KPMG Klynveld EDP Audit

Samsom BedrijfsInformatie

COMPACT

KWARTAALBLAD EDP AUDITING

7 x EDP-Auditing en de praktijk

Is EDP-Auditing niet meer dan
het scherpen van een ganzeveer?
Drs. M.A. van Alphen RA / Internatio-Müller nv

Automatiseringsfunctie:
slachtoffer van EDP-auditors?
Drs. F.J.G. Fransen / Neddata bv

EDP-Audit: iets bijzonders?
Drs. P.J.A. Lekkerkerker / Shell Nederland bv

Automatisering - slagader
van het bankbedrijf
Drs. N.J. Krever / Bank Mees & Hope

EDP-Audit: nuttig, zinvol, mogelijk?
J.J.A. Leenaars RA / Robeco Groep

Strafrecht en
computerrelated crime
Mr. Ong Sien Hien / Officier van Justitie
aan het parket Rotterdam

Juridische maatregelen tegen
misbruik van informatie
Prof. mr. H. Franken / Hoogleraar
rechtswetenschap informaticarecht
RU Leiden

SPECIAL

1990

Compact ®
Jaargang 17, special bij nr. 4
Een uitgave van KPMG Klynveld EDP Audit en Samsom BedrijfsInformatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 4 x per jaar.

Redactie
D. Steeman RA (hoofdredacteur)
Drs. R.G.A. Fijneman RA
Mw. D. Jansen Heijtmajer RI
A.W. Neisingh RA
Drs. P. Veltman RA

Redactiesecretariaat
Mw. A.M.F. Hofland,
Klynveld EDP Audit,
K.P. van der Mandelaan 41
3062 MB Rotterdam
Tel.: 010 - 453 47 40
Fax: 010 - 453 47 77

Vormgeving
Zetterij Hans Geurts, Nieuw-Vennep

Aan deze special werkten mee
Drs. M.A. van Alphen , RA
Prof. Mr. H. Franken
Drs. F.J.G. Fransen
Drs. N.J. Krever
J.J.A. Leenaars, RA
Drs. P.J.A. Lekkerkerker
Mr. Ong Sien Hien
D. Steeman, RA

Abonnementen
ƒ 135,- per jaar incl. BTW. Losse nummers ƒ 50,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.

Abonnementsadministratie
Samsom BedrijfsInformatie
Postbus 4
2400 MA Alphen aan den Rijn
Tel.: 01720 - 6 68 00
Fax: 01720 - 7 59 33
Adreswijzigingen - ook tijdelijke - moeten minstens 8 weken voor de verschijningsdatum bekend zijn.

Uitgever
J.R.M. Masselink

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 - 1645

Inhoudsopgave

D. Steeman
Vennoot KPMG Klynveld
EDP Audit

Betekenis van EDP Auditing voor de controlerende accountant

1 Inleiding

Het EDP-auditing beroep is in Nederland ontstaan vanuit de behoefte van accountants in hun controlerende en adviserende functie. Voor deze bijdrage wordt vooral uitgegaan van de controlerende functie, dus de controle voor het afgeven van een verklaring bij de jaarrekening. De adviesfunctie van de accountant is uit hoofde van het fungeren van de accountant altijd latent aanwezig. Dat de EDP auditor daarin een rol speelt moge duidelijk zijn na het lezen van dit artikel zelfs zonder daar expliciet aandacht aan te geven.

Accountants onderkenden reeds vroegtijdig de betekenis van mechanisatie en automatisering van gegevensverwerking voor hun werk. Voor wat betreft de automatisering dateert deze onderkenning praktisch uit de begin jaren zeventig toen de administratieve automatisering doorzette. De betekenis is sedertdien alleen maar toegenomen met de verdergaande automatisering van zowel administratieve processen als van processen welke direct verband houden met de primaire activiteiten van ondernemingen (logistieke processen).

Accountantscontrole richt zich uiteindelijk op gegevens in de jaarrekening, deze gegevens komen als eindresultaat tot stand op basis van soms uitgebreide processen van gegevensverwerking van primaire vastleggingen welke direct voortvloeien uit de activiteiten van een onderneming.

De betrouwbaarheid van de gegevens in de jaarrekening waarover de accountant zijn oordeel geeft is mede gebaseerd op de (administratieve) organisatie rond de gegevensverwerking. Deze stelling geldt zowel voor geautomatiseerde als niet-geautomatiseerde gegevensverwerking.

Men kan zeggen, dat naar mate de organisatie kwalitatief beter is, de accountant meer gebruik kan maken van (kan steunen op) deze organisatie.
Hiertoe is uiteraard onderzoek nodig naar die kwaliteit waarbij in de controleleer wordt gesproken van onderzoek naar opzet (architectuur), bestaan (is het gebouw er) en werking (maakt men er goed gebruik van).

Uitzonderingen daargelaten en rekening houdend met bepaalde kritische aspecten gelegen rond de beheersing van besturings-software, kan worden gesteld dat de automatisering een verbetering in kwalitatieve zin zowel van de administratieve organisatie als het produkt van de gegevensverwerking ten gevolge heeft gehad.

Dit betekent dat de accountant een toenemende behoefte aan onderzoek van de (geautomatiseerde) gegevensverwerking en de administratieve organisatie daaaromheen heeft (of zou moeten hebben).

Daarenboven onstaat bij belanghebbenden dan wel bij (wettelijke) toezichthoudende organen als Raden van Commissarissen, De Nederlandsche Bank, behoefte om via de bestuursorganen van een huishouding een uitspraak van de accountant te vragen over de kwaliteit van de door hem gecontroleerde organisatie van de automatisering.

2 Ontwikkeling in de controle-aanpak

Vrijwel parallel aan de ontwikkeling van

de automatisering heeft zich in de controleleer een discussie afgespeeld rond de vraag of de controle vanuit de gegevens dient plaats te vinden dan wel vanuit het systeem. De gegevensgerichte versus de systeemgerichte controle.

De algemeen aanvaarde gedachtengang is dat nog de ene vorm noch de andere vorm in optima forma kan worden toegepast.

Gegevensgerichte controle is niet mogelijk zonder (minimale) waarneming terzake van opzet en bestaan van de administratieve organisatie (het systeem).
Systeemgerichte controle kan niet gebeuren zonder op z'n minst cijferbeoordeling en -analyse van de informatie welke door de gegevensverwerking wordt opgeleverd.

De mate waarin gegevens- of systeemgericht zal worden gecontroleerd wordt niet voor de hele huishouding, waarvoor de accountant de jaarrekening dient te controleren, eenduidig vastgesteld. De accountant zal per onderdeel van de huishouding en daarbinnen per informatiestroom (de inkopen, de verkopen, de afgesloten verzekeringen etc. en daarbinnen eventueel per soort inkoop, verkoop of verzekering etc.) nagaan welke de controle-aanpak zal zijn. De bepaling van de richting van zijn controle-aanpak wordt daarbij niet alleen bepaald door de kwaliteit van de informatiesysteem en de automatiseringsorganisatie doch ook door overwegingen van efficiency en effectiviteit van de controle.

Een sprekend voorbeeld hiervan is, dat de juistheid van de rekening-courantverhoudingen van een bank met haar cliënten op eenvoudige wijze door middel van saldobiljetten kan worden vastgesteld. Waarom zal de accountant dan, als het uitsluitend om het vaststellen van die juistheid gaat, het hele ingewikkelde rekening-courantsysteem gaan onderzoeken op de opzet, het bestaan en de werking (gedurende de controleperiode) als hij via de cliënten van de bank langs deze betrekkelijk eenvoudige, dus efficiënte weg vrijwel volledige zekerheid (effectief) kan krijgen? Uiteraard zullen er in dit voorbeeld complicerende factoren zijn, hieraan wordt in dit kader voorbij gegaan.

De gegevensgerichte controle kan aantrekkelijk worden doordat de accountant zelf gebruik gaat maken van de computer.

Uiteindelijk zal voor ieder onderdeel een controlemix worden bepaald waarin beide richtingen min of meer of zelfs in gelijke mate vertegenwoordigd zijn.

3 Deskundigheid van de accountant op het gebied van de automatisering

Het theoretische uitgangspunt in de accountantskringen is lange tijd geweest dat iedere accountant een zodanige opleiding dient te hebben dat hij een voldoende eigen oordeel kan hebben over de automatisering voor zover dit zijn controle betreft. Zolang de accountantscontrole nog sterk gegevensgericht plaatsvindt, kan de opleiding toereikend zijn voor wat betreft de informatieverwerkende systemen zelf. Indien de accountant zich een oordeel wenst te vormen over de automatiseringsorganisatie blijkt vaak zijn onvermogen om tot de essentie door te dringen. Dikwijls is het niet meer dan een taalprobleem. Hij spreekt niet de algemene taal van de automatiseringsmensen, noch de specifieke waar het gaat om hardware en software waar de organisatie mee werkt.

Zodra de controle uit noodzaak (het kan niet anders) of om doelmatigheid meer systeemgericht wordt uitgevoerd, staat de accountant voor een groter probleem. Meer nog dan bij de gegevensgerichte controle zal hij de automatiseringsorganisatie dienen te onderzoeken en te beoordelen ten aanzien van opzet, bestaan en werking van de interne controle. De diepgang en frequentie van het onderzoek wordt groter.

Maar ook de informatiesystemen zullen voor de accountant een probleemgebied vormen, hoewel hij of zijn medewerkers de materiekennis meestal bezitten, zal toch de aard (bijvoorbeeld technische documentatie) een relatief hoge drempel vormen voor daadwerkelijk onderzoek.

Het moeilijke punt voor de accountant is, dat de techniek zodanig snel verandert dat dit een vrij permanente belemmering vormt om op dit gebied bij te blijven, gegeven het feit dat ook andere gebieden zoals verslaglegging, belasting, wetgeving e.d. vrij dynamisch zijn.

Opleidingen op het gebied van automatisering in relatie tot accountantscontrole

blijken nauwelijks effectief te zijn. De verworven kennis verdwijnt snel indien deze niet wordt omgezet in ervaring door praktische toepassing. Om verschillende redenen komt men uiteindelijk niet tot het daadwerkelijk doen. Zowel gebrek aan tijd op het moment dat het er op aankomt of uiteindelijke desinteresse of drempelvrees zijn hier debet aan.

Uitsluitend de praktische toepassing van microcomputers in de overwegend gegevensgerichte controle kan als een doorslaand succes worden bestempeld.

4 Wat betekent EDP-audit voor de accountant

EDP-audit kan worden omschreven als:

Het onderzoek gericht op het beoordelen van een of meer kwaliteitscriteria van de automatisering uitmondend in een oordeel en eventueel daaraan gerelateerde adviezen.

Over het begrip kwaliteit valt natuurlijk ruimschoots te discussiëren. In de literatuur over EDP-auditing worden van oudsher genoemd de criteria:
- betrouwbaarheid;
  - juistheid;
  - volledigheid;
  - tijdigheid;
  - bevoegdheid;

  | aspecten
- vertrouwelijkheid (soms genoemd exclusiviteit);
- continuïteit (beschikbaarheid);
- controleerbaarheid;
- doelmatigheid;
- doeltreffendheid.

In zijn artikel in Compact herfst 1990 onderscheid M.J. van der Vos naast genoemde criteria en met weglating van het criterium doeltreffendheid nog:
- bruikbaarheid;
- flexibiliteit;
- onderhoudbaarheid;
- overdraagbaarheid;
- koppelbaarheid.

De volgorde van de hiervoor genoemde criteria geeft tevens de ontwikkeling van het vak EDP-auditing aan. Zoals in de inleiding gesteld onderkenden accountants reeds vroegtijdig de noodzaak tot beoordeling van de automatisering. Het ging toenmaals vooral om het criterium betrouwbaarheid met de hier als voorbeeld aangegeven aspecten. Het kwaliteitsbeeld was toen beperkt namelijk voor zover nodig voor de behoefte van de accountantscontrole.

De criteria vertrouwelijkheid en continuïteit zijn voor de accountant aan het kwaliteitsspectrum toegevoegd. Niet ten behoeve van het oordeel als controleur van de jaarrekening. Wel in de vorm van een eventuele bijzondere opdracht in het kader van zijn fungeren voor de huishouding. Voorbeeld: het memorandum van De Nederlandsche Bank.

Voor deze criteria en de daarbij behorende hier niet nader uitgewerkte aspecten, kunnen redelijk normen worden gedefinieerd.
Deze normen dienen meestal gegeven de specifieke situatie in overleg tussen de auditor en de auditee worden gedefinieerd.

De overige criteria maken het kwaliteitsspectrum compleet en worden gehanteerd vanuit de behoefte van de opdrachtgever in zijn specifieke situatie. De normering is hier veel moeilijker en afhankelijk van het subjectief inzicht van zowel de auditor als de auditee. De effectiviteit van oordeel en eventueel advies is afhankelijk van overtuigingskracht en geloofwaardigheid aan de kant van de auditor en de bereidheid tot accepteren aan de kant van de auditee.

De betekenis van de EDP-auditor voor de accountant schuilt vooral daar waar de accountant zich door onvoldoende deskundigheid in de diepte, gebrek aan tijd en affiniteit wil laten bijstaan door een meer op de automatisering geverseerde EDP-auditor. Dit tast de functie van de accountant niet aan mits hij zich een oordeel kan vormen over de kwaliteit van de EDP-auditor zelf. Het is in veel gevallen uiterst doelmatig om de EDP-auditor in te schakelen.

Een voorwaarde voor de inschakeling is dat men het eens is over de opdrachtomschrijving. Een opdracht in de trant van: "Wil je eens naar het computercentrum kijken", zoals dit in het verleden nog wel eens voorkwam, is niet acceptabel en komt ook niet meer voor. Niettemin is de waarschuwing op zijn plaats dat een zo zorgvuldig mogelijke opdrachtsdefiniëring een basis is voor succes en het vermijden van teleurstelling achteraf.

5 Ontwikkeling van het vakgebied EDP-auditing

Vanuit de oorspronkelijke behoefte met name bij accountants tot het verkrijgen van een oordeel over de betrouwbaarheid heeft de EDP-auditor zijn functie zien uitgroeien.
In de breedte van de opdrachtgevers, waarbij ook de leiding op verschillende niveau's zich als opdrachtgevers aandienen.
In de aard van de opdrachten van strikt beoordelend tot richtinggevend adviseren en zelfs meewerken aan bijvoorbeeld het ontwerpen van het interne controleraamwerk voor een informatiesysteem in ontwikkeling.

In de soort opdrachten als het beoordelen van en adviseren over:
- Juridische aspecten van software contracten (zie hiervoor Compact Winter 1990)
- de privacy wetgeving
- het testen van een systeem op veiligheid (bestand tegen hackers)

De EDP-auditor is natuurlijk niet de enige dienstaanbieder op het terrein van de kwaliteitsbeoordeling en de advisering over kwaliteitsaspecten. Hij heeft een zekere exclusiviteit op de criteria waaruit het vak is ontstaan. Voor de criteria anders aan betrouwbaarheid, wordt de exclusiviteit minder en treden concurrenten op als organisatie-adviseurs en informatici in brede zin.

Zijn exclusiviteit wordt bepaald door de deskundigheid op het gebied van techniek en organisatie.

Universitaire opleidingen staan borg voor het niveau van de EDP-auditing waarbij Nederland voorop loopt in de ontwikkeling van het vak.

6 Slotopmerkingen

Terugkerend naar de titel van het artikel kan worden gesteld dat de accountant in theorie het onderzoek naar de kwaliteit van informatiesystemen en automatiseringsorganisatie zelf kan doen.

De ervaring leert dat de praktijk anders is en dat de accountant er verstandig aan doet zich tot de EDP-auditor te wenden voor die onderdelen van zijn werk die met automatisering te maken hebben. De aard van de opdracht kan varieren tot het geven van een consult tot het ontwerpen van (delen van) het controleprogramma voor zover van betrekking op de geautomatiseerde gegevensverwerking.

Op dit gebied kan met de huidige gelijdelijke tendens tot meer systeemgericht controleren nog veel uitbreiding van het werkterrein van de EDP-auditor worden verwacht.

De eens wel geponeerde stelling: "de EDP-auditor zal de accountant verdringen uit zijn functie" kan gevoegelijk naar het rijk der fabelen worden verwezen.

Beide functies zullen elkaar nodig hebben:

De accountant om zijn verantwoordelijkheid te kunnen dragen.

De EDP-auditor om een goede boterham te eten.

De heer Steeman, RA studeerde in 1969 af als registeraccountant en is al meer dan 20 jaar werkzaam in de EDP Auditing. Van 1975 tot 1987 fungeerde hij als buitengewoon hoogleraar Accountancy aan de Erasmus Universiteit. De heer Steeman is vennoot van KPMG Klynveld EDP Audit.

