COMPACT WINTER

BEHEERSING VAN IT ALS OPPORTUNITY

1994/4

KWARTAALBLAD EDP-AUDITING

Compact ®
Jaargang 21, nummer 4
Een uitgave van KPMG Klynveld EDP Auditors en Samsom BedrijfsInformatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 4 x per jaar.

Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
J.C. Boer RE RA
Ir. J.A.M. Donkers
Drs. R.G.A. Fijneman RE RA
Mw. S.M. Keijl
Drs. P. Veltman RE RA

Redactiesecretariaat
Mw. I. de Koning,
Samsom BedrijfsInformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 01720 - 66 746
Fax : 01720 - 66 569

Vormgeving
Bureau Karakter, Delft

Aan dit nummer werkten mee
J.C. Boer RE RA
Drs. J.A.C. van Geel
R.A. Jonker RA
Ing. A.P.J. Mouwen
Prof. A.W. Neisingh RE RA
Drs. P. Veltman RE RA
Drs. E.P.R. van Vroenhoven RE RA

Abonnementen
f 135,- per jaar incl. BTW. Losse nummers f 45,- 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 - 66 800
Fax : 01720 - 75 933
Adreswijzigingen - ook tijdelijke - moeten minstens 8 weken voor de verschijningsdatum bekend zijn.

Uitgever
Drs. Th.P.M. Brinkman

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 - 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals: • beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacy-wetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor EDP-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG Klynveld EDP Auditors.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG Klynveld, KPMG Klynveld EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij Samsom BedrijfsInformatie BV, deel uitmakend van Wolters Kluwer NV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij het secretariaat verkrijgbaar is.

De ontwikkelingen in informatietechnologie stagneren geenszins. Of er nu in bepaalde gevallen sprake is van 'oude wijn in nieuwe zakken' of dat daadwerkelijk nieuwe hulpmiddelen, systemen en dergelijke worden aangeboden, is niet eens van belang. De snelheid van verandering geeft de (potentiële) gebruikers van informatietechnologie het gevoel dat ze achter de feiten aanhollen. Als ze net enigszins begrepen hebben wat een relationele database is, worden ze alweer geconfronteerd met begrippen als client server en gedistribueerde databases.

Dit alles levert een gevoel van onbehagen op, dat op diverse lagen in een organisatie kan ontstaan. De consequentie hiervan kan een defensief mechanisme zijn tegen iedere vorm van verandering in de informatietechnologie. Zo blijkt soms dat het algemeen management ieder veranderingsvoorstel van de automatiseringsmanager blokkeert. Dit verschijnsel is in een aantal middelgrote organisaties zeer goed waar te nemen, echter ook in grootschalige organisaties kan hiervan sprake zijn (vooral op business unit-niveau).

Dit leidt tot een impasse, waarbij niet meer op basis van rationele argumenten kan worden gecommuniceerd. Veelal blijkt deze te zijn ontstaan door onvoldoende communicatie op functioneel niveau tussen het management en de verantwoordelijke interne en/of externe automatiseerders.
Een functionele en beheersmatige benadering van informatietechnologie kan soelaas bieden bij het oplossen van een bestaande of het voorkomen van een mogelijke impasse.

De ontwikkelingen in de informatietechnologie zijn vele en op alle ingaan is ondoenlijk, zeker binnen de context van één Compact. Dit nummer beoogt via een aantal artikelen inzichtelijk te maken dat die vele ontwikkelingen in de informatietechnologie best te beheersen zijn. Voor het definiëren van de beheersingsstructuren zijn verschillende hulpmiddelen beschikbaar, zoals de uit de Verenigde Staten afkomstige SAC Reports, de recentelijk gepubliceerde Code of practice voor Informatiebeveiliging, en ander referentiemateriaal. In het artikel van Veltman wordt hierop nader ingegaan. Feitelijk kan het management de informatietechnologie op verantwoorde wijze offensief tegemoet treden, mits hiervoor (minimale) beleidsafspraken en beheersingsstructuren zijn vastgesteld. Deze offensieve benadering van informatietechnologie zou ook door een certificerend accountant kunnen worden gehanteerd. Het belang van het toe- en inpassen van informatietechnologie in het kader van zijn certificerende activiteiten wordt, als vervolg op de inhoud van Compact 1993/4, nogmaals belicht.

Hopelijk levert deze Compact een bijdrage aan de bewustwording bij zowel het management als de certificerend accountant dat informatietechnologie veel meer een 'opportunity' dan een 'threat' is. EDP-auditors kunnen bij dit bewustwordingsproces een belangrijke ondersteunende rol vervullen.
De redactie wenst u veel leesplezier met dit nummer van Compact. Tevens wenst zij u een succesvol en vooral gezond 1995 toe.

