben.

Systems auditability: Friend or foe? - W.E. Perry en H.C. Warner
The Journal of Accountancy (Febr. 1978) - S 142

De behoefte om dit artikel te schrijven vloeit bij Perry en Warner voort uit het feit, dat volgens hen: "Auditing and control procedures for EDP systems have failed to keep pace with the introduction of new technology and new concepts in EDP systems design".
Het begrip "auditability" wordt in dit artikel als volgt aangeduid:
"Auditability reflects the interrelationship between audit and control. The auditability of computer-based information systems refers to the features and characteristics needed to verify the adequacy of controls as well as to verify the accuracy and completeness of data processing results".

"Controls" worden onderscheiden in:

- general controls : gericht op het geheel van EDP-activiteiten,
- application controls: gericht op specifieke toepassingen.

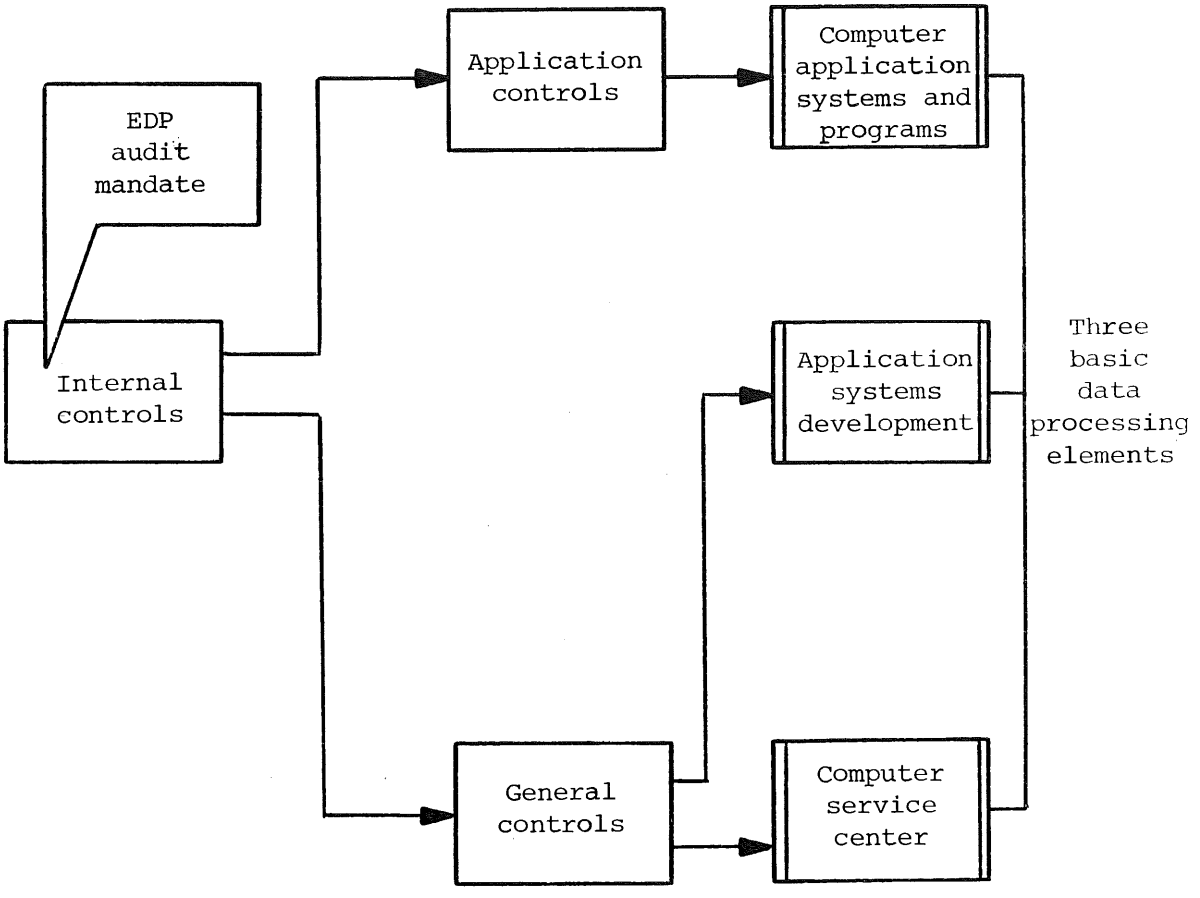
De relaties voor wat betreft interne controle tussen de drie hoofdfuncties van de automatiseringsactiviteiten, te weten:

- computer application systems and programs,
- application systems development,
- computer service center (hardware, personeel, ruimte, algemene procedures),

zijn in onderstaand schema (figuur 1) weergegeven.