Drs. M.A. van Alphen RA
Lid Raad van Bestuur
Internatio-Müller NV

Is EDP-auditing het slijpen van de ganzeveer?

Centraal in dit artikel staan de meer algemene aspecten van de EDP-audit, zoals die naar voren komen in de financiële beleidsvorming van een onderneming, in dit geval Internatio-Müller.

1 Ondernemingsschets

Internatio-Müller bestaat uit een holdingmaatschappij met circa 80 werkmaatschappijen in binnen- en buitenland en 11.000 werknemers. In personeelsomvang lopen deze dochters uiteen van 10 tot 2.500 medewerkers. Ook de activiteit van de ondernemingen is onderscheiden van aard; zij vindt plaats in handel, transport en techniek. Op zich betekent dit dus al dat de administratieve organisatie van de ondernemingen nogal verschillend is.
Concreet vertaalt dit zich in:
- De gediversificeerde bedrijfstypologieën leveren een grote schakering aan informatiebehoeften.
- De decentrale verantwoordelijkheid inzake bedrijfsvoering beperkt de mogelijkheid tot het geven van uniforme richtlijnen.
- De kleinschaligheid van een aantal werkmaatschappijen legt beperkingen op aan de mogelijkheid van functiescheiding en creëert een spanningsveld tussen efficiency en betrouwbaarheid.

Ten behoeve van de beheersbaarheid is het concern verdeeld in een aantal sectoren waarbinnen groepen bedrijven zijn samengebracht met dezelfde markt of hetzelfde produkt of dezelfde dienst. Aan het hoofd van iedere sector staat een sectordirecteur met in ieder geval een sectorcontroller.

De vraag is nu hoe in een dergelijk concern de administratieve automatisering het financieel-administratieve beheer optimaal kan ondersteunen?
Op zoek naar een antwoord op die vraag wil ik mij concentreren niet op de automatisering van het Centraal Kantoor van de groep, maar op die van de werkmaatschappijen inclusief de financiële rapportage naar het Centraal Kantoor toe.

Wat het Centraal Kantoor betreft heeft Internatio-Müller overigens enige jaren geleden zowel de functies van het eigen rekencentrum als die van de eigen interne accountantsdienst overgedragen aan externe organisaties.
Wat de onderneming wel centraal onder meer nog heeft, en dit is van belang voor de rest van deze beschrijving, zijn kleine, hoogwaardige centrale afdelingen: Informatie-Technologie, Groepscontrolling en Operational Audit.

Voor wat betreft de organisatie van de werkmaatschappijen zijn wij enerzijds uiteraard geïnteresseerd in een zo efficiënt mogelijke administratieve automatisering ten behoeve van de bedrijfsvoering, anderzijds willen wij waarborgen voor de betrouwbaarheid gezien de risico's die wij dragen als moeder-aandeelhouder.
In ons concern garandeert de holdingmaatschappij de verplichtingen van de dochters, in ieder geval in het Nederlandse wetsgebied. Dit betekent dat er niet alleen belangstelling is voor een zo groot mogelijk overschot van de opbrengsten boven de kosten, maar ook dat geen overmatige risico's worden gelopen c.q. verrassingen worden ondervonden bij het beheer van de activa en passiva en de off-balance verplichtingen.

2 Maatregelen

Welke maatregelen kunnen wij nu nemen vanuit het centrum om deze doeleinden te bereiken?

1. De leiding van de werkmaatschappijen en sectoren ervan doordringen dat administratieve automatisering niet zonder meer aan anderen moet worden overgelaten maar een *wezenlijk onderdeel van de directieverantwoordelijkheid* is. In de ondernemingsplannen dient EDP separate aandacht te krijgen.

2. Zorgdragen voor *deskundige sectorcontrollers* die de adminstratieve automatiseringsfunctie goed tot haar recht kunnen laten komen. In dit verband is het overigens de vraag, of het wel zo zeker is dat wij naar aparte "information officers" toegaan, los van de controllers. Waar de primaire taak van de controller is om de financiële data te verwerken, wijzigt de methode waarop dit gebeurt niet dit principe. Vandaar ook de titel van dit artikel: "Is EDP-auditing het slijpen van de ganzeveer?" Hier mag de lezer ook invullen "het poetsen van de kroontjespen?"

3. Afhankelijk van de behoefte zorgen voor een *centrale adviesfunctie* c.q. het geven van voorschriften voor de geautomatiseerde gegevensverwerking in de administratie van de bedrijven.

4. Zorgen voor *adequate controle* van de administratieve organisatie inclusief uiteraard EDP.

Wat betreft punt 3, de "voorgangersrol", ziet men dat de grotere concerns centraal steeds minder gedetailleerd voorschrijven op welke wijzen en met welke systemen de administratieve EDP-functie in de werkmaatschappijen moet worden ingevuld. De lokaal-verantwoordelijken krijgen, naarmate de kennis van automatisering steeds meer verspreid wordt enerzijds en de gebruiksvriendelijkheid alsmede de servicebereidheid van de leveranciers toenemen anderzijds, de vrijheid en mogelijkheid om hun eigen keuze te maken.
Dit laat natuurlijk onverlet de wenselijkheid om bij gelijksoortige problematieken, zoals projectbeheersingssystemen bij installatiebedrijven, ook het gebruik van dezelfde systemen aan te bevelen.

In hetzelfde kader van de voorgangersrol is zichtbaar, dat het apparaat dat oorspronkelijk voor de controle achteraf was bedoeld, meer ook een ex ante rol krijgt. Dit is overigens een weerslag van het fenomeen dat ook bij de accountantskantoren steeds belangrijker wordt, namelijk de groei van de adviespraktijk ten opzichte van de controlepraktijk.

Ik zal daarom verder in dit artikel geen helder onderscheid meer maken tussen adviezen/voorschriften vooraf en controle achteraf.

3 Organen

Welke centrale organen zijn nu betrokken bij deze maatregelen? Dat zijn:
- Groepscontrolling;
- Informatie-Technologie;
- Operational Audit;
  alsmede de
- externe accountant.

Groepscontrolling
Groepscontrolling direkt onder de Raad van Bestuur speelt een sleutelrol in het financieel-administratieve dit beleid. Als wegbereider voor beleid en als opsteller van geconsolideerde verantwoordingen en bedrijfseconomische analyses wordt de effectiviteit van de afdeling in hoge mate bepaald door de administratieve organisatie en geautomatiseerde gegevensverwerking bij de werkmaatschappijen.

Algemeen geldend: Kwaliteit aan de basis van de informatieverzorgingspiramide bepaalt de kwaliteit aan de top.

In het kader van deze functie stelt Groepscontrolling dan ook haar eisen aan de administratieve organisatie en automatisering bij de maatschappijen. Zij werkt daartoe nauw samen met de hiernavolgende staffuncties Informati-Technologie en Operational Audit en met onze externe accountant.
Tezamen met de sectorcontrollers vervult dit samenwerkingsblok een contructieve functie in het kwaliteitsverbeteringsproces van administratieve organisatie en automatisering.

Informatie-technologie
De centrale afdeling Informatie-Technologie ressorteert eveneens rechtstreeks onder de Raad van Bestuur. De functie van deze afdeling is tweeledig:
a. het ondersteunen bij het ontwikkelen van een strategisch groepsbeleid in-

zake informatie- en automatiseringssystemen;
b. het bevorderen dat de informatiesystemen bij de bedrijven zodanig worden opgezet dat ze voldoen aan de randvoorwaarden zoals geformuleerd in het concernbeleid.

Het doel is om:
- de kwaliteit en de betrouwbaarheid van de informatiesystemen te verhogen;
- eventuele risico's bij de invoering te beperken;
- uitwisseling van kennis en ervaring mogelijk te maken tussen de sectoren en/of werkmaatschappijen.

Daarom spreken wij in ons automatiseringsbeleid de voorkeur uit voor gebruikmaking van kwalitatief hoogwaardige standaardtoepassingspakketten en zijn wij nog steeds voorstander van het gebruik van twee met name genoemde infrastructuurleveranciers.
Eventueel benodigd maatwerk mag de structuur van het standaardpakket niet aantasten.
Ten behoeve van het vaststellen welke standaardpakketten kwalitatief hoogwaardig zijn, zouden wij *onafhankelijke certificering* sterk toejuichen. Deze mag geïnitieerd worden door de pakketleverancier, maar dient uiteraard niet de geur met zich te dragen hierdoor geïnspireerd te zijn. Het is van groot belang en zal ook bevorderend werken voor de acceptatie van de pakketten, als een onafhankelijk certificaat wordt meegeleverd. Hier ligt ons inziens een mooi werkterrein voor het Instituut Certificering van Informatie-Technologie Produkten (ICIT).

Systeemontwikkeling in de betekenis van volledig maatwerk komt alleen daar voor waar dit gezien het specifieke karakter van de bedrijfsactiviteiten en de strategie van de desbetreffende onderneming geboden is.

De investeringen in de automatisering dienen gebaseerd te zijn op een informatieplan, reikend van de strategie van de onderneming tot aan het aspect continuïteit en beveiliging. Dit alles met afweging van kosten en baten.

Hoewel toetsing van de effectiviteit van de op te zetten informatiesystemen in eerste instantie de aandacht heeft, worden de criteria efficiency, integriteit, continuïteit en controleerbaarheid van het systeem zelf, alsmede de kwaliteit van de leveranciers mede in de oordeelsvorming betrokken. Met name betreffende de drie laatstgenoemde criteria wordt samengewerkt met de afdeling Operational Audit.
Rapportering vindt plaats aan het lokale management, de sectorleiding en aan de de Raad van Bestuur. Indien nodig maakt Informatie-Technologie deel uit van de stuurgroep als toezichthouder op het traject van voorbereiding tot en met installering. Dit vooral bij de invoering van complexe en dus risicovolle projecten.

Operational Audit
Sedert 1985 beschikt Internatio-Müller over een centrale afdeling Operational Audit als uitvloeisel van het overdragen van de Financial Audit-functie aan de openbare accountant.

Operational Audit heeft als hoofdtaak: het beoordelen van inrichting en werking van de interne organisatie in het algemeen en de administratieve organisatie in het bijzonder over de volle breedte van het concern.
De beoordelingscriteria zijn effectiviteit, efficiency en beheersbaarheid.

De door Operational Audit uitgevoerde audits hebben voornamelijk een preventief karakter en in beginsel is iedere werkmaatschappij, of deel hiervan, object van onderzoek in een cyclus van drie à vier jaar. De uitkomsten van de onderzoeken worden in chronologische volgorde aan het lokale management, de sectorleiding en aan de Raad van Bestuur gerapporteerd.
De bevindingen en aanbevelingen worden besproken in een driemaandelijkse bijeenkomst van Raad van Bestuur, Groepscontrolling en Operation Audit.
Afhankelijk van het belang van de situatie worden acties naar de betrokken sectoren ondernomen. Een min of meer vaststaand uitgangspunt is dat binnen een periode van één jaar een followup-audit plaatsvindt.

Omdat in onze zienswijze EDP de *"machinekamer"* van de administratieve organisatie is, maakt deze deel uit van het beoordelingspakket van Operational Audit.
De reeds eerder genoemde kenmerken van de Internatio-Müller-structuur, te weten diversiteit in typologieën, decentrale bedrijfsvoering en schaalgrootteverschillen, hebben hun invloed op omvang, diepgang en inhoud van de EDP-audits.

Gevolg: veel maatwerk met prioriteitenstelling op basis van risicoschatting.

De huidige situatie geeft aan dat in de praktijk het accent meer ligt op de criteria integriteit, continuïteit en controleerbaarheid dan op effectiviteit en efficiency, aangezien de werkmaatschappijen geacht kunnen worden zelf met name de laatste aspecten na te streven.
De onderzoekobjecten zijn: applicaties, beveiliging en organisatie.
De applicaties moeten ruim worden gezien. Hoewel het financiële karakter de boventoon voert, zijn ook applicaties ten behoeve van primaire en ondersteunende processen van niet-financiële aard object van onderzoek (produktiebesturing, planning, logistiek, en dergelijke).
Technical EDP-audits behoren niet tot het werkpakket. Indien zij nodig zijn worden zij uitbesteed.

Op het terrein van beoordeling van financiële systemen wordt nauw samengewerkt met onze externe accountant.

Externe accountant
Onze externe accountant heeft zijn eigen verantwoordelijkheid inzake de jaarrekeningcontrole. Uit dien hoofde verricht hij al naargelang het belang van geautomatiseerde systemen EDP-audits. De uitkomsten hiervan verschijnen in de vorm van conclusies en aanbevelingen in de management letters. Tegenwoordig bevat nagenoeg elke mangement letter wel een paragraaf over EDP.

Hoewel de onderzoeken van externe accountants verricht worden met name met het oog op het certificaat bij de jaarrekening, komt als bijprodukt dikwijls een oordeel over bijvoorbeeld de efficiency vrij.
Bovendien verricht de EDP Audit Groep van onze accountant op verzoek van het Centraal Kantoor of van sectoren/werkmaatschappijen specifieke audits met min of meer technisch karakter.

In het kader van kwaliteitsverbetering vervullen deze onderzoeken een waardevolle functie. Afhankelijk van het gewicht worden op korte termijn followupaudits gestart, danwel vormen zij de basis voor inpassing in het eerstvolgende Auditplan; een dergelijk plan stellen wij jaarlijks vast en wordt uitgevoerd door Operational Audit.

Resumerend kan worden gesteld dat de EDP-audit in wijde zin, ook preventief, tot stand komt binnen het samenwerkingsverband van bovengenoemde afdelingen en de externe accountants.

4 Mededeling in jaarverslag

In het kader van dit nummer van Compact lijkt mij een enkele kanttekening op zijn plaats bij het wetsvoorstel om op aanbeveling van de Commissie Franken het Burgerlijk Wetboek Boek 2 artikel 391 lid 2 aan te vullen. Het gaat om een voorschrift, dat in het jaarverslag van een onderneming voortaan een mededeling moet worden opgenomen omtrent de genomen maatregelen in verband met de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

Mede als lid van de Raad voor de Jaarverslaggeving wil ik onderstrepen, dat invoering van het wetsvoorstel mij ongelukkig voorkomt. De beveiliging en het zorgdragen voor een betrouwbaar informatiesysteem is een onderdeel van verantwoord ondernemerschap. Als zodanig verdient het geen uitzonderingspositie, want wat is dan het argument om niet ook te pleiten voor bijvoorbeeld een verklaring inzake milieuzorg, inzake een correcte naleving van de ARBO-wet, inzake het behartigen van de belangen van allerlei minderheidsgroeperingen in de onderneming, enz.

Deze opinie wordt des temeer ondersteund door het feit, dat in de Memorie van Toelichting als argument wordt vermeld, dat opname van een dergelijke verklaring "de directie dwingt zich rekenschap te geven van dit onderdeel van de gang van zaken binnen de onderneming". Waar dit een begrijpelijke eis kan zijn voor een bankverslag, gezien het belang van het geldafgevend publiek bij een adequate geautomatiseerde gegevensverwerking, dat immers als essentieel onderdeel van de bankoperaties moet worden beschouwd, bestaat deze situatie bij het algemene bedrijfsleven niet.

Indien tegengeworpen wordt dat volgens artikel 391 van het BW aan een aantal andere zaken van het ondernemen ook aparte aandacht in het jaarverslag moet worden gegeven (gedoeld wordt hier op de mededelingen omtrent de verwachte gang van zaken, investeringen, financiering, research en ontwikkeling, enz.), wordt uit het oog verloren dat dit op zich impliciet goedkeurende mededelingen

zijn. Er wordt daar gevraagd om uiteen te zetten hoe een en ander binnen of rondom de onderneming ervoor staat, niet of het goed geregeld is.

In dit geval evenwel moet ervan uitgegaan worden, dat slechts een positieve verklaring acceptabel is. In vele gevallen zal dit betekenen dat de certificerende accountants, opdat zij de verklaring kunnen steunen, additionele werkzaamheden zullen moeten verrichten, welke verder gaan dan noodzakelijk in het kader van de jaarrekeningcontrole. Anders wordt het een formele verklaring zonder inhoud, en hoewel dit in andere wetsgebieden wel eens voorkomt, ben ik daarvan als Nederlands ondernemer geen voorstander.
De goedkeurende verklaring van de accountant met de huidige reikwijdte houdt impliciet in, dat er geen zodanige organisatorische problemen bestaan die de continuïteit van de onderneming direct in gevaar zouden brengen, danwel een getrouw beeld van de jaarrekening in de weg staan.