Drs. R.G.A. Fijneman RE RA

Geautomatiseerde gegevensbewerking en jaarrekeningcontrole

R.A. Jonker RA

Dit artikel wijdt een beschouwing aan de op de geautomatiseerde gegevensbewerking gerichte werkzaamheden die de accountant in het kader van zijn jaarrekeningcontrole over het algemeen zal moeten uitvoeren. Het artikel is gebaseerd op de gedachtenvorming in de NIvRA-werkgroep 'Standaarden en Normen'.
Deze werkgroep bereidt een publikatie voor waarin een aanzet zal worden gegeven tot objectivering van het referentiekader dat de accountant gebruikt bij het beoordelen van de geautomatiseerde gegevensbewerking in het kader van de jaarrekeningcontrole. Het onderwerp dat in dit artikel centraal staat zal daar deel van uitmaken.

INLEIDING

Automatisering en accountantscontrole zijn onlosmakelijk met elkaar verbonden. Reeds vanaf het eerste moment dat de automatisering haar intrede deed in de informatieverzorgende processen hebben accountants studie verricht naar de invloed daarvan op de accountantscontrole.
Het doel van dergelijke studies was vooral een antwoord te vinden op de vraag of het accountantscontroleproces anders zou moeten worden ingericht als gevolg van de automatisering van informatiesystemen. Deze studies richtten zich daarmee in het bijzonder op de afbakening van de taak en de verantwoordelijkheid van de accountant in het kader van de jaarrekeningcontrole. Reeds in 1970 verschenen deel 1 en deel 2 van de NIvRA-geschriftenreeks 'Automatisering en controle'. In 1975 werden zij gevolgd door een derde deel. Te zamen vormen zij een samenhangende studie naar de 'invloed van de automatisering van de administratie op de accountantscontrole'.
Deze publikaties gaven in de tijd gezien echter geen afdoende antwoord op de hiervoor geformuleerde vraag naar de invloed van automatisering van informatieverzorgende processen op de accountantscontrole. Driet ontwikkelingen noopten tot vervolgonderzoek op dit terrein, te weten:

- de voortschrijdende automatisering, zowel in kwantitatief als in kwalitatief opzicht;
- ontwikkelingen in de aanpak en uitvoering van de accountantscontrole in het algemeen en meer in het bijzonder ten aanzien van de EDP-audit (bijvoorbeeld risico-analyse);
- wettelijke verplichtingen bij de jaarrekeningcontrole (Wet computercriminaliteit).

De op deze terreinen verschenen publikaties bieden echter onvoldoende inzicht in de samenhang tussen het hedendaagse (op risico-analyse gebaseerde) accountantscontroleproces en de daaruit voortvloeiende beoordeling van de geautomatiseerde gegevensbewerking.

In dit artikel wordt een theoretisch referentiekader geschetst voor de beoordeling van de geautomatiseerde gegevensbewerking die de accountant minimaal zal moeten verrichten om tot een oordeel over de getrouwheid van de jaarrekening te komen. In het vervolg van dit artikel wordt deze beoordeling aangeduid als *eerste lijns EDP-audit*. Een en ander in tegenstelling tot andere vormen van EDP-audit, waarbij de invalshoek niet de jaarrekeningcontrole betreft, maar welke primair ten behoeve van het management worden uitgevoerd (rekencentrumaudit, onderzoek naar de kwaliteit van de ontwikkelingsorganisatie, systeemaudit en dergelijke). Dergelijke onderzoeken behoren tot de zogenaamde tweede lijns EDP-audit.
Achtereenvolgens wordt in dit artikel ingegaan op:

- de betekenis van de automatisering voor de jaarrekeningcontrole;
- de taak en verantwoordelijkheid van de accountant aangaande de eerste lijns EDP-audit;
- de reikwijdte van de eerste lijns EDP-audit, waarbij aandacht zal worden besteed aan de daarbij te hanteren kwaliteitscriteria en te beoordelen objecten;
- de eerste lijns EDP-audit in relatie tot het hedendaagse op risico-analyse gebaseerde accountantscontroleproces.