Figure 1

Internal control relationship



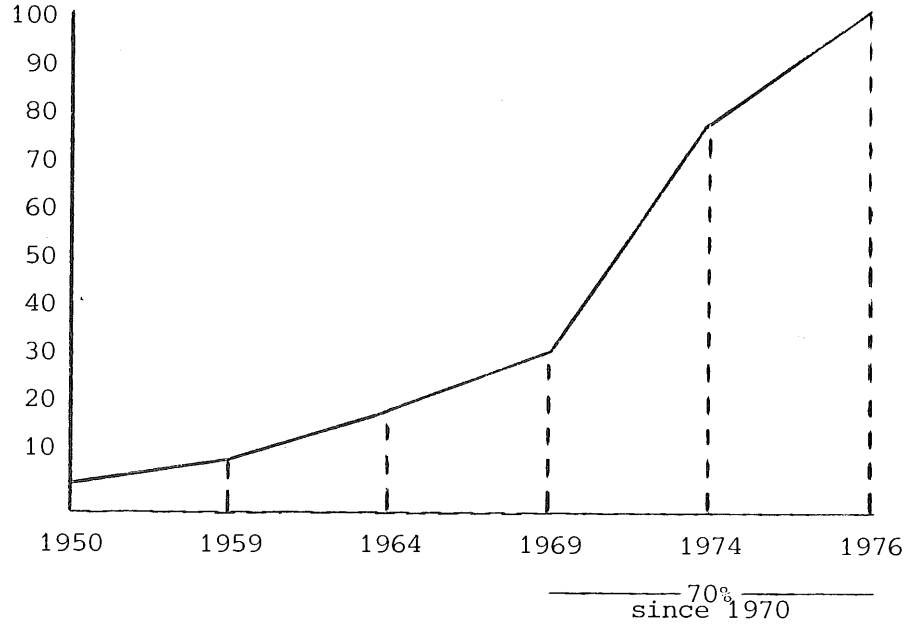
De verantwoordelijkheid voor interne controle lijkt gefragmenteerd te zijn. De toereikendheid van de maatregelen van interne controle in de handmatige fasen in de transactieverwerking behoort tot de verantwoordelijkheid van het betreffende lijnmanagement. De gebruikers zijn daarnaast verantwoordelijk voor het specificeren van de controle-eisen binnen het geautomatiseerde systeem. De leiding van de automatiseringsafdeling is verantwoordelijk voor de ontwikkeling van de systeemtoepassing en het opnemen van voldoende maatregelen van interne controle hierin.
De controles dienen echter geëvalueerd te worden binnen de context van de totale systeemtoepassing en van de controledoelstellingen.
Ten behoeve van de beoordeling van de maatregelen van interne controle in geautomatiseerde systemen vindt de externe accountant ondersteuning in:

- het werk van de interne accountant,
- technieken voor het gebruik van de computer in de controle,
- het identificeren van "control points" binnen het systeem; op deze "control points" toetst de accountant de werking van de interne controle.

Het aandeel van de EDP-auditfunctie binnen het geheel van controle-activiteiten van de interne accountant is volgens het SAC(Systems Auditability and Control)-rapport de laatste jaren sterk toegenomen, hetgeen uit de volgende grafiek blijkt:

Figure 2

Trend in establishing an EDP audit function



Het onderzoek van het Institute of Internal Auditors leidt onder meer tot de volgende conclusies:

- Ten gevolge van de toenemende complexiteit en gebruik van geautomatiseerde informatieverwerkende systemen neemt de behoefte aan EDP-controle toe.
- Er zullen nieuwe hulpmiddelen en technieken ten behoeve van het toetsen van de juistheid en volledigheid van de gegevensverwerking moeten worden ontwikkeld.
- Accountants moeten betrokken worden in de systeemontwikkelingsfase, opdat tijdig het nieuwe geautomatiseerde systeem van voldoende maatregelen van interne controle wordt voorzien.