Naar mijn verwachting zal het Nederlandse bedrijfsleven zelf voortgaan met het ontwikkelen van de mogelijkheden die de voortschrijdende automatiseringstechnieken bieden ten behoeve van het besturen en het doen functioneren van de bedrijfshuishouding en de verantwoording die daarover moet worden afgelegd.

5 Tot slot

Vanwaar "Is EDP-auditing het slijpen van de ganzeveer?" als titel voor dit artikel?
De lezer moet mij niet vastpinnen op de feitelijke onjuistheid van de vergelijking computer/ganzeveer. Dat de ganzeveer enkel kan schrijven en de computer ook kan rekenen en logische bewerkingen zonder menselijke tussenkomst kan uitvoeren, is duidelijk.
Het gaat mij meer om met behulp van dit archaïsche beeld een tweeledige boodschap door te geven aangaande mijn visie op de positie van EDP in het geheel en van de professie van EDP-audit:

1. EDP, althans administratieve automatisering, maakt deel uit van een groter geheel, namelijk administratieve organisatie, ook wel aangeduid als bestuurlijke informatieverzorging. Termen als "van strategisch belang", "beslissingsondersteunend", "tool of management", enz. doen hier niets aan af.
   Het relatieve gewicht van EDP wordt echter steeds zwaarder vanwege de grotere afhankelijkheid van de bedrijfsvoering. Afstompen van de ganzeveer werkt dan ook meer dan evenredig in negatieve zin door in de output van de administratieve organisatie als geheel.
   Het aanscherpen van de ganzeveer levert daarom een relatief grote bijdrage aan het verbeteren van de Adminstratieve Organisatie en verdient daarom alle aandacht. Dat de bedrijfsleiding zich hierbij dikwijls, al of niet noodgedwongen, zal concentreren op de resultaten en de organisatorische aspecten en niet op de techniek, doet hieraan niets af.

2. Een advies aan het adres van de EDP-audit beroepsgroep. Het lijdt geen twijfel dat beantwoording aan alle criteria zoals gedefinieerd in NIVRA-geschrift 53, een schaap met vele discipline-poten vraagt. De opdrachtgever zal dienen aan te geven welke EDP-objecten op welke criteria beoordeeld moeten worden. De auditor dient voor zichzelf zorgvuldig af te wegen of zijn deskundigheid hierop adequaat is afgestemd, dat wil zeggen of hij de kennis en de kunde heeft om met het juiste mes de ganzeveer te slijpen.

Drs. M.A. van Alphen, RA behaalde zijn doctoraal Economie aan de Erasmusuniversiteit te Rotterdam. Vervolgens deed hij ervaring op in diverse functies in het bedrijfsleven, waarna hij in 1982 in dienst trad bij Internatio-Müller N.V. Thans maakt hij er deel uit van de Raad van Bestuur en is met name belast met de financiële portefeuille. Sedert 1978 is de heer Van Alphen registeraccountant.

Drs. F.J.G. Fransen
Algemeen Directeur Neddata B.V.

EDP-audit bij een intern automatiseringshuis

1 Ondernemingsschets

De Koninklijke Nedlloyd Groep NV is actief op het gehele terrein van transport, zowel ter zee als op het land en in de lucht, alsmede op het terrein van expeditie, opslag en distributie. In de loop der jaren heeft Nedlloyd zich ontwikkeld van scheepvaartonderneming tot een bedrijf waarbij het accent in toenemende mate is komen te liggen op logistieke dienstverlening: de totale beheersing van fysieke goederenstromen ten behoeve van verladers en ontvangers waar ook ter wereld.

De kernactiviteiten zijn:
- containerlogistiek op wereldwijze schaal, voornamelijk gebaseerd op eigen scheepvaartverbindingen;
- opslag en distributie- en transportnetwerken te land, op Europese schaal;
- gespecialiseerd vervoer, zoals het confectievervoer en het vervoer van chemicaliën, ten minste op Europese schaal.

Daarnaast heeft Nedlloyd belangen in energie en neemt deel in brancheverwante ondernemingen, onder andere op het gebied van luchtvaart en overslag van containers.

De omzet over 1989 (x f 1 miljoen) was als volgt opgebouwd:

Zeescheepvaart	2.479
Overig transport	2.981
Energie	179
Deelnemingen	370
Totaal	6.009

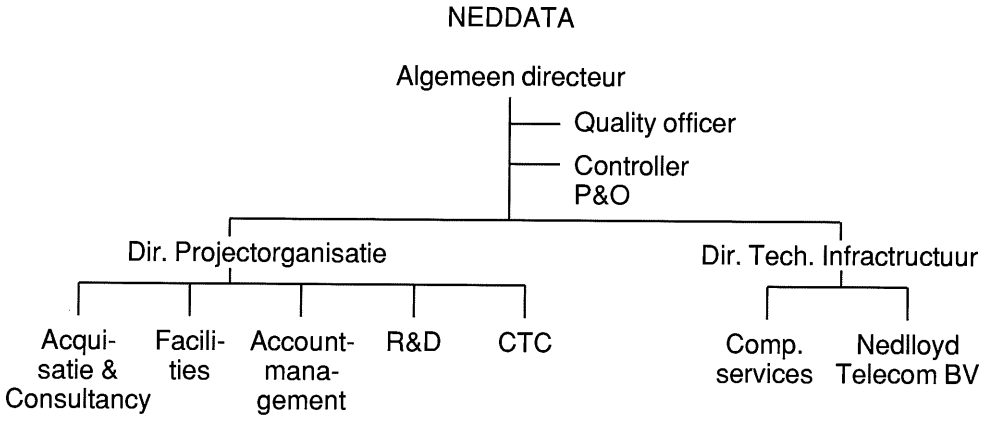
Het aantal werknemers bedraagt 24.300.

Organisatorisch is Nedlloyd ingedeeld in divisies en een aantal stafdirectoraten.

2 De automatiseringsfunctie bij Nedlloyd

De automatiseringsfunctie is verspreid over Nedlloyd. Op groepsniveau is er het stafdirectoraat Groep Nedlloyd Informatica (GNI). Enerzijds vaardigt GNI beleidslijnen uit, die in de groep geldig zijn, onder meer via het Bureau Nedlloyd Standards, verantwoordelijk voor de standaardisering van voor de groep relevante gegevens. Anderzijds toetst GNI namens de Raad van Bestuur het automatiseringsaspect in investeringsplannen van divisies en werkmaatschappijen.
Divisies en/of werkmaatschappijen hebben, naar eigen keuze, al dan niet eigen automatiseringsafdelingen. De activiteitenpakketten variëren van complete zelfverzorging (systeemontwikkeling + produktie) tot kleinschalig systeembeheer.

Dan is er Neddata BV, een compleet automatiseringshuis dat als profitcentre opereert. Vooralsnog is Neddata vrijwel uitsluitend actief ten behoeve van Nedlloyd-bedrijven. Nauw gelieerd met Neddata is Nedlloyd Telecom BV, dat belast is met de verdere uitbouw en het beheer van alle telecommunicatiefaciliteiten binnen Nedlloyd, waaronder het private network Neptune. Het organogram van Neddata ziet er als volgt uit:



Figuur 1

Systeemontwikkeling geschiedt bij Neddata volgens SDM II. Er wordt met ORACLE-dbms en ORACLE 4-GL gewerkt tenzij dat om performance-redenen niet kan. CASE-tools (onder andere van ORACLE en McDonald Douglas), vormen het dagelijkse gereedschap, geïnstalleerd op workstations en PC's. In de produktie-omgeving staan opgesteld een IBM-3090 en een grote DEC-VAX-cluster, alsmede een AS400 en een TANDEM-nonstop-machine ten behoeve van het telexverkeer.
Het Private Network is gebaseerd op X.25 en X.400 en naar mogelijkheid vendor-onafhankelijk geconfigureerd.

Neddata telt circa 300 werknemers. Samen met BSO heeft Neddata een dochteronderneming, TransportData. TransportData richt zich op de automatisering binnen de transport- en distributiebranche, zowel nationaal als internationaal.

Nedlloyd heeft op groepsniveau een beveiligingscoördinator. Security-aspecten in de produktie en binnen het netwerk zijn primair de verantwoordelijkheid van Neddata, respectievelijk Nedlloyd Telecom BV. Regelgeving en optimalisering vinden plaats in overleg met de beveiligingscoördinator.

3 EDP-audit bij Neddata

Binnen Nedlloyd kan Neddata onderwerp zijn van een EDP-audit. Recent zijn bij Neddata twee audits uitgevoerd, één bij de afdeling Computer Network Services (CNS) en één bij de afdelingen Consultancy en System Development (de projectorganisatie). Deze audits waren nogal verschillend van karakter. Zonder deze audits concreet de revue te laten passeren zal onderstaand een aantal aspecten worden toegelicht dat bij een audit van belang is, met name als het een intern automatiseringshuis of interne automatiseringsafdeling betreft.

4 Wie vraagt om de audit en waarom?

Allereerst is het de vraag wie de audit initieert. In dit geval kan dat zijn de Raad van Bestuur, een klant of Neddata zelf. Onmiddellijk daarmee verbonden is de vraag, waarom de audit wordt verricht, wat de aanleiding is en wat het doel. Wordt de audit door de Raad van Bestuur geïnitieerd, dan zou de aanleiding onder meer kunnen liggen in het gevoel onvoldoende greep te hebben op de automatisering of in de vraag of de ermee gemoeide gelden wel nuttig besteed zijn. De doelstelling zal dan zijn tot heldere criteria te komen ten behoeve van beleidsformulering. Een gevolg zou kunnen zijn dat de automatiseringsfunctie wordt gereorganiseerd, of (extreem) wordt opgeheven.
Een klant zou om een audit kunnen vragen omdat de prijs/prestatie-verhouding verslechtert of omdat projecten alsmaar uit de hand lopen. Verhoging van de servicegraad en verbetering van het beheersapparaat moeten dan het resultaat zijn. Het zou echter, al dan niet expliciet, ook de bedoeling van de klant kunnen zijn aldus aan te tonen dat hij voortaan maar beter de automatisering in eigen beheer kan uitvoeren. Men zou deze audit toetsend ("is het wel in orde") danwel bevestigend ("zie je wel, het is foute boel") kunnen noemen.
Neddata zou om dezelfde redenen ook zelf een audit kunnen laten uitvoeren. Die zou dan ondersteunend en/of bevestigend kunnen zijn: men weet dat het beter kan en vraagt een deskundige om daarover zijn licht te laten schijnen, res-

pectievelijk men weet dat de zaken goed voor elkaar zijn en wil dat door een externe deskundige nog eens laten bevestigen.
De "natuurlijke" houding van de onderzochte partij ten opzichte van de onderzoeker zal in beide situaties nogal verschillen. In het eerste geval zal de adviseur wellicht met achterdocht worden bekeken, hij is immers een soort politieagent; in het tweede geval is het eerder een vriend. Wordt de auditor met argwaan bekeken, dan is uitvoering van zijn aanbevelingen zeker geen vanzelfsprekende zaak. Wil een audit succes kunnen hebben, dan zal derhalve aan de acceptatie van de mogelijke uitkomsten veel aandacht moeten worden besteed. Opdrachtgever en onderzochte zullen het erover eens moeten zijn dat een audit nuttig is en op welke punten de audit gericht zal zijn. Daarmee is het volgende belangrijke punt aan de orde.

5 Waarop is de audit gericht?

Betreft het een doorlichting van de gehele automatiseringsorganisatie, is het een doorlichting van een systeem op gebruikersnut of misschien op doelmatigheid van de programmatuur of betreft het de betrouwbaarheid van een systeem? De opdracht zal helder moeten zijn beschreven. Dit is nodig om een degelijk plan van aanpak te kunnen opstellen en om vast te kunnen stellen wie bij de audit betrokken moeten worden. Van groot belang is daarbij natuurlijk de houding die de onderzoeker ten toon spreidt. Stelt hij zich op als een politieagent of schoolmeester "die wel even komt vertellen hoe het moet", dan is de kans op een succesvolle audit uiteraard aanzienlijk kleiner dan in het geval dat hij zich als adviseur raadgevend en ondersteunend manifesteert.

6 Welke normen worden gehanteerd?

Van belang is natuurlijk ook welke normen er gehanteerd zullen worden. Wordt er getoetst aan de procedures, regels en richtlijnen die bij de organisatie in gebruik zijn, of zijn de normen geldig die door de auditor worden aangedragen? Zijn er überhaupt normen die algemeen geldig zijn? Deze vragen zijn bij een betrouwbaarheids-audit veel eenvoudiger te beantwoorden dan bij de doorlichting van de automatiseringsorganisatie.

7 Wie verricht de audit?

Ten slotte is de vraag waarop de audit gericht zal zijn van belang bij de keuze van degene die het onderzoek zal uitvoeren. Voor de hand liggende kandidaten zijn enerzijds de externe accountant of een extern adviesbureau van algemene dan wel specialistische aard en anderzijds interne "bureaus", bijvoorbeeld de afdeling Interne accountancy of de afdeling (Administratieve) Organisatie. Met name als de te onderzoeken organisatie zelf de audit heeft geïnitieerd, is het zinvol om in ieder geval eigen mensen in het team op te nemen. Niet alleen is dit een leerrijke ervaring voor betrokkenen, ook de invoering kan hierdoor soepeler verlopen. Wordt de audit "opgelegd" dan is inbreng van eigen mensen nog steeds het overwegen waard, maar zal dan met meer zorg omgeven moeten worden.
Is het bureau geselecteerd, dan is nog van belang welke persoon de opdracht uitvoert. Over welke vaardigheden, kennis en kunde moet hij beschikken? Moet hij primair accountant zijn of EDP-auditor of informaticus, of is een allround organisatie-adviseur beter op zijn plaats? Zowel de opdrachtgever als de onderzochte partij zullen vertrouwen moeten hebben in de onderzoeker, wil er sprake van zijn dat met de uitkomsten van de audit ook daadwerkelijk iets gedaan wordt.

In de tabel zijn bovengenoemde vragen nog eens samengevat en worden enkele aanbevelingen terzake gedaan.

8 Enkele succesbepalende factoren

Een audit kan zeer nuttig zijn. Het is zaak de kans op succes zo groot mogelijk te maken door aan de randvoorwaarden veel aandacht te schenken.

Een opsomming van een aantal belangrijke factoren (in willekeurige volgorde) geeft het volgende beeld:
- steun van de topleiding, zowel aan de kant van de opdrachtgever als bij de onderzochte organisatie;
- duidelijke afbakening van de opdracht;
- onafhankelijkheid van de teamleden; de schuldvraag ligt om de hoek!;
- goede introductie bij de te onderzoeken organisatie;
- planmatige en voor betrokkenen inzichtelijke werkwijze, geen geheimzinnigdoenerij;

Soort audit en teamsamenstelling.

soort deskundigheid / *Soort audit*	Automatisering							Mogelijke teamsamenstelling		
	Algemeen	Apparatuur Harde prog.	Programmatuur	Organisatie-kunde	Beveiligings-aspecten	Adm. Org./ Accountancy	m.b.t. Toepassingsgebied	Aantal	Extern/ intern	Discipline
Algemene doorlichting	+++	+	+	+++	+	+	++	1 à 3	E + I[1]	Organisatie-/ informatica-adviseurs
Specifieke doorlichting										
Apparatuur	+	+++	++					1 à 3	E + I[2]	Systeem-programmeurs
Procedures	+			+	+	+++		1 à 3	1[3]	accountants, adm. organisatiedeskundigen
Doelmatigheid	+	+	+++		+			≥ 1	1[3]	Gekwalificeerde programmeurs
Beveiliging	++	+	+	+	+++	+		1 à 3	1[4]	Beveiligings-specialisten
Systeemontwikkeling (betrouwbaarheid)	+	+	++		+	+++	++	≥ 1	1[3]	(EDP)-accountants
Systeem-doorlichting										
Algemeen nut	++	+	+	++		+	+	1 à 3	1[3]	Organisatie-/ informatica-adviseurs
Specifiek aspect	++		+	+		++	++	1 à 3	1[3]	Accountants, organisatie-/ informatica-adviseurs

+++ = uitgebreide kennis/kunde
++ = behoorlijke kennis/kunde
\+ = enige kenis/kunde
= niet van belang

1) Onafhankelijkheid is hier zeer belangrijk, mede gezien het niveau binnen de organisatie waarop zich de doorlichting afspeelt. Dit leidt er mijns inziens toe dat ten minste de teamleider een externe gekwalificeerde organisatie-/informatica-adviseur dient te zijn. Opnemen van interne functionarissen in het team kan nuttig zijn in verband met "kennis van de organisatie" en verhoging van de acceptatiegraad bij de, bij de doorlichting betrokken, medewerkers.