INVLOED VAN DE AUTOMATISERING OP DE CONTROLE

De aan de jaarrekening (waarin de uitkomsten van de bedrijfsvoering in financiële zin worden weergegeven) ten grondslag liggende gegevens zullen niet zelden op geautomatiseerde wijze worden bewerkt en vastgelegd. De accountant dient zich rekenschap te geven van de consequenties die de automatisering in de gecontroleerde organisatie heeft voor zijn controle. Het doel van deze beoordeling is het de accountant mogelijk te maken op de meest efficiënte wijze tot een oordeel over de getrouwheid van de jaarrekening te komen [Jenk92]. Soms betekent dit dat de accountant kiest voor een controle-aanpak waarbij hij (geheel of gedeeltelijk) gebruik maakt van de in de automatiseringsorganisatie en geautomatiseerde processen (te zamen: de geautomatiseerde gegevensbewerking) opgenomen maatregelen van interne controle. In bepaalde gevallen heeft de accountant echter geen keuze. De geautomatiseerde gegevensbewerking is dan van dien aard dat een 'traditionele controle-aanpak' buiten de geautomatiseerde gegevensbewerking om niet mogelijk is.

Eerste lijns EDP-audit is voor de accountant van belang.

De noodzakelijke (in het kader van de jaarrekeningcontrole) op de geautomatiseerde gegevensbewerking gerichte werkzaamheden worden veelal uitgevoerd door specialisten (EDP-auditors die al dan niet registeraccountant zijn) die werkzaam zijn bij hetzelfde samenwerkingsverband waarvan ook de accountant deel uitmaakt.[1] De accountant maakt dan gebruik van de bevindingen van deze EDP-auditors. Dit laat echter onverlet dat de accountant een ongedeelde verantwoordelijkheid heeft voor de verklaring bij de jaarrekening. In wezen fungeert de EDP-auditor dan in opdracht en onder supervisie van de accountant. Dit betekent dat de accountant in samenspraak met de EDP-auditor moet kunnen aangeven welke aspecten in het kader van de jaarrekeningcontrole in de EDP-audit moeten worden betrokken. Meer concreet houdt dit in dat de accountant in staat moet worden geacht aan te geven welke onderdelen van de geautomatiseerde gegevensbewerking aan een onderzoek moeten worden onderworpen en welke kwaliteitscriteria, controledoelstellingen en normen daarbij moeten worden gehanteerd. Voorts moet de accountant het rapport van de EDP-auditor op zijn merites kunnen beoordelen en op niveau met hem over zijn bevindingen kunnen communiceren.

Dit artikel gaat niet in op de vraag of de accountant in het algemeen gesproken (mede gelet op de inhoud van de accountantsopleiding) over voldoende deskundigheid beschikt om zijn verantwoordelijkheid in dezen te kunnen dragen. Wel biedt dit artikel de accountant een theoretisch referentiekader om hem bij de eerste lijns EDP-audit te ondersteunen.

Om - volgens de doelstelling van dit artikel - invulling te kunnen geven aan de eerste lijns EDP-audit is het noodzakelijk dat:

a. de structuur van het hedendaagse accountantscontroleproces in beeld wordt gebracht;
b. invulling wordt gegeven aan de inhoud van het kwaliteitsoordeel in het kader van de eerste lijns EDP-audit.

Ad a
In de volgende paragraaf wordt een gestandaardiseerde weergave gepresenteerd van het proces van accountantscontrole zoals dat tegenwoordig in het algemeen wordt toegepast. Deze weergave vormt vervolgens de leidraad aan de hand waarvan invulling aan de eerste lijns EDP-audit wordt gegeven.

Ad b
Het gaat hierbij om het benoemen van de entiteiten van dit kwaliteitsoordeel. Deze entiteiten betreffen:

- de kwaliteitsdoelstelling van de eerste lijns EDP-audit;
- de kwaliteitscriteria waaruit deze kwaliteitsdoelstelling is opgebouwd;
- de objecten van de eerste lijns EDP-audit.

Het middel dat daarvoor gebruikt wordt, zal in dit artikel worden aangeduid met de term kwaliteitsboom. Kwaliteitsbomen worden in wetenschappelijke publikaties regelmatig toegepast om het algemene begrip kwaliteit uit te werken in specifieke daaraan te stellen eisen (zie bijvoorbeeld [Dele90]).

HET ACCOUNTANTSCONTROLEPROCES

De commissie 'Voortgezette Educatie Registeraccountants' (VERA) introduceerde in 1990 de cursus 'COBRA' (Controle beheerst door risico analyse). Daarin wordt een min of meer gestandaardiseerd overzicht gegeven van het op risico-analyse gebaseerde proces van accountantscontrole (zie figuur 1).