2) Bij deze doorlichting zal veelal een beroep gedaan moeten worden op externe deskundigheid, enerzijds voor de verzameling van gegevens (bijvoorbeeld via monitorprogramma's) en anderzijds omdat voor een juiste analysering en interpretering van die gegevens - bij ontbreken van algemeen bekende en aanvaarde normen - ervaringsgegevens van soortgelijke rekencentra van groot belang zijn. Niet in het minst met het oog op het leereffect zullen interne functionarissen een nuttige rol in de doorlichting kunnen spelen.

3) Zolang aan de onafhankelijkheidseis voldaan wordt en de interne functionarissen kwalitatief van voldoende niveau zijn, kan deze doorlichting heel wel intern geschieden. Wordt een van beide voorwaarden niet vervuld, dan zal een beroep op externe deskundigen gedaan moeten worden.

4) Hier geldt hetzelfde als bij noot 3. Indien in een organisatie een "security-officer" werkzaam is, dan zou deze doorlichting onder zijn supervisie kunnen geschieden.

- tijdige (tussentijdse) terugkoppeling opdat geen overvaleffect ontstaat;
- bij gemengde externe/interne teams duidelijke afspraken met betrekking tot verantwoordelijkheiden;
- zorgvuldige teamsamenstelling; de kwaliteit van de onderzoekers moet boven alle twijfel verheven zijn;
- toekomstgerichte opstelling; het is immers de bedoeling dat het morgen beter gaat.

9 Tot slot

Een EDP-audit zoals hierboven omschreven is in principe een eenmalige aangelegenheid. Daardoor zijn de conclusies en aanbevelingen vaak drastisch van aard en is invoering daarvan een niet gering karwei. Veel beter ware het dat auditing een element is van de normale bedrijfsvoering, bijvoorbeeld als onderdeel van een kwaliteitsprogramma. Bij kwaliteitsprogramma's is toetsing een essentieel onderdeel. Betrokkenen weten wat er te wachten staat en kunnen dus niet (onaangenaam) verrast worden. Audits zullen dan veelal door interne medewerkers worden verricht. Evengoed is het dan van tijd tot tijd verstandig om eens door een externe, onafhankelijke bril het eigen functioneren te laten bekijken. Als het goed is, heeft dan de auditor de vriendenrol. Hij stelt immers nog eens vast dat "alles prima voor elkaar is".

Drs. F.J.G. Fransen studeerde Bedrijfseconometrie in Tilburg. Hij was onder meer werkzaam bij ENKA/AKZO, GITP/ adviseur personeel en organisatie en - als adjunct-directeur financiën en beheer - bij BASF-Nederland. Sinds 1988 werkt hij bij Neddata, het zelfstandige automatiseringshuis van Nedlloyd, waar hij thans algemeen directeur is.

Drs. P.J.A. Lekkerkerker
Directeur Financiën Shell Nederland BV

EDP-audit: iets bijzonders?

De titel van dit artikel is niet gekozen met de achterliggende gedachte: "Daar kan ik nog alle kanten mee op". Nee, op de vraag die besloten ligt in deze titel, wordt onderstaand wel degelijk ingegaan.
De titel is mede ingegeven door de komst van een toch wel specialistisch vakblad (als ik het zo mag stellen) en dat in een tijd waarin Shell Nederland BV druk bezig is EDP-audit als een normaal onderdeel van het audit-proces te beschouwen.

1 Ondernemingsschets

Shell Nederland BV is een onderdeel van de Koninklijke/Shell Groep en bestuurt een aantal Shell-werkmaatschappijen in Nederland.
Deze werkmaatschappijen zijn onder andere:
- Nederlandse Aardolie Maatschappij BV voor exploratie en winning van olie en gas in Nederland en op het Nederlandse Continentale plat (50% Shell, 50% Esso);
- Shell Nederland Raffinaderij BV voor de verwerking, opslag en doorvoer van ruwe olie en olieprodukten;
- Shell Nederland Chemie BV voor de vervaardiging en verkoop van chemische produkten op basis van aardolie;
- Shell Nederland Verkoop Maatschappij BV voor de verkoop van aardolieprodukten en aanverwante produkten en diensten.

Naast het bestuur van deze werkmaatschappijen heeft Shell Nederland bovendien een coördinerende functie voor het beleid ten aanzien van personeel, financiën, omgevingsvraagstukken en public affairs ook ten behoeve van een aantal andere Nederlandse Shell-maatschappijen, waaronder:
- Shell Tankers BV;
- Shell Research BV met laboratoria in Amsterdam en Rijswijk; en
- het Centraal Kantoor van Shell in Den Haag, de zetel van enkele dienstverlenende maatschappijen van de Koninklijke/Shell Groep.

Kenmerkend voor Shell, ook in Nederland, is de decentrale organisatie van de bedrijfsvoering met een grote mate van autonomie voor de werkmaatschappijen en de bedrijfseenheden daarin. Centrale coördinatie vindt slechts plaats waar dit strikt noodzakelijk en profijtelijk is.

De organisatie van de informatievoorziening

Deze organisatorische opzet geldt met name ook voor de informatievoorziening, waarbij de autonome bedrijfseenheden ook hiervoor een directe lijnverantwoordelijkheid hebben.
Deze bedrijfseenheden hebben elk hun eigen zogenaamde Informatie en Organisatie (IO) afdeling, die uitvoering moet geven aan de informatieplannen, en de specificatie van informatiesystemen en van gegevensstructuren.
Daarnaast zijn er organisaties voor de meer centrale Informatie Technologie (IT) faciliteiten en diensten, zoals voor het bouwen van applicaties, voor data processing en telecommunicatie. De term IT wordt tegenwoordig binnen Shell gebruikt voor het integrale scala van computerapparatuur, programmatuur communicatienetwerken en het opereren daarvan.
In het bijzonder hebben we in Nederland een facilitair bedrijf voor data processing, data-opslag en communicatie, waar alle onderdelen van Shell in Neder-

land gebruik van (kunnen) maken. Organisatorisch is dit bedrijf bij Shell Nederland BV ondergebracht.

Voor de noodzakelijke cohesie en mogelijkheid van integratie op het IT-gebied zijn er vrij kleine beleidsafdelingen op centraal niveau, bemand met ervaren medewerkers. Deze afdelingen houden zich vooral bezig met methoden en standaards voor de IT-infrastructuur en voor het bepalen van gegevensstructuren die meerdere bedrijfseenheden aangaan.

2 Beleidspunten voor de besturing van de informatievoorziening

Een goede sturing is nodig als we letten op de toenemende afhankelijkheid van de informatiesystemen en de groeiende kosten van informatietechnologie. Daarbij komt ook het strategische belang om door middel van de toepassing van IT een voorsprong op de concurrentie te verkrijgen of te behouden.

Een belangrijk management-principe dat wij hanteren is: "De justificatie van alle investeringen (waarin begrepen de IT-investeringen) en de realisatie van de baten is een lijnverantwoordelijkheid". Dit houdt in dat de eindverantwoordelijkheid duidelijk gelegd is bij het management van de werkmaatschappijen en de bedrijfseenheden.
Onderkend wordt, dat het effectief besturen van het gebruik van Informatie Technologie een lastige zaak is, waar nog niet alle managers evenveel ervaring mee hebben. In dit verband zeg ik wel eens dat Informatie Technologie uit de puberteit groeit en volwassen aan het worden is. In zo'n overgang moeten ouders zich ook aanpassen.
Binnen Shell trachten wij dit proces te begeleiden door voor managers een aantal belangrijke richtlijnen helder en duidelijk op een rijtje te zetten en veel aandacht te geven aan de praktische invulling daarvan.
Ik wil enkele van die richtlijnen hier noemen:

- IT-plannen moeten worden ontwikkeld als een integraal deel van het bedrijfsplan, en worden als zodanig opgenomen in het zogenaamde Country Business Plan, waarover ook jaarlijks verantwoording wordt afgelegd.

- De planning van de informatievoorziening moet voor elke werkmaatschappij worden vastgelegd en up-to-date gehouden in een informatieplan. Dit plan bevat onder andere:
  - een beoordeling in hoeverre de huidige informatiesystemen voldoen aan de behoeften van het bedrijf;
  - een taxatie van de technische kwaliteit van de systemen en de IT-infrastructuur;
  - een beoordeling waar mogelijkerwijs nieuwe IT-toepassingen de bedrijfsdoelstellingen en -strategie beter kunnen ondersteunen;
  - een complete lijst van investeringsvoorstellen voor IT-toepassingen en infrastructuur, met bijbehorende kosten, baten, risico's en prioriteiten;
  - een implementatieplan, met de benodigde organisatie en middelen.

- Het gebruik van reeds beschikbare applicatie-software (elders binnen Shell ontwikkeld of van derden) dient uitputtend te worden onderzocht, voordat eigen systeemontwikkeling wordt overwogen.

- Investeringsvoorstellen voor informatiesystemen of voor de IT-infrastructuur moeten net als andere investeringsvoorstellen volgens binnen Shell gangbare procedures worden beoordeeld.

- Alle werkmaatschappijen dienen maatregelen te nemen en deze periodiek te beproeven met betrekking tot informatiebeveiliging en de continuïteit van de bedrijfsvoering in geval van calamiteiten.
  In ons geval, waar verschillende werkmaatschappijen gebruik maken van hetzelfde facilitair bedrijf, is het dus zaak dat naast de technische invulling bij het data center, er met name ten aanzien van de procedures en de discipline om de procedures te volgen een management-verantwoordelijkheid bestaat voor die verschillende werkmaatschappijen. Dus ook ten aanzien van dit aspect geldt: IT is een lijnverantwoordelijkheid.

3 De rol van (EDP-)audit

In het voorgaande heb ik aangegeven dat binnen Shell de term IT wordt gehanteerd; de term EDP (Electronic Data Processing) wordt niet gebruikt. Het ligt dus voor de hand de term EDP-audit te vervangen door IT-audit. Merkwaardigerwijs wordt bij ons dan ineens weer ge-

sproken van "computing audit". Ik neem aan dat in het kader van dit artikel het gebruik van beide termen niet tot verwarring behoeft te leiden.

Echter, alvorens op computing audit verder in te gaan, wil ik graag nog een opmerking van meer algemene aard maken. Binnen Shell is het de verantwoordelijkheid van het management van iedere Groepsmaatschappij om een adequaat systeem van beheersmaatregelen op te zetten en te handhaven. Dit systeem dient zodanig te functioneren, dat mede met behulp hiervan op de beste manier wordt bijgedragen om de maatschappijdoelstellingen te realiseren. Deze maatregelen dienen alle activiteiten te omvatten, dus zowel operationele, technische, commerciële als administratieve. Voorts worden duidelijke eisen aan deze maatregelen zelf gesteld. Zij dienen bijvoorbeeld volledig en consistent te zijn, uit oogpunt van kosten doeltreffend en doelmatig, en in overeenstemming met wetten en andere regelgeving.

Als aanvulling op dit proces van besturing en beheersing van activiteiten is een belangrijke plaats toegekend aan audits. In dit artikel wil ik wat dieper ingaan op de rol van Internal Audit. Onder Internal Audit wordt bij Shell verstaan de onafhankelijke en systematische beoordeling van de beheersmaatregelen die een bedrijfseenheid heeft getroffen. Het doel van dit soort audits is te komen tot een opinie over de kwaliteit van de beheersmaatregelen als geheel binnen een bepaald gebied van onderzoek. Hierbij is het van groot belang, dat tekortkomingen met betrekking tot bepaalde maatregelen worden geïdentificeerd en gerapporteerd aan de hoogste leiding van dat bedrijfsonderdeel. Ik doel hier op zwakheden, die bijvoorbeeld kunnen leiden tot het lopen van onaanvaardbare risico's of tot het verspillen van aangewende middelen. In voorkomende gevallen worden vervolgens aanbevelingen gedaan voor verbetering van de kwaliteit van de "instrumenten". Hierbij is tevens van belang dat er overeenstemming wordt bereikt met de auditee over de acties die zullen worden ondernomen.

Uit het voorgaande moge duidelijk geworden zijn, dat in ons denken computing audits ofwel EDP-audits tot het takenpakket van Internal Audit worden gerekend.

Hierbij onderkennen we in het algemeen drie soorten computing audits.

1 Een onderzoek naar de kwaliteit van een operationeel informatiesysteem, meestal als onderdeel van een audit van een organisatie of bedrijfsproces.
In dit geval wordt ten aanzien van het informatiesysteem een oordeel gegeven over onder andere:
   - de toegevoegde waarde aan het bedrijfsdoel;
   - de functionele en technische kwaliteit;
   - de procedures;
   - de controles op invoer, uitvoer, verwerking, bestanden, enz.;
   - de verantwoordelijkheden voor beheer en operatie;
   - de beveiliging en de continuïteit.

2 Een audit van een organisatie of een afdeling, waarvan het primaire doel het leveren van IT-diensten en -faciliteiten betreft. Men denke hierbij aan rekencentra, communicatienetwerken, interne softwarebureaus, en dergelijke.
Hierbij kan audit te maken krijgen met opdrachten ten aanzien van:
   - beleid en organisatie;
   - planning en evaluatie;
   - financiering en doorbelasting;
   - service-contracten;
   - prestatienormen en verslaggeving;
   - beveiliging en continuïteit.

3 Een kwaliteitsoordeel over de beheersinstrumenten voor een project, bijvoorbeeld de ontwikkeling van een informatiesysteem of een infrastructurele IT-voorziening.
Het is binnen Shell niet gebruikelijk dat Internal Audit zich intensief bemoeit met de inhoudelijke kwaliteit van een project. De verantwoordelijkheid voor de uitvoering van dit soort projecten ligt bij de projectleider en zijn team.
Voor de sturing van projecten van enige omvang wordt een stuurgroep geformeerd, onder voorzitterschap van de budgetverantwoordelijke lijnmanager van het juiste niveau. Deze manager is bijna altijd de "eigenaar" van het eindprodukt van het project. Hij of zij is verantwoordelijk voor het beheer en voor de realisatie van de baten van dit produkt. Bewaking van de kwaliteit van het project is in de eerste plaats een zaak van de projectleider en de bij de uitvoering betrokken organisaties.

Slechts in incidentele gevallen is er sprake van een onafhankelijke project audit, waarbij Internal Audit een goede rol kan spelen. Ook kan Internal Audit worden verzocht een advies te geven over het raamwerk van controles en de beveiliging van een IT-systeem dat in ontwikkeling is. In voorkomende gevallen wordt ervoor gewaakt dat Audit geen lijntaken uitvoert.
Overigens is het belangrijk zich te realiseren dat gedurende het tijdsverloop van een project de kosten oplopen, maar daarentegen de mogelijkheden voor effectieve managementsturing afnemen. Dit pleit voor extra aandacht van het management in het beginstadium van een project, met name tijdens het toepasbaarheidsonderzoek.

Verdiepen we ons in de vraag hoe binnen Shell wordt gedacht over de bemanning van de Internal Audit Afdeling (helaas is be"vrouw"ing van Audit bij ons nog onvoldoende), dan blijkt dat Audit niet meer wordt gezien als een afdeling waarin men als specialist carrière bij Shell kan maken. Zij wordt eerder beschouwd als een plaats voor management-training. Na een aantal jaren werkzaam te zijn geweest in een bedrijfsfunctie als marketing, logistiek, financiën, informatievoorziening, research, procestechnologie, etc., kan men voor ongeveer drie jaar in aanmerking komen voor een audit-positie.
Vanzelfsprekend zal de bedrijfskennis en -ervaring van pas komen, maar zal een aanvulling van kennis op het gebied van audit vaak noodzakelijk zijn. Daarnaast zal vandaag de dag een aanvulling van kennis ten aanzien van de IT-aspecten nodig zijn, tenzij de kandidaat zelf uit deze discipline voortkomt.

Gewapend met deze kennis, en de mogelijkheid tot het inroepen van specialisten, wordt de algemene auditor in staat geacht een onderzoek te doen naar een operationeel informatiesysteem (als onderdeel van een bedrijfsfunctie) of een ontwikkelingsproject.
Uiteraard zal voor operationele audits van onder andere rekencentra, meer IT-specialistische kennis en ervaring benodigd zijn. Maar dat geldt mutatis mutandis voor operationele audits van bijvoorbeeld een stoomkraker in chemie ook. Kortom, de benodigde IT-kennis en -ervaring is voor de drie zojuist genoemde soorten audits verschillend.

Dit leidt ons dan terug naar de vraag of EDP-audit iets bijzonders is. Shell Nederland was er vroeg bij met de oprichting van een specifieke EDP-audit discipline in het begin van de zeventiger jaren. Inmiddels is deze EDP-audit discipline weer volledig geïntegreerd in de Internal Audit Afdeling, waarbij elke auditor wordt geacht de meeste opdrachten met EDP-aspecten te kunnen uitvoeren. In die gevallen waarbij een diepgaande IT-kennis en -ervaring noodzakelijk wordt geacht, zal er een auditor worden genomineerd met die achtergrond, of zullen er specialisten uit de IT-vakdiscipline worden ingeroepen. Ook dit is, zoals eerder gezegd, weinig bijzonder: de audit-functie binnen Shell Nederland houdt zich ook bezig met opdrachten in andere vakdisciplines, zoals de winning van olie en gas, de raffinage en distributie van olieprodukten, en dergelijke.

Ik heb al eerder gezegd: IT is zo langzamerhand de puberteit ontgroeid en volwassen geworden, zij het wellicht met wat minder levenservaring dan de andere "takken van sport" waarin we ons bewegen. Opvoeding blijft zo nu en dan nodig. In zijn algemeenheid echter verdient IT ook qua audit dezelfde benadering als andere (ondersteunende) processen van onze Maatschappij.

Kortom: mijn conlusie luidt: er is niets nieuws onder de zon.

Drs. P.J.A. Lekkerkerker studeerde wiskunde aan de Universiteit van Utrecht. Zijn loopbaan kenmerkt zich door het feit dat hij binnen één organisatie (Shell) tal van verschillende (management-)functies heeft bekleed. Per 1 februari van dit jaar werd de heer Lekkerkerker benoemd tot Directeur Financiën van Shell Nederland B.V.

Drs. N.J. Krever
Lid Hoofddirectie
Bank Mees & Hope

Beheersing van de automatisering en de rol van EDP Audit bij Bank Mees & Hope

1 Inleiding

In dit artikel geven wij weer op welke wijze binnen Bank Mees & Hope (hierna ten noemen Mees & Hope) de automatisering wordt beheerst.
Allereerst wordt ingegaan op de invloed van informatietechnologie en de visie daarop van Mees & Hope. Vervolgens komt de rol van Automatisering aan de orde. De eisen die Mees & Hope stelt aan automatisering en de wijze waarop zij heeft geregeld dat een continue beheersing plaatsvindt, wordt daarna behandeld. Welke rol EDP Audit binnen Mees & Hope speelt met betrekking tot het totaal complex van beheersingsmaatregelen wordt aangegeven in het volgende gedeelte. Ten slotte worden enkele ontwikkelingen weergegeven op het gebied van automatisering en onze verwachtingen omtrent de wijze waarop de afdeling EDP Audit op deze ontwikkelingen kan inspelen.

2 De invloed van de informatietechnologie

De negentiger jaren zijn de jaren van de informatierevolutie. Juist nu, en dat zal zich in de komende jaren krachtig doorzetten, reikt de informatietechnologie ons nieuwe mogelijkheden aan. Enerzijds heeft deze technologie grote invloed op de interne organisatie van bedrijven, en zal wellicht aanpassingen binnen deze bedrijven dwingend opleggen. Anderzijds creëert zij nieuwe commerciële mogelijkheden, waarbij informatie als produkt kan worden beschouwd. De partij die over de juiste informatie beschikt en deze bovendien ter beschikking kan stellen aan haar handelspartners heeft de business. Door een juiste en goed gedoseerde toepassing van informatietechnologie kan de concurrentiekracht van het bedrijf worden vergroot. Via samenwerking met leveranciers (andere financiële instellingen en bedrijven die specifieke kennis of produkten inbrengen) tracht Mees & Hope de beschikking te verkrijgen over krachtige (informatie)produkten.
Wellicht nog belangrijker is de samenwerking met cliënten, waarbij het inspelen op de informatiebehoeften van de cliënt en het realiseren van een op hem afgestemde informatievoorziening van essentieel belang is.
Juist door het tot stand brengen van een electronische "link" wordt de band met de cliënt verstevigd en zal hij bereid zijn eerder business te gunnen aan zijn electronische business partner.

Mees & Hope wil in de markt herkend worden als een professionele kwaliteitsbank, die geen produkten, maar tailormade probleemoplossingen aandraagt, en zich onderscheidt door creativiteit, initiatief en integriteit. Dit beeld wordt ondersteund door een adequate informatievoorziening naar de cliënten, hetgeen wij beschouwen als een van de critical success factoren.

Teneinde de genoemde ontwikkelingen met betrekking tot de interne en externe informatievoorziening in goede banen te leiden is binnen Mees & Hope een start gemaakt met de ontwikkeling van het informatiebeleid.
Dit informatiebeleid is direct afgeleid van de strategische doelstellingen van de bank, waarbij een relatie tussen de interne en externe informatievoorziening expliciet wordt onderkend. Beide vormen van informatievoorziening dienen zo optimaal mogelijk op elkaar te worden afgestemd. De behoefte van de cliënt be-

paalt uiteindelijk de vorm en inhoud van de externe informatiestroom. De interne informatievoorziening richt zich zowel op een optimale invulling van onze informatierol naar buiten toe als op een adequate informatievoorziening ten behoeve van de interne bedrijfsprocessen.

3 Automatisering bij Mees & Hope

Mees & Hope beschouwt de afdeling Automatisering als een afgeleide functie van het informatiemanagement, maar met een duidelijk zelfstandige rol en een eigen verantwoordelijkheid. Enerzijds treedt de afdeling Automatisering op als facilitator voor de bouw van geautomatiseerde systemen. Anderzijds is zij verantwoordelijk voor het creëren van de technische infrastructuur, op een zodanige wijze dat wensen of eisen vanuit het informatiemanagement op een effectieve en doelmatige wijze kunnen worden gehonoreerd.

Binnen Mees & Hope is een hoge graad van automatisering bereikt.
De zeventiger jaren kenmerken zich vooral door automatisering van de interne verwerkingsprocessen en de administratie van de bank, met als doel een efficiënte verwerking tegen lage kosten. In de tachtiger jaren heeft de automatiseringsinspanning zich veel meer verplaatst naar de front-office. Als doelstelling gold het voorzien in kwalitatief hoogstaande informatie ter ondersteuning van de primaire processen (de commerciële dienstverlening) tegen aanvaardbare kosten. In de negentiger jaren zal de trend van de front-office automatisering worden voortgezet en zal worden gestreefd naar interne integratie van systemen. Tevens zal de inspanning zich meer en meer richten op het tot stand brengen van externe integratie met leveranciers en cliënten.

De automatiseringstechnische infrastructuur moet zodanig zijn dat de hiervoor geschetste toekomstige ontwikkelingen op een soepele wijze kunnen worden ingepast en gerealiseerd. Hiertoe is het triplex-model ontwikkeld. Dit model onderscheidt drie niveaus van gegevensverwerking: het centraal, het decentraal en het lokaal niveau. Het lokale niveau betreft de gegevensverwerking op een PC waarbij de informatie uitsluitend van belang is voor de individuele medewerker. Het decentraal niveau betreft de informatievoorziening die uitsluitend voor meerdere medewerkers binnen een afdeling van belang is. Het centraal niveau ten slotte betreft de gegevensverwerking en informatievoorziening voor zover het belang daarvan uitstijgt boven dat van de afdeling. De gebruiker heeft binnen het triplex-model uitsluitend te maken met de inbreng van gegevens en de opvraag van informatie, waarbij het voor hem transparant is op welk niveau de gegevensverwerking en de informatievoorziening plaatsvindt. Binnen dit model worden faciliteiten beschikbaar gesteld waardoor eindgebruikers in staat zijn zonder of slechts met geringe tussenkomst van Automatisering zelf in hun informatiebehoeften te voorzien.
Aan cliënten kan via het centraal niveau informatie ter beschikking worden gesteld die op lokaal of decentraal niveau is opgebouwd.

4 Beheersing van de kwaliteit van informatie

Mees & Hope stelt hoge eisen aan de kwaliteit van de informatie. Dit betreft onder meer de functionaliteit hiervan alsmede de interne controle en beveiliging.

Hiervoor is reeds de eis die Mees & Hope stelt aan de functionaliteit beschreven: de functionele specificaties van de op te leveren informatie moeten passen binnen de strategische doelstellingen van de bank, waarbij de externe informatiestroom moet zijn gebaseerd op de behoeften van de cliënt, terwijl de interne informatievoorziening enerzijds zo optimaal mogelijk daarop is afgestemd en anderzijds gericht is op de besturing van de interne organisatie.

In het kader van dit artikel gaan wij nader in op de eis van interne controle en beveiliging. Mees & Hope stelt de eis dat informatie betrouwbaar (en actueel) moet zijn, dat de informatie beschikbaar moet zijn binnen een bepaalde tijdsspanne en dat de vertrouwelijkheid van de informatie gewaarborgd is. Om waarborgen te verkrijgen dat bij voortduring aan deze eisen wordt voldaan, betekent dit dat impliciet ook eisen worden gesteld aan de operationele geautomatiseerde gegevensverwerking en informatievoorziening, alsmede aan de veranderingsprocessen die invloed hebben op de operationele verwerking. Deze eisen zijn afgeleid van de aan informatie gestelde eisen. Zo wordt bijvoorbeeld ten aanzien van de operationele verwerking in het kader van de betrouwbaarheid van informatie als eis gesteld dat de gege-

vens slechts mogen worden gemuteerd via daartoe ter beschikking staande applicaties en uitsluitend door personen die uit hoofde van hun functie daarvoor in aanmerking komen. Voorts dienen binnen de operationele verwerking waarborgen aanwezig te zijn dat de inbreng en verwerking juist, volledig en tijdig geschiedt en dat deze controleerbaar is. Onder operationele verwerking rekenen wij de automatiseringsorganisatie, inclusief de technische infrastructuur en programmatuur, alsmede de wijze waarop de gebruikersorganisatie hiermee omgaat.

De zorg voor de invulling van de kwaliteitseisen ligt bij de direct betrokkenen en is een lijnverantwoordelijkheid. Bij Mees & Hope is het voldoen aan de kwaliteitseisen één van de randvoorwaarden bij de opzet en werking van alle processen die, hetzij direct, hetzij indirect, de geautomatiseerde gegevensverwerking kunnen beïnvloeden.
De praktische invulling van dit alles vinden wij terug in het genoemde informatiebeleid, het beveiligingsbeleid, de organisatiestructuur van de bank, de gehanteerde procedures, de technische infrastructuur, de toegepaste methoden en middelen voor systeemontwikkeling, etc.
Daar waar noodzakelijk en mogelijk worden procedures zoveel mogelijk technisch afgedwongen.

Als voorbeeld moge het onderhoud van programmatuur dienen. Drie partijen zijn hierbij betrokken: het Rekencentrum, de afdeling Systeembouw en de gebruikersorganisatie. Ieder heeft een eigen verantwoordelijkheid met betrekking tot respectievelijk produktie, ontwikkeling en acceptatie.
De procedure die wordt gehanteerd, richt zich op de blijvende juistheid van programmatuur. Deze procedure wordt technisch ondersteund door een geautomatiseerd systeem, waarin voor elk van de drie partijen logisch gescheiden omgevingen zijn onderkend: de produktieomgeving, de ontwikkelomgeving en de acceptatie-omgeving. Tevens is een tussenomgeving gecreëerd, waarlangs iedere overdracht van en naar de drie omgevingen plaatsvindt. Op deze wijze worden zes verplicht te doorlopen fasen (de processen) voor de overdracht van programmatuur onderkend en is gecontroleerd onderhoud mogelijk. Via het toegangsafschermend systeem RACF worden zowel de verschillende omgevingen als het gebruik van de processen afgeschermd. Ook de ontwikkeling van nieuwe systemen wordt via dit mechanisme geleid. Naast programma's wordt ook het onderhoud van andersoortige objecten (waaronder documentatie) ondersteund door dit mechanisme. Ook toekomstige ontwikkelingen mogen geen inbreuk plegen op het principe van gecontroleerd onderhoud van programmatuur. Zo zullen bij de inzet van DB2 binnen ditzelfde mechanisme faciliteiten worden ontwikkeld voor de overdracht van specifieke DB2-objecten.

De eisen van interne controle en beveiliging die wij stellen ten behoeve van de interne bedrijfsvoering zijn dermate strikt dat deze ook tegemoet komen aan eisen die diverse externe instanties stellen aan de geautomatiseerde gegevensverwerking:
- De Nederlandsche Bank, die eisen stelt aan de geautomatiseerde gegevensverwerking bij banken in het kader van haar toezichthoudende taak;
- de Wet op de Privacy en de daaruit geformuleerde gedragscode, waaruit eisen voortvloeien ten aanzien van de geautomatiseerde gegevensverwerking en informatievoorziening;
- assuradeuren, die eisen stellen bij het aangaan en de continuatie van fraudeverzekeringen.

5 De functie EDP Audit bij Mees & Hope

Voor het realiseren van de kwaliteitseis die is gesteld met betrekking tot informatie draagt de hoogste leiding de eindverantwoordelijkheid.
Via het delegatieproces wordt binnen Mees & Hope hieraan invulling gegeven. Dit ontslaat de hoogste leiding echter niet van het zich zelfstandig een oordeel vormen omtrent de opzet en de werking van het stelsel van getroffen beheersingsmaatregelen. Antwoord moet worden verkregen op de vraag in hoeverre dit stelsel evenwichtig en toereikend is voor de verwezenlijking van de kwaliteitsdoelstelling.

Voor de vorming van dit oordeel laat de leiding zich bijstaan door een van de lijnorganisaties onafhankelijk deskundige. De afdeling EDP Audit is hiermee belast. De ondernemingsleiding verwacht van deze afdeling dat zij eventuele onvolkomenheden in de opzet en de werking van het complex van beheersingsmaatregelen tijdig signaleert, de daaruit voort-

vloeiende risico's meldt en adviseert ten aanzien van alsnog te treffen maatregelen.
De afdeling EDP Audit maakt deel uit van de Interne Accountantsdienst.
De Interne Accoutantsdienst van Mees & Hope heeft ten aanzien van de interne jaarrekening een certificerende functie. Ten behoeve van deze certificering zal de IAD zich onder meer een oordeel moeten vormen over de opzet en de werking van de geautomatiseerde gegevensverwerking. Bij Mees & Hope is de EDP Audit-functie binnen de IAD vanuit deze behoefte ontstaan. De onafhankelijkheid van de EDP Audit is gewaarborgd doordat de IAD ressorteert onder de hoogste leiding en daardoor onafhankelijk is van de lijnorganisatie.

In de dagelijkse praktijk neemt de adviserende rol een steeds grotere plaats in. Dit geldt voor de IAD in het algemeen en de EDP Audit in het bijzonder. Dit is niet zo verwonderlijk, omdat, indien risico's worden gelopen, de ondernemingsleiding dit vooraf wil weten om bewust een beslissing te nemen voor het al dan niet accepteren van deze risico's.
In concreto houdt dit in dat de afdeling EDP Audit vooraf bij nieuwe ontwikkelingen wordt betrokken. Zij denkt mee over mogelijk te treffen maatregelen en adviseert daarover. Als norm hanteert zij daarbij de kwaliteitseis die is gesteld aan informatie.

6 Toekomstige ontwikkelingen ten aanzien van automatisering

De in gang gezette automatisering binnen Mees & Hope zal zich in de toekomst in versneld tempo voortzetten. Dit is enerzijds het gevolg van het feit dat de omgeving in versneld tempo eisen stelt aan de bank, terwijl anderzijds ook de technologische ontwikkelingen zich steeds frequenter aandienen. Deze veranderingen uiten zich onder meer in een reeds doorgevoerde wijziging van onze organisatiestructuur, de grotere behoefte aan ad hoc-informatie, het gebruik van nieuwe transactievormen, de behoeften die de cliënt nu en in de toekomst heeft ten aanzien van informatie-uitwisseling en de informatieplicht aan De Nederlandsche Bank. Hierna bespreken wij in het kort enkele ontwikkelingen. In de volgende paragraaf zullen de gevolgen daarvan voor de inspanning van EDP Audit worden aangegeven.

De wijziging van de organisatiestructuur heeft gevolgen voor automatisering. Zodra bedrijfsonderdelen worden verzelfstandigd tot business units moeten instrumenten worden gehanteerd om de resultaten van deze units te meten. Eén van deze instrumenten is een toegespitste profit-center-gewijzigde administratie met toedelingscriteria voor de kosten en de opbrengsten. De automatisering van een dergelijke administratie vereist een aanzienlijke inspanning. Ook informatie over processen en beslissingsvoorbereidende informatie zal per business unit moeten worden vervaardigd.