Hoe dicht dit concept bij de praktijk staat bewijst een vergelijking daarvan met de controle-aanpak van enkele grote accountantsorganisaties, zoals die enkele jaren geleden in het *MAB* werd gepubliceerd (1989 en 1990). In het kader van dit artikel is daarom besloten het in de COBRA-cursus gehanteerde controleproces als leidraad te hanteren bij de verdere uitwerking van de eerste lijns EDP-audit.

Fasen van het controleproces

Conform figuur 1 worden de volgende fasen in het controleproces onderscheiden:

1 *Geabstraheerd wordt van de situatie dat de op de geautomatiseerde gegevensbewerking gerichte werkzaamheden verricht zijn door EDP-auditors in dienst van de gecontroleerde of door EDP-auditors die niet in dienst van het samenwerkingsverband zijn. In die situaties zal de EDP-auditor niet in opdracht en onder supervisie van de accountant fungeren. Voor het vervolg van het betoog is dit onderscheid echter minder relevant. Van belang is dat de accountant een ongedeelde verantwoordelijkheid heeft, hetgeen hem noopt tot een kritische beoordeling van de verrichte werkzaamheden.*

1. *Voortraject*
Acceptatie van de opdracht, vaststellen van de voorwaarden, opstellen van de opdrachtbevestiging.

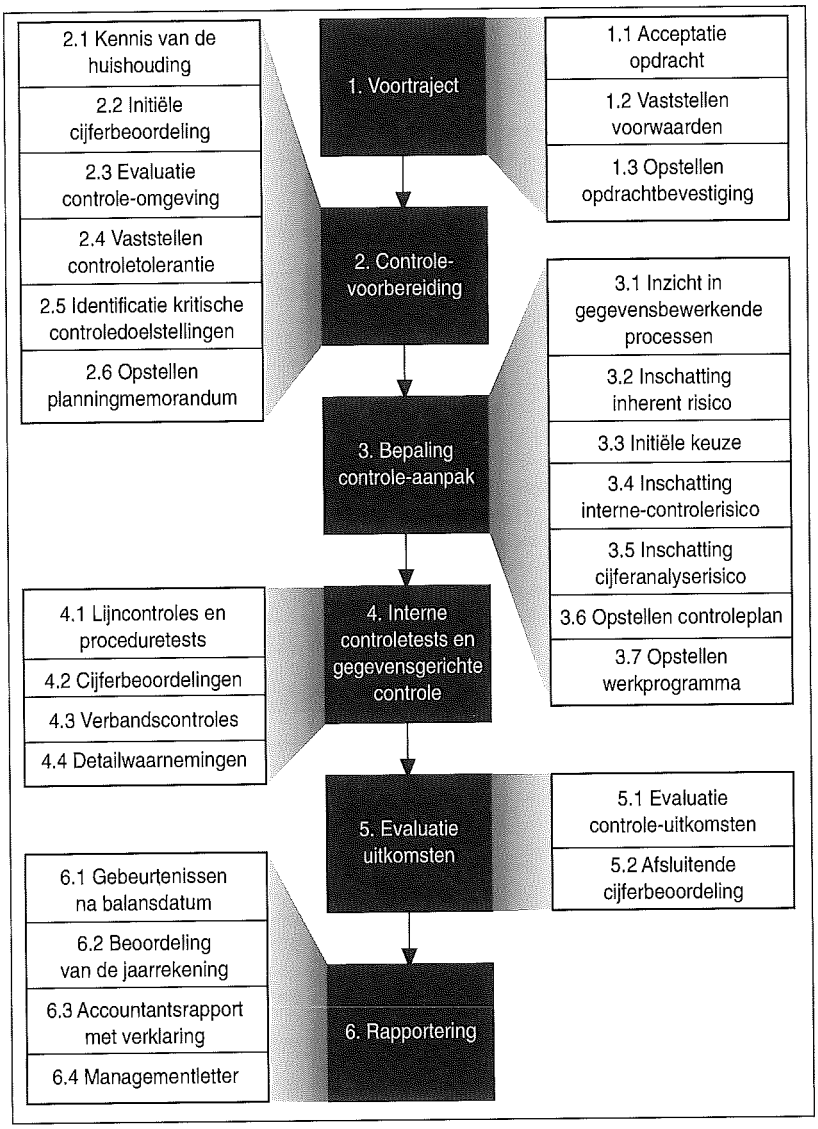
2. *Controlevoorbereiding*
Kennis van de huishouding, initiële cijferbeoordeling, evaluatie controle-omgeving, vaststellen controletolerantie, identificatie kritische controledoelstellingen, opstellen planningmemorandum.