De tendens is aanwezig dat Mees & Hope steeds meer te maken zal krijgen met behoefte aan nieuwe informatie die direct ter beschikking moet staan en waarvan de verwachting is dat de daarvoor ontwikkelde software slechts een beperkte levensduur zal hebben. De ontwikkelafdeling binnen Automatisering zal daarom de beschikking moeten hebben over geavanceerde hulpmiddelen waarmee het ontwikkelen van software snel en efficiënt kan geschieden. Daarnaast worden aan de gebruikers faciliteiten geboden om op flexibele wijze informatie op te vragen en naar verschillende invalshoeken te rangschikken of te presenteren.

Het is onze stellige overtuiging dat onze cliënten zich meer en meer zullen begeven op het terrein van Electronic Data Interchange (EDI). Dit vereist van Mees & Hope een aanzienlijke automatiseringsinspanning. De reeks van produkten die momenteel aan cliënten wordt aangeboden op het gebied van electronic banking zal worden uitgebouwd. Tevens zal uniformering en integratie van de afzonderlijke produkten plaatsvinden. Hierbij zullen diverse nieuwe technieken worden gebruikt. Daarnaast zullen maatregelen moeten worden getroffen om in de toekomst, naast de strikt bancaire rol op het gebied van de financiële informatievoorziening, ook betrokken te worden bij de berichtenuitwisseling ten aanzien van goederenstromen tussen handelspartijen.

7 Toekomst van EDP Audit

Van de afdeling EDP Audit verwachten wij dat zij direct inspeelt op bovengenoemde veranderingen in de automatiseringsstructuur.
Het is uit beheers- en kostenoverwegingen van belang dat zij in een vroeg stadium wordt betrokken bij nieuwe ontwik-

kelingen op automatiseringsgebied om tijdig vanuit haar specifieke deskundigheid op het gebied van de interne controle en beveiliging een adviserende rol te spelen.
Wij realiseren ons dat door de toenemende complexiteit en automatiseringsgraad het steeds moeilijker zal zijn het vooraf gestelde niveau van interne controle en beveiliging te bewaren. Toch willen wij dit niveau binnen Mees & Hope handhaven. Uitgaande van een gedegen risico-analyse zal een kosten/nut-afweging moeten worden gemaakt van te treffen maatregelen. Het gaat hierbij vooral om op inventieve en creatieve wijze een efficiënte oplossing te vinden die voldoet aan de betrouwbaarheids- en beveiligingseisen. Van de afdeling EDP Audit verwachten wij dat zij een positieve bijdrage levert om dit doel te bereiken.

Het ter beschikking stellen van nieuwe faciliteiten zal vaak tot gevolg hebben dat nieuwe risico's worden gelopen. Evenzo geldt dit voor het geven van faciliteiten aan andere gebruikers, waaronder derden. Wij geven enkele voorbeelden:

- Het ter beschikking stellen van programmeer- en opvraagfaciliteiten impliceert, dat wordt afgeweken van de huidige standaard dat gebruikers slechts via strikt gereguleerde programmatuur gegevens kunnen opvragen en wijzigen. Onderscheid moet nu worden gemaakt tussen enerzijds gegevens waarvoor deze standaard gehandhaafd blijft en anderzijds gegevens waarover de gebruiker vrijelijk mag beschikken. De structuur van logische afscherming dient hierop te worden aangepast.
- De geplande uitbreidingen op het gebied van elektronische berichtenuitwisseling met cliënten noodzaken dat kritisch moet worden gekeken naar de wijze waarop Mees & Hope de authenticiteitscontrole en de lijnbeveiliging voor de toekomst zal regelen.
- De aanpassing van de technische infrastructuur heeft een herstructurering van de bestaande verantwoordelijkheidsstelling tot gevolg, evenals een aanvulling op bestaande procedures. Op grond daarvan zal een complex van eisen worden geformuleerd dat moet worden gesteld aan de technische infrastructuur.

Van de afdeling EDP Audit verwachten wij dat zij actief zal participeren in deze en alle hier niet genoemde ontwikkelingen. Uit het voorgaande moge duidelijk zijn dat naarmate binnen Mees & Hope de automatisering verder voortschrijdt ook de participatie van EDP Audit steeds belangrijker en noodzakelijker zal worden voor het bedrijf en de Interne Accountantsdienst. In de toekomst zal de afdeling EDP Audit wellicht ook worden ingeschakeld bij andersoortige onderzoeken, zoals onderzoeken naar de efficientie en de effectiviteit van systemen.

Niet alleen bij Mees & Hope zal de rol van EDP Audit toenemen, maar ook bij vele andere bedrijven zal dit het geval zijn. De volgende voorbeelden dienen ter illustratie:

- Steeds meer functionaliteit, die voorheen via de applicaties moest worden geregeld, zal worden gelegd in de besturingsprogrammatuur.
  Een programmeur behoeft daardoor steeds minder rekening te houden met de omgeving waarbinnen de applicatie zal draaien. Een fout in een applicatie heeft slechts gevolgen voor die ene applicatie. Een fout of een verkeerde parameter-setting van de systeemprogrammatuur heeft echter gevolgen voor elke applicatie die gebruik maakt van deze systeemprogrammatuur. Gegeven de risico's zal men daardoor eerder neigen tot beoordeling van de systeemprogrammatuur, waarvoor de deskundigheid van een EDP-auditor is vereist.
- Bij de voorbereidingen tot aanpassing van de wetgeving op het gebied van computercriminaliteit wordt overwogen het bestuur van de onderneming een mededeling te laten opnemen in het jaarverslag omtrent de maatregelen in verband met de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. De controlerend accountant moet deze mededeling betrekken bij de certificering van de jaarrekening.
  Afhankelijk van de automatiseringsgraad van het desbetreffende bedrijf zullen werkzaamheden moeten worden verricht, waarvoor de inzet van een EDP-auditor is vereist.

8 Samenvatting en conclusie

"The information revolution is changing the nature of competition". De partij die de juiste informatie ter beschikking kan stellen aan haar cliënten, zal zaken naar zich toe kunnen trekken. De interne informatievoorziening zal hierop moeten

zijn afgestemd, alsmede op de interne sturing van de organisatie. In dit kader heeft Mees & Hope reeds een hoge graad van automatisering bereikt. Dit houdt tevens in dat de processen binnen Mees & Hope sterk afhankelijk zijn van het goed functioneren van de geautomatiseerde gegevensverwerking. De verwachting is dat, gegeven de reeds in gang gezette ontwikkelingen, deze afhankelijkheid nog groter zal worden. Het is voor Mees & Hope daarom noodzaak bij iedere ontwikkeling na te gaan of voldaan wordt aan de kwaliteitseis die wij stellen aan informatie. Evenzo geldt dit voor de dagelijkse verwerking van de gegevens. Daarom is een complex van maatregelen getroffen waarbij onder meer de kwaliteitseis wordt gerealiseerd. Deze maatregelen zijn organisatorisch, procedureel of technisch van aard. Om vast te stellen dat dit complex in opzet en in werking voldoende waarborgen geeft dat de kwaliteitseis bij voortduring wordt bereikt, laat de ondernemingsleiding zich bij de beoordeling ervan bijstaan door de afdeling EDP Audit. Naast deze toetsende functie neemt de adviserende functie van de afdeling EDP Audit op het gebied van interne controle en beveiliging een steeds grotere plaats in. Binnen Mees & Hope heeft EDP Audit zeker toekomst. En onze stellige overtuiging is dat dit buiten Mees & Hope ook het geval zal zijn.

Drs. N.J. Krever studeerde Economische Wetenschappen aan de Rijksuniversiteit van Groningen. Hij begon zijn loopbaan bij Philips Gloeilampenfabriek N.V., waarna hij de overstap maakte naar de financiële wereld. Van 1960 tot 1974 was hij werkzaam bij de Amro Bank, daarna bij Bank Mees & Hope NV, waar hij sinds 1 januari 1978 lid van de Hoofddirectie is.

J.J.A. Leenaars RA
Lid Beleidscomité Robeco Groep

EDP-audit: nuttig, zinvol, mogelijk?

In dit artikel komt een drietal min of meer gescheiden onderwerpen aan de orde:
- de invloed van een externe toezichthouder op EDP-auditing binnen een onderneming;
- de invloed van toekomstige ontwikkelingen in automatiseringsland op EDP-auditing;
- de richting waarin EDP-auditing als vak zich zou kunnen ontwikkelen.

1. De invloed van een externe toezichthouder op EDP-auditing

Omdat de Robeco Groep zowel instellingen bedoeld in de Wet Toezicht Kredietwezen als instellingen bedoeld in de Wet Toezicht Beleggingsinstellingen bevat, zal in het navolgende kort worden ingegaan op de rol die toezicht door De Nederlandsche Bank in beide soorten instellingen speelt.

Van groot belang is hierbij onderscheid te maken naar de wijze waarop het toezicht plaatsvindt. Bij instellingen die vallen onder de Wet Toezicht Kredietwezen is sprake van zogenaamd bedrijfseconomisch toezicht. Bij instellingen die bedoeld worden in de Wet Toezicht Beleggingsinstellingen is sprake van toezicht dat marginaal van aard is. Grof gezegd vindt bij bedrijfseconomisch toezicht een materiële controle plaats op zowel beleidsuitgangspunten als beleidsuitvoering, terwijl bij marginaal toezicht alleen toetsing aan een aantal algemene uitgangspunten plaatsvindt.

De rationale achter dit onderscheid is gelegen in het feit dat de wetgever heeft erkend dat bij een bank of een kredietinstelling sprake dient te zijn van zogenaamde crediteurenbescherming: de hoofdsom dient "te allen tijde" terugbetaald te kunnen worden aan de crediteur.
Bij beleggingsinstellingen daarentegen is geen sprake van crediteurenbescherming: een belegger loopt bewust risico over de hoofdsom van de door hem gedane belegging.
De wetgever wil er primair voor zorgen dat een aspirant-belegger adequate informatie wordt verstrekt. (Overigens is ook de goede werking van de kapitaalmarkt een aandachtspunt.)

Toezicht op grond van de Wet Toezicht Kredietwezen

In september 1988 heeft De Nederlandsche Bank een zogenaamd memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen het licht doen zien. DNB hanteert daarbij vanuit haar functie als toezichthouder uiteraard het uitgangspunt dat het gaat om gebeurtenissen die de liquiditeits- en/of solvabiliteitspositie van een instelling wezenlijk kunnen aantasten. De primaire verantwoordelijkheid ligt vanzelfsprekend bij het management van de instelling, waarbij de Bank, meer expliciet dan voorheen, wenst te worden geïnformeerd over de wijze waarop aan de zorg voor betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking inhoud wordt gegeven.

De externe accountant is aangewezen als interface tussen de instelling en DNB. Hij dient zijn controle-opdracht daartoe indien nodig aan te passen en door middel van de jaarlijks uit te brengen management letter verslag te doen van zijn bevindingen. Via de bij elke bank bestaande tripartite overeenkomst tussen de instelling, externe accountant en DNB wordt DNB vervolgens geïnfor-

meerd over de uitslagen van het verrichte onderzoek.

Van belang nu is te onderkennen dat er een parallel bestaat tussen de wettelijke controleplicht van een accountant waar het de jaarrekeningen van grotere ondernemingen betreft en een soort wettelijke EDP-audit voor instellingen die onder de reikwijdte van de Wet Toezicht Kredietwezen vallen. De parallel gaat verder. Evenzeer als bij jaarrekeningen het geval is, is er ter zake van de hier bedoelde maatregelen op het gebied van betrouwbaarheid en continuïteit geen stelsel van normen voorhanden waaraan de aangetroffen actualiteit kan worden getoetst. Evenmin als de waardering van onderhanden werk bij een aannemer op een gestandaardiseerde wijze plaatsvindt, zijn er min of meer aanvaarde normen rondom bijvoorbeeld backup-procedures voorhanden.

De externe accountant wordt dan ook voor een bijzonder zware taak gesteld. Zeker daar waar geen interne accountantsdienst functioneert - hetgeen toch bij een aantal kleinere banken het geval is - dient binnen beperkt beschikbare tijd een oordeel te worden gevormd over niet alleen het ontwerp voor allerlei procedures en organisatorische aspecten maar vooral ook over de naleving daarvan. Hierbij lijkt het accent sneller op een incident te kunnen vallen dan in een jaarrekeningcontrole het geval is. Het komt mij voor dat een aantal audit-technieken ter realisatie van deze doelstelling nog in ontwikkeling is.

Nu geven recente uitspraken van DNB reden om nog enige tijd voor de ontwikkeling van deze technieken aanwezig te achten:
- Van enigszins algemeen aanvaarde normen op het bedoelde gebied is geen sprake.
- De betrokken externe accountants verschillen zeer van mening omtrent de werkingssfeer van verschillende toegepaste maatregelen.
- Tussen de gecontroleerde banken bestaan zeer grote verschillen op het onderhavige gebied. Dit geldt met name de backup-problematiek.

In het genoemde memorandum wordt een belangrijke plaats ingeruimd voor beleid op het gebied van beveiliging.
Als voorbeeld vermeld ik de doelstelling van het beveiligingsbeleid zoals dat ter zake van Roparco door mij is geformuleerd: "Het creëren van zodanige faciliteiten in applicaties, automatiseringsorganisatie en procedures dat de gebruikers *hun* interne controlefunctie kunnen waarmaken.
Dit vertaalt zich in:
- het voorkomen van onopzettelijke fouten;
- het signaleren van opzettelijke fouten;
- het voorkomen van ongeautoriseerde toegang.

Bovengenoemde procedures dienen zoveel mogelijk geautomatiseerd te worden ondersteund.

De uitwerking in controleprogramma's dient binnen het volgende raamwerk te gebeuren:
- organisatie;
- scheiding van test- en produktie-omgeving;
- continuïteit;
- toegangscontrole;
- distributie van uitvoer;
- in applicaties op te nemen geprogrammeerde controles.

Ten slotte dient gedefinieerd te worden op welke wijze in de ontwikkeling van applicaties wordt geparticipeerd."

Op de mogelijke divergentie die hier ligt met het memorandum van DNB waar het gaat om opzettelijke fouten zoals bijvoorbeeld fraude, ga ik hier niet in. Aangetekend zij dat de externe accountant van de Robeco Groep, Coopers & Lybrand Dijker Van Dien, er zich na enige discussie in kon vinden.

Toezicht op grond van de Wet Toezicht Beleggingsinstellingen
De Nederlandsche Bank is volgens de Wet Toezicht Beleggingsinstellingen eveneens aangewezen als toezichthouder voor beleggingsinstellingen. Het toezicht gaat hierbij veel minder ver dan bij banken en dergelijke: het is zoals boven al gemeld marginaal van aard. Hoewel uit informele gesprekken met functionarissen van de toezichthouder blijkt dat men ter zake van het hier bedoelde toezicht ook een zekere evolutie veronderstelt - het bloed kruipt immers waar het niet gaan kan - is toch de algemene verwachting dat voorschriften zoals bedoeld in het memorandum voor instellingen die onder de werkingssfeer van de Wet Toezicht Kredietwezen vallen, hier niet aan de orde zullen komen.

Dit laatste neemt niet weg dat evenzeer als bij een kredietinstelling het geval is,

het management van een beleggingsinstelling de primaire verantwoordelijkheid voor het beveiligings- en continuïteitsbeleid draagt. Bij grotere instellingen, zeker bij diegene die giraal effectenverkeer kennen, zullen derhalve ook zonder deze bemoeienis van DNB vérgaande maatregelen worden getroffen om de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking te waarborgen.

Uitwijkfaciliteiten
Van bijzonder belang is nog de beschikbaarheid van zogenaamde uitwijkfaciliteiten. Het bovengenoemde memorandum maakt een aantal malen gewag van een gestructureerde risico-afweging. Hierbij komen ook zaken als vandalisme, sabotage, terrorisme, bedrijfsspionage en dergelijke aan de orde. Een afdoende preventieve bescherming tegen dit soort restrisico's lijkt me onmogelijk; een kosten/baten-analyse die als kosten een al dan niet gedeeld operationeel uitwijkcentrum in zich draagt, is zeker voor de wat kleinere instellingen haast onhaalbaar. Hierbij komt nog dat elke insider weet hoe moeilijk het is om de gegevensverwerking de facto te herstarten in een ander computercentrum.
Naar mijn mening dient ook gewaakt te worden voor een schijnzekerheid waarbij bijvoorbeeld wel computerfaciliteiten maar geen gebruikers aanwezig zijn. (Straaljagers storten bijna altijd overdag neer in verband met het nachtvliegverbod; het risico van een "binnenvliegende F-16" doet zich derhalve bijna per definitie voor tijdens kantooruren.)

2. De invloed van toekomstige ontwikkelingen in automatiseringsland op EDP-auditing

Binnen het beperkte kader van dit artikel geef ik slechts een tweetal voorbeelden: EDI en image processing.

EDI is een verzamelbegrip. Voor ons doel kunnen we dit begrip het beste definiëren als geautomatiseerde middelen om tot externe integratie te komen. Het is duidelijk dat in omgevingen waar zeer grote bedragen bij wijze van routine via netwerken naar andere organisaties worden overgemaakt, zeer bijzondere beveiligingsmaatregelen noodzakelijk zijn. Ook hier lijkt de EDP-audit met een zekere neiging tot accentvorming op het incident een zeer zware opgave toebedeeld. Detecterende maatregelen zijn vrij eenvoudig te definiëren en te handhaven; preventieve maatregelen daarentegen zijn bijzonder moeilijk zodanig te implementeren dat geen incidenten kunnen voorkomen. Vooral een zelfstandig eigen oordeel van de externe EDP-auditor ontmoet schier onoverkomelijke problemen. Zeer efficiënte controlemaatregelen zoals de verbandscontrole en de cijferbeoordeling ontbreken nu eenmaal. Om wat ouderwetse termen te gebruiken: niet zozeer opzet en bestaan maar naleving en werking van de bedoelde maatregelen van interne controle vormen hier een bijzonder moeilijk hoofdstuk.

Een tweede ontwikkeling die ik kort wil aanstippen, is de zogenaamde image processing: het op beeldplaat vastleggen van elektronische kopieën van papieren documenten, voorzien van indices waarin zoekargumenten zijn opgenomen, die men kan gebruiken om de betrokken documenten terug te vinden.
In tegenstelling tot de voorgaande ontwikkeling, EDI, levert image processing een substantiële bijdrage aan de versterking van de interne controle binnen administratieve verwerkingsprocessen. De huidige technologie (zogenaamde WORM-technologie) immers laat niet anders dan eenmalig vastleggen - niet wijzigen - toe.
Dit betekent dat in essentie een ideale audit-trail is gecreëerd. Hierbij dient natuurlijk wel te worden aangetekend dat de documenten als zodanig niet kunnen worden verwijderd, maar dat de indices op een bijzondere manier moeten worden beveiligd omdat de toegang tot de individuele documenten van zo'n audittrail door ongeautoriseerde wijziging van de indices wel degelijk kan worden bemoeilijkt. Ik kan me evenwel audit-software voorstellen die beeldplaten "direct" benadert, waardoor dergelijke manipulaties een audit niet kunnen frustreren.

3. De richting waarin EDP-auditing als vak zich zou kunnen ontwikkelen

Reeds in 1987 werd onder auspiciën van het Limperg instituut een onderzoek uitgevoerd naar de wijze waarop het maatschappelijk verkeer in de verschillende onderdelen gebruik zou willen maken van de diensten van de accountant. Deze onderdelen van maatschappelijk verkeer betroffen directies, commissarissen, ondernemingsraden, aandeelhouders en dergelijke van kleine, middelgrote en grotere ondernemingen. De diepgaande enquête die aan de conclusies

van het onderzoek ten grondslag ligt, stelde vragen over velerlei onderwerpen waarmee de accountant zich verbonden voelt.
Ik beperk me hier tot de conclusies die ter zake van het onderwerp automatisering werden bereikt. De meest opzienbarende conclusie was wel dat er zeer belangrijke behoefte bestaat aan automatiseringsadvies, hetwelk men graag bij de accountant zou onderbrengen indien men ervan overtuigd zou zijn dat voldoende deskundigheid beschikbaar was. Tussen deze veronderstelde deskundigheid en de behoefte aan advies gaapt een groot gat dat mijns inziens door EDP-auditors kan worden opgevuld. Dat het hierbij niet primair gaat om betrouwbaarheid en continuïteit laat zich als volgt toelichten:

In automatiseringsland geldt een wet die ik de 200/200/50-regel noem. Deze laat zich enigszins gechargeerd in de volgende vraag samenvatten: "Waarom zijn de werkelijke kosten van een systeem twee keer groter dan het budget, waarom duurt de ontwikkeling van een systeem twee keer langer dan begroot, en waarom levert zo'n systeem maximaal vijftig procent van de beloofde functionaliteit?"

Indien EDP-auditing zich zou richten op de onderzoekscriteria doelmatigheid en doeltreffendheid ligt een zeer grote markt voor de EDP-auditors van de huidige generatie open. Het is daarbij een gemeenplaats om te stellen dat deze EDP-auditors skills moeten ontwikkelen om een zinvolle bijdrage te kunnen leveren aan een antwoord op de bovengenoemde drie vragen in het kader van de 200/200/50-regel.

De heer J.J.A. Leenaars, RA studeerde Bedrijfseconomie aan de Hogere Economische School te Rotterdam en vervolgens Accountancy. Momenteel is hij werkzaam bij de Robecogroep. Daar is hij lid van het Beleidscomité, belast met de Portefeuille Financiën en Systemen. Zijn grote productiviteit heeft geleid tot vele publikaties en lezingen.

Mr. Ong Sien Hien
Officier van Justitie aan het Parket Rotterdam

Strafrecht en computerrelated crime

Uit de strafrechtelijke praktijk blijkt dat "echte" computerfraude, dat wil zeggen dat er in de programmatuur van een computersysteem wordt geknoeid, (nog) niet vaak voorkomt. De meest gesignaleerde computercriminaliteit vindt plaats met behulp van een computer en/of een computerprogramma in een geautomatiseerde omgeving. Uiteraard is daarbij de heel "gewone" software-kopiëring buiten beschouwing gelaten. Immers, dit laatste is zo algemeen verspreid dat dat haast tot de klasse kleine criminaliteit moet worden gerekend.
Echt verbazingwekkend is het misschien niet dat de menselijke factor een grote rol blijkt te spelen in de meer omvangrijke fraudegevallen. Het blijkt immers dikwijls eigen personeel te zijn dat iets anders met de hem toevertrouwde middelen doet dan de bedoeling is. Gebrekkige beveiliging en een te groot vertrouwen in personen op voor het bedrijf cruciale plaatsen zijn daaraan debet.

1 Strafrechtelijke mogelijkheden

Het strafrechtelijke systeem, dat wat betreft de computercriminaliteit nog in het tijdperk van de ganzeveer leeft, is te verdelen in twee van elkaar afhankelijke systemen: het materiële strafrecht, dat beschrijft welke gebeurtenissen in strafbare feiten omschreven kunnen worden, en het formele strafrecht, dat beschrijft welke middelen mogen worden gebruikt om strafbare feiten op te sporen en te bewijzen en op welke wijze iemand voor die strafbare feiten kan worden veroordeeld.
Om iets van de moeilijkheden te begrijpen bij de opsporing en vervolging van computercriminaliteit moet men ervan doordrongen zijn dat deze twee systemen, hoewel in de praktijk van elke dag als zeer klemmend en belemmerend ervaren, een verworvenheid zijn van ons democratisch gevormde rechtssysteem en als zodanig van een hoog moreel gehalte.
Dat betekent dat er een grote waarde aan moet worden gehecht en dat, ondanks de ogenschijnlijk soms nutteloze moeilijkheden en barrières die het met zich mee kan brengen, de procedureregels strikt moeten worden nageleefd. Pas dan verwerft een rechtelijke uitspraak immers gezag en is er geen sprake van willekeur.
Een en ander neemt niet weg dat te grote hindernissen moeten worden opgeruimd en nieuwe opsporingsmiddelen moeten worden toegelaten. Daarop zal in een ander artikel dieper worden ingegaan.

Dit artikel gaat met name in op de praktijk van de opsporing. Daar dient een groot aantal problemen zich aan. Zo pakte een rechter-commissaris in strafzaken tijdens een huiszoeking een computerband op, rolde deze een eindje af, hield de band tegen het licht en sprak: "Deze band hoeft niet meer, want er staat niets op!"
Gebrek aan kennis dus! En dan hebben we het alleen nog maar over de hardware. De werking van al die dozen komt de gemiddelde jurist onbegrijpelijk voor.
Ook de politie is nog niet echt in staat goede opsporing te doen. Men is dan ook zeer afhankelijk van de aangever zelf. Maar deze is op zijn beurt weer aangewezen op de automatiseringsdeskundige. En al te vaak blijkt dat nu juist één van de mogelijke verdachten.
Alleen al om deze vicieuze cirkel te doorbreken is onafhankelijke deskundigheid noodzakelijk.

Hoe ingewikkeld het verder kan worden blijkt uit de volgende geparafraseerde opmerking uit een vonnis betreffende een computerzaak: "Een bestand is een geschrift in de zin van artikel 225 SR, indien een dergelijk bestand is opgeslagen in een *extern* geheugen."
Eén van de eerste problemen die ik aan de EDP-auditors van KPMG heb voorgelegd, was: "Vertel eens, wat is een extern geheugen en deugt dit als onderscheidend criterium voor het al dan niet zijn van een geschrift in de zin van artikel 225 SR?"
Om twee redenen konden zij toen geen antwoord geven:

a. Men kon het er niet over eens worden wat precies onder extern geheugen moest worden verstaan.
b. Men wist niet wat art. 225 SR inhield en hoe dit in de context van het strafrecht moest worden beoordeeld.

Dit omlijnt een tweede moeilijkheid.
Ook al begrijp ik (iets van) wat de EDP-auditor aan mij tracht uit te leggen, dan nog is het niet direct duidelijk wat ik in juridicis met die kennis kan doen.
Of andersom, doordat ik niets weet van EDP-auditing kan ik aan de EDP-auditor niet de juridisch relevante vragen stellen!

Kortom, begripsverwarring door niet aansluitend taalgebruik en gebrek inzicht in het kennisgebied over en weer.

Om deze methodologische kenniskloof te overbruggen zijn er thans contacten tussen enerzijds juridische gespecialiseerden met belangstelling voor EDP-auditing en andersom.

2 Forensische EDP-auditor

Eigenlijk zou uit deze contacten een aparte specialisatie moeten voortvloeien in de vorm van een forensisch EDP-auditor, vergelijkbaar met de forensische psychiater en de gerechtstolken. "Forensisch" betekent in dit kader "ten behoeve van het gerecht".
De EDP-auditor met dit specialisme zou zijn kennis en zijn bevindingen zodanig moeten "vertalen" dat deze bruikbaar worden voor en binnen het juridische betekenis- en denkkader.
De vanuit het juridisch systeem noodzakelijke antwoorden op vragen liggende op het EDP-auditing-terrein kunnen voor de EDP-auditor weleens volstrekt onzinnig, onnodig en zelfs onbeantwoordbaar blijken. In zo'n geval dient de wetgever te spreken.
Uit de discussies rond de nieuwe wetgeving computercriminaliteit blijkt reeds hoe ver beide denkkaders van elkaar zijn verwijderd en hoe moeilijk het is beide gebieden op elkaar te laten aansluiten.
Indien op louter theoretisch terrein er al grote problemen zijn, laat het zich indenken welke problemen op praktisch opsporings- en vervolgingsterrein ontstaan. Ook daar zou het advies van een forensisch EDP-auditor van pas komen.
Een voorbeeld. Onze nationale luchtvaartmaatschappij doet aangifte bij de politie te Haarlem dat er honderden retourtjes Amsterdam-New York door haar zijn uitgevoerd, maar dat de daarbij behorende betalingen op raadselachtige wijze uit de boeken zijn verdwenen. Het vermoeden bestaat dat er ergens in het internationale vluchtreserveringssysteem is geknoeid of in de aansluiting met het eigen geheel geautomatiseerde administratieve verwerkingssysteem of op de eigen eveneens geautomatiseerde financiële afdeling. Kortom, de froude kon overal in het systeem zijn gepleegd.
Wat kan de hoofdagent te Haarlem doen die deze aangifte opneemt?
De commissaris bellen of een hem bekend officier van Justitie zal niet veel helpen, want ook die worden niet gehinderd door gespecialiseerde kennis.
Hij legt dus contact met de Centrale Recherche Inlichtingendienst, de CRI, afdeling Computerfrauden.
Zijn eerste vraag zal dan luiden: "Zullen we alles in beslag nemen", maar die zal op een categorisch "Nee" stuiten. Immers, wat moet in beslag genomen worden? Alle computers en alle software? Waar staan die dingen en hoe moet dat eigenlijk? En hoe blij wordt de aangever als door zo'n inbeslagneming heel het bedrijf wordt platgegooid. Tenslotte is een dergelijke maatregel juridisch wel mogelijk.
Als we niet alles in beslag mogen nemen, hoe moeten we dan het lek boven krijgen? Met welke middelen, binnen welk juridisch kader?
Het is hier niet de plaats om deze problemen op te lossen. Maar wel om ons af te vragen: "Wat roept een aangever over zich af bij aangifte?" "Welke risico's loopt hij zakelijk?" "Zijn er andere wegen om het lek te dichten?"

Naar mijn mening moet een forensisch geschoold EDP-auditor ook op dit soort vragen antwoord kunnen geven. Hij

moet in staat zijn het bedrijfsmanagement een zodanig advies te geven dat dit een juiste beslissing kan nemen. Dat wil zeggen dat de forensisch EDP-auditor niet alleen strafrechtelijk operationeel gericht moet zijn, hij moet ook meer civielrechtelijk georiënteerde adviezen kunnen geven.
Zo zal indien de eventuele dader binnen de organisatie wordt aangetroffen, toch de fraudemethode zodanig juridisch duidelijk moeten worden beschreven dat de kantonrechter bereid is een ontslagprocedure te honoreren.
In geval van een civiele schadeloosstellingsprocedure zal er ook een voor de civiele rechter kenbaar verhaal moeten komen, wil schadevergoeding kunnen worden toegewezen.

Wil een advocaat uit de voeten kunnen met automatiseringsfraude, dan is de hulp van een forensisch EDP-auditor onontbeerlijk. De veelgebruikte oplossing van de "gouden" handdruk lijkt niet langer werkbaar. Immers, te veel mensen zijn thans min of meer thuis in de geautomatiseerde systemen. Voor het plegen van fraude behoeft men niet langer over echt gespecialiseerde kennis te beschikken, zodat op alle niveaus in een geautomatiseerd systeem kan worden geknoeid.

Het bovenstaande in aanmerking genomen, is het voorstelbaar dat de EDP-auditor zijn werkzaamheden niet dient te starten *nadat* de fraude heeft plaatsgevonden. Hij dient al in de preventieve sfeer de ondernemer te adviseren. Het technisch snelste en economisch voordeligste automatiseringssysteem hoeft immers uit strafrechtelijk oogpunt niet het veiligste systeem te zijn. De forensisch EDP-auditor moet daarom ook in staat zijn een geautomatiseerd systeem te kunnen doorlichten op de juridische risico's.
Net als iemand die, omdat hij dronken rijdend een ongeval heeft veroorzaakt, ondanks het feit dat hij verzekerd is, niets krijgt uitgekeerd omdat hij zichzelf in een gevaarlijke situatie heeft gebracht (de leer van het toe te rekenen risico), zo kan iemand met een volledig *niet* beveiligd geautomatiseerd systeem geen hulp verwachten van politie en justitie indien er daadwerkelijk iets gebeurt.

Dit betekent niet dat de eis van volledige, absolute beveiliging wordt gesteld. Maar een eis van een redelijke beveiliging zal in de wet worden neergelegd. Het vinden van de juiste balans tussen een kosteneffectieve automatisering enerzijds en een voldoende beveiligd systeem (wat altijd duurder is) anderzijds is een taak die door een forensisch EDP-auditor moet kunnen worden opgelost. Door zijn kennis van de belangen en mogelijkheden van in een (mogelijk) proces betrokken partijen moet hij kunnen inschatten wat partijen over en weer van elkaar in redelijkheid mogen verlangen op het terrein van kostenaspecten en beveiligingsmaatregelen.

Al concluderend:
Er moet een specialisme forensische EDP-auditing komen. Dit specialisme houdt in dat daardoor op adequate wijze alle partijen in een (mogelijk) juridisch geding (van zowel civiel, straf- als administratief rechtelijk) worden voorgelicht over de mogelijkheden en onmogelijkheden van een geautomatiseerd systeem, welke juridische gevaren zo'n systeem in zich bergt en wat daartegen naar een redelijke maatstaf gemeten te doen is.

3 Aangiftebereidheid

Tot slot enige opmerkingen over de aangiftebereidheid van bedrogen ondernemers en instellingen. Deze is niet erg groot.
Een van de hoofdredenen lijkt de schaamte te zijn. Dat fraude voorkomt op zich lijkt niet het ergste, maar dat een zo vooruitstrevend bedrijf met een zo geavanceerd geautomatiseerd systeem wordt bedrogen, is kennelijk zo'n aantasting van het imago dat een bedrijf wil uitstralen, dat ze het liever binnenskamers houdt.
Toch komt zo'n opvatting mij wat kortzichtig over. Niet alleen blijven zodoende de omvang en aard van de computerfraudes onduidelijk, maar ook gaat de bedenker van het kwaad "betrekkelijk" vrijuit, waardoor hij elders zijn zegenrijke arbeid kan voortzetten. Bij een aantal gepakte fraudeurs blijkt immers dat zij bij andere werkplekken op eervolle wijze, maar plotseling zijn vertrokken. Navraag naar het waarom stuit dan op een muur van welwillend zwijgen, wat de ware speurder alleen maar bewijst dat er veel onder tafel wordt gespeeld.
Gebrek aan inzicht in de wijze van fraude maakt het ontwikkelen van adequate tegenmaatregelen en opsporingsmethoden alleen maar moeilijk, terwijl er aantoonbaar veel (economische) schade wordt aangebracht.
Het Platform Computercriminaliteit is er-

voor bedoeld om juist dit gebrek aan inzicht op te heffen. Ondanks de speciaal voor dit Platform ontwikkelde meldingsmethode (die justitieel ingrijpen uitsloot) is de opbrengst aan zaken niet echt omvangrijk geweest.
Is de conclusie dan dat computercriminaliteit een zeepbel is die bij even blazen klapt? Of is er werkelijk een dreigend gevaar, maar blijft het onzichtbaar omdat het "low key" wordt gespeeld door mogelijke aangevers?
Het Platform Computercriminaliteit is er niet uitgekomen. Ieder van de deelnemers (en die vertegenwoordigden grote delen van de maatschappij betrokken bij automatisering, zowel makers als gebruikers) kende woestwilde, adembenemende fraudes uit eigen kring, zonder deze te kunnen (mogen?) concretiseren in harde data.

Het is een misverstand te denken dat elke aangifte automatisch vervolging betekent. Over vervolging valt te praten. Het is ook een misverstand dat aangifte automatisch negatieve gevolgen heeft voor het imago.
Aangifte heeft haar preventieve werking voor de organisatie en voor de maatschappij waarbinnen de organisatie functioneert. Zij is een signaal dat wij niet willoos zijn overgeleverd aan de computer en zijn bedienaren.
De forensisch EDP-auditor kan daarbij als "bewaker" optreden. Uiteraard zal hij wijzen op de risico's en de nadelen van aangifte. Maar op de lange duur en in het algemene belang is aangifte toch voordeliger.

Mr. Ong Sien Hien doorliep zijn studie Rechten in Nijmegen. Na een periode als Rechterlijk Ambtenaar in opleiding was hij enige tijd als Wetenschappelijk Medewerker Strafrecht en Strafprocesrecht verbonden aan de Katholieke Universiteit Brabant te Tilburg. Momenteel is de heer Ong Sien Hien Officier van Justitie te Rotterdam, alsmede lid van het Platform Computercriminaliteit.

Prof. mr. H. Franken
Hoogleraar Rechtswetenschap Informaticarecht,
Rijksuniversiteit te Leiden

Wetgeving tegen misbruik van informatie

1 Een pakket van maatregelen

Kennis is macht. Dat betekent dat kennis ook ten nadele van anderen kan worden gebruikt. We kunnen daarbij denken aan de schending van geheimen en het manipuleren van gegevens (vormen van fraude). Bovendien kan de overdracht van informatie worden verstoord. Het is buiten kijf dat deze vormen van misbruik van informatie grote schade kunnen veroorzaken.
Het is nu in de eerste plaats aan de burger zelf om schade ten gevolge van informatiemisbruik te voorkomen. Hiertoe kan hij voor de hand liggende fysieke beschermingsmaatregelen nemen en waarborgen in de organisatie van zijn onderneming inbouwen. Ook is het noodzakelijk om een beveiliging in de te gebruiken programmatuur aan te bregen. Daarna komen juridische maatregelen aan de orde. Het is te vergelijken met de beveiliging van een huis. Vóór iemand met vakantie gaat, sluit hij zijn woning af; men volstaat niet met te vertrouwen op een wettelijk verbod van inbraak.
De juridische maatregelen kunnen ook liggen in de preventieve sfeer, zoals het deponeren van broncode, maar we denken dan voornamelijk aan de overdracht van het risico op schade aan een derde door het uitdrukkelijk regelen van licenties, het opnemen van een concurrentiebeding in arbeidsovereenkomsten met werknemers (volgens gegevens uit de praktijk de grootste risicogroep) en het sluiten van verzekeringsovereenkomsten.
Daarnaast kan de overheid hulp bieden door middel van wetgeving zowel op het gebied van het strafrecht als op het terrein van het privaatrecht.

2 Strafrechtelijke maatregelen

In mei laatstleden is de zogenaamde Wet computercriminaliteit bij de Tweede Kamer ingediend. Deze wet behelst een aantal voorstellen tot wijziging van het Wetboek van Strafrecht. Deze wijzigingen hebben zowel betrekking op de middelen van informatietechniek als op de bescherming van gegevens.
In de eerste plaats wordt voorgesteld de vernieling, beschadiging, onbruikbaarmaking dan wel het veroorzaken van storing in de werking van middelen van informatietechniek strafbaar te stellen, indien daardoor

- het functioneren van de openbare infrastructuur schade wordt toegebracht, en/of
- een gemeen gevaar voor goederen of de levering van diensten te duchten is, en/of
- levensgevaar voor anderen te duchten is.

Dit voorstel is bedoeld om aanslagen op de continuïteit van het functioneren van informatietechnische processen waaraan algemene belangen zijn verbonden, te kunnen tegengaan. Tevens dient het om aanslagen op informatietechnische middelen, welke mogelijk zeer ernstige gevolgen zullen hebben, te kunnen bestraffen.
In de tweede plaats is voorgesteld om "computervredebreuk" strafbaar te stellen. Het betreft het zich wederrechtelijk toegang verschaffen tot geautomatiseerde gegevensverwerkende systemen. Hierbij zal alleen van strafbaarheid sprake zijn, indien bij het "wederrechtelijk binnendringen" een beveiliging daartegen wordt doorbroken. De plaats waar de beveiliging is aangebracht, is te beschouwen als de grens tussen het "pri-

vé-terrein" en het voor een ieder toegankelijke gebied.
De achtergrond van dit voorstel is gelegen in de opvatting dat strafbaarstelling wenselijk is omdat computervredebreuk als zodanig onbehoorlijk is. Het betreft het ongenood binnendringen in het privé-domein van een ander. Tevens speelt een rol dat met strafbaarstelling een drempel kan worden opgeworpen tegen eventuele op het binnendringen volgende schadelijke handelingen, zoals het wijzigen en wissen van gegevens en de kennisneming of het kopiëren van vertrouwelijke gegevens.

Andere voorstellen hebben direct betrekking op de bescherming van gegevens. Daarbij gaat het steeds om gegevens (waaronder ook programma's) die zijn opgeslagen, worden verwerkt of overgedragen door middel van een geautomatiseerd werk.

Met het totaal van voorstellen is een afgerond geheel ontworpen, waarmee strafbaar wordt gesteld:
1. dat personen zich wederrechtelijk toegang verschaffen tot beschermde gegevens;
2. dat wederrechtelijk verkregen gegevens worden bekendgemaakt of op bepaalde wijze gebruikt; en
3. dat niet wederrechtelijk verkregen gegevens met een geheim karakter wederrechtelijk worden bekendgemaakt of op een bepaalde wijze gebruikt. Bij de laatste categorie hebben we het oog op niet wederrechtelijk afgeluisterde of opgenomen telecommunicatie, gegevens die berusten bij zogenaamde geheimhouders en bedrijfsgeheimen.

3 Zuinig met strafrecht

Het strafrecht vormt weliswaar een noodzakelijke aanvulling op preventieve maatregelen, maar het uiteindelijke effect kan niet anders dan beperkt zijn. Dit houdt in dat men terughoudend moet zijn bij het hanteren van het strafrecht. In de huidige voorstellen is van deze terughoudendheid op twee manieren blijk gegeven. In de eerste plaats door niet alle gedragingen strafbaar te stellen, die als onoirbaar worden aangemerkt en in de ons omringende landen soms wel strafbaar zijn of worden gesteld. In Nederland is bijvoorbeeld voorgesteld om het onbevoegd gebruik van informatietechnische middelen niet strafbaar te stellen. In de tweede plaats door sommige onoirbaar geachte handelingen slechts strafbaar te stellen wanneer aan bepaalde voorwaarden is voldaan. Zo is in het voorstel tot strafbaarstelling van computervredebreuk een belangrijke beperking aangebracht door deze alleen te richten op het inbreken in *beveiligde* systemen.
Met laatstgenoemde eis wordt aangegeven, dat de beveiligingsmaatregel een grens van het computersysteem aangeeft. Om deze grens te overschrijden is opzet van de dader nodig. Tevens wordt met het stellen van deze grens expliciet aangegeven welke gegevens de beheerder van een computersysteem wil beschermen. Het "laten slingeren" van gegevens maakt de kennisneming daarvan immers niet onrechtmatig. Het grondrecht om inlichtingen te vergaren zoals omschreven in artikel 10 EVRM geeft dit duidelijk aan. Van binnendringen kan in de voorgestelde bepaling alleen sprake zijn indien men zich toegang verschaft tegen de onmiskenbare wil van de rechthebbende. Deze wil zou kunnen blijken uit de woorden "verboden toegang" of iets dergelijks. In het wetsvoorstel is gesteld, dat woorden alleen (bijvoorbeeld op het beeldscherm) niet voldoende zijn, want daarmee wordt een "toegang per ongeluk" niet voorkomen. Dit gevaar is in veel mindere mate aanwezig wanneer een hogere drempel wordt aangebracht, die bestaat uit bepaalde tegen het wederrechtelijk binnendringen gerichte beveiligingsmaatregelen. Het is als met een woonhuis: de deur moet niet alleen dicht zijn, maar ook op slot.

4 Rechtspersonenrecht

Bij de strafbaarstelling van computervredebreuk blijkt zelfwerkzaamheid van het potentiële slachtoffer een conditio sine qua non. Een dergelijke eis moge nieuw zijn, maar deze sluit aan bij de gewone gang van zaken in het handelsverkeer. Immers ook bij betrekkelijk kleine vorderingen voorziet een crediteur zich van zekerheden. Daarbij rekent men niet uitsluitend op bescherming door de rechter bij het niet nakomen van een verbintenis, maar men vestigt een pand- of hypotheekrecht of vraagt bij voorbaat een garantstelling. Ten aanzien van vele door het strafrecht bestreken handelingen - vooral in de vermogenssfeer - blijft het potentiële slachtoffer evenwel passief. Hij wacht af of hem niets zal overkomen en als dat onverhoopt wel het geval is, moet de overheidsrechter genoegdoening of compensatie geven. Nu blijkt die overheidsrechter dat werk niet meer

aan te kunnen. Vooral dit verschijnsel vormt een reden om te bezien of er in het civiele recht mogelijkheden zijn om maatregelen tegen het misbruik van informatie te stimuleren.
Een belangrijke aanzet om drempels op te werpen tegen nonchalance ten aanzien van de beveiliging van gegevensstromen bestaat uit het stellen van regels dienaangaande voor rechtspersonen. Een regeling in Boek 2 Titel 8 BW is denkbaar. Daarbij laten zich de volgende varianten onderscheiden:

A. Als onderdeel van de controle van de jaarrekening zou door de registeraccountant een oordeel moeten worden gegeven over de beveiliging van de geautomatiseerde gegevensverwerkende systemen waarvan de onderneming zich bedient.
B. Een deskunde (AC-accountant of EDP-auditor) zal een oordeel moeten uitspreken met betrekking tot de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking.
C. Een verklaring betreffende de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking wordt door de directie opgenomen in het jaarverslag van de onderneming, over welke verklaring de accountant zich dient uit te laten.

Variant A
Variant A verdient althans voorlopig - geen aanbeveling. De accountantsverklaring bij de jaarrekening is gericht op de vraag of deze een getrouw beeld geeft van het vermogen en het resultaat van de vennootschap. Daarbij worden geautomatiseerde gegevensverwerkende systemen alleen in de controle betrokken voor zover dat dienstig is aan het doel van de jaarrekeningcontrole. Men zou in deze variant veel meer van de accountant gaan vragen, namelijk een oordeel over het totale stelsel van geautomatiseerde systemen in het bedrijf.

Variant B
Bij variant B is gedacht aan een afzonderlijk oordeel over de mate van beveiliging van de geautomatiseerde gegevensverwerkende systemen door een specifieke deskundige. Hiervoor valt te denken aan een accounant die is gespecialiseerd op het gebied van automatisering en controle (AC-accountant of EDP-auditor). Zolang er nog geen sprake is van reglementering van de opleiding voor deze specialisten, kan een verklaring van een AC-accountant of EDP-auditor niet het gewicht hebben, dat aan een accountantsverklaring ten aanzien van de jaarrekening toekomt. Het zal dan meer gaan om een onderhandse verklaring - een management letter -, waarvoor het probleem geldt dat deze niet buiten de kring van de bestuurders van de vennootschap komt.

Variant C
Er resteert variant C. Deze houdt in dat het bestuurorgaan van de rechtspersoon een verklaring moet opnemen in zijn jaarverslag over met name de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Hieruit volgt met zoveel woorden dat de verwantwoordelijkheid voor de mate en kwaliteit van beveiliging bij de directie ligt. Deze zou in de eerste plaats, analoog aan het voorschrift in de Wet persoonsregistraties op grond waarvan iedere houder van een persoonsregistratie verplicht is een reglement op te stellen, schriftelijk moeten aangeven aan welke eisen de beveiliging in het betrokken bedrijf moet voldoen. Vervolgens zou in het jaarverslag moeten worden aangegeven dat de beveiliging conform het reglement is uitgevoerd, zodat het bestuur instaat voor de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Ten slotte kan de accountant door deze verklaring van het bestuur te toetsen aan het reglement publiekelijk uitspreken of deze verklaring van de directie al dan niet terecht is gegeven.
Hoewel de vergadering van de Nederlandse Juristen Vereniging in 1988 zich ten aanzien van een wijziging van het rechtspersonenrecht afhoudend opstelde, heeft het NIVRA zich recentelijk als een voorstander daarvan uitgesproken. In geschrift 53 *Automatisering en controle* wordt een uitwerking gegeven van kwaliteitsoordelen over de informatievoorziening in aansluiting op bovengenoemd voorstel in de variant C. Van belang is bovendien, dat De Nederlansche Bank op 20 september 1988 een memorandum heeft uitgegeven omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen. DNB formuleert daarin op grond van haar toezichthoudende taak op het bankwezen een aantal aandachtspunten om deze betrouwbaarheid en continuïteit vast te stellen. DNB heeft de banken in Nederland daarbij de verplichting opgelegd aan de externe accountant op te dragen zich periodiek een oordeel te vormen "omtrent de betrouw-

baarheid en continuïteit van voor de bedrijfsprocessen essentiële geautomatiseerde gegevensverwerking".
Het moge zo zijn dat hiermee een nieuwe last op het bedrijfsleven wordt gelegd, deze last is gerechtvaardigd door het grote belang dat aandeelhouders en crediteuren hebben bij een expliciete zorg van het management voor een ongestoorde informatieverwerking in de onderneming.

5 Conclusie

De nieuwe wetsvoorstellen zijn afgestemd op de praktijk. Over de handhaafbaarheid ervan is diepgaand overleg geweest. Zij sluiten bovendien aan bij de tendens, dat ook verzekeraars steeds meer clausules in de polissen opnemen, die inhouden dat beveiligingsmaatregelen verplicht zijn. De jurisprudentie speelt hierop in door de laatste jaren het begrip "merkelijke schuld" van de verzekerde ruim uit te leggen. We mogen daarom stellen dat men zich thans alleen op bescherming door anderen (verzekeraars, overheid) kan beroepen als de benadeelde-eigenaar zelf zich ook voorzichtig heeft gedragen. Voor bescherming van gegevens geldt, dat de houder daarvan moet handelen met de zorgvuldigheid, die in het maatschappelijk verkeer ten aanzien van zijn "eigen" gegevens betaamt.

Dieper op deze materie wordt ingegaan in het boek *Dilemma's van aansprakelijkheid*, te verschijnen bij Gouda Quint, Arnhem december 1990.

Prof. Mr. H. Franken volgde zijn studie aan de Rijksuniversiteit te Leiden en de Sorbonne te Parijs. Hij was achtereenvolgens advocaat en rechter te Rotterdam.
Nu is hij hoogleraar in de Inleiding tot de Rechtswetenschap en het Informaticarecht aan de Rijksuniversiteit te Leiden. Ook was professor Franken voorzitter van de Commissie Computercriminaliteit (ook wel "Commissie Franken" genoemd).