3. *Bepaling controle-aanpak*
Inzicht in de aard en de omvang van de gegevensbewerkende processen, inschatting inherent risico, initiële keuze controle-aanpak, interne-controlerisico en cijferanalyserisico, opstellen controleplan en werkprogramma.

4. *Uitvoering interne-controletests en gegevensgerichte controle*
Lijncontroles en proceduretests, cijferbeoordelingen, verbandscontroles en detailwaarnemingen.

5. *Evaluatie*
Evaluatie controle-uitkomsten, afsluitende cijferbeoordeling.

6. *Rapportering*
Beoordeling gebeurtenissen na balansdatum, beoordeling van de jaarrekening, opstellen accountantsrapport met verklaring, managementletter.



Figuur 1. Het accountantscontroleproces.

KWALITEITSBOOM EERSTE LIJNS EDP-AUDIT

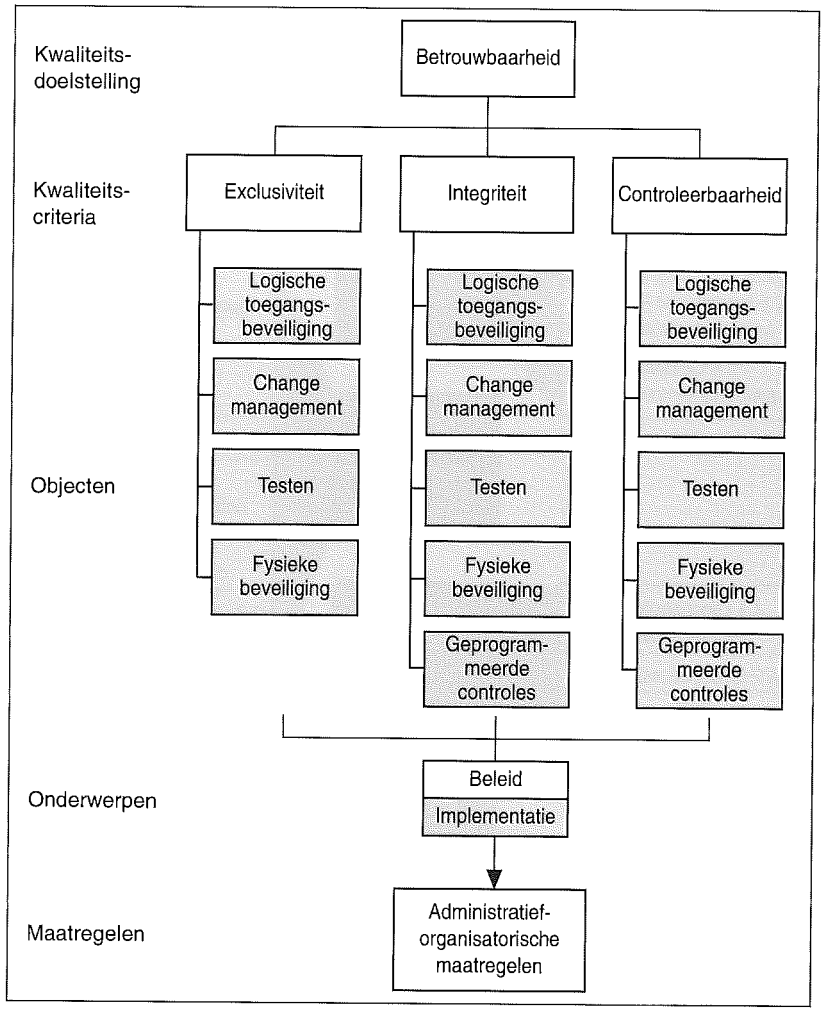
Zoals hiervoor is aangegeven, wordt in deze paragraaf aandacht besteed aan de inhoud van het kwaliteitsoordeel in het kader van de eerste lijns EDP-audit. Dit zal mede op schematische wijze gebeuren in de vorm van een kwaliteitsboom, die is opgenomen in de figuren 2 en 3 op de volgende pagina.

Bovenaan de kwaliteitsboom bevindt zich de kwaliteitsdoelstelling. In casu betreft dit het met de eerste lijns EDP-audit te bereiken doel. Kwaliteitsoordelen over de geautomatiseerde gegevensbewerking kunnen zich richten op de kwaliteitsdoelstellingen betrouwbaarheid, continuïteit, effectiviteit en efficiency [NIvRA89]. Gelet op het met de eerste lijns EDP-audit te bereiken doel komen alleen de betrouwbaarheid en de continuïteit aan de orde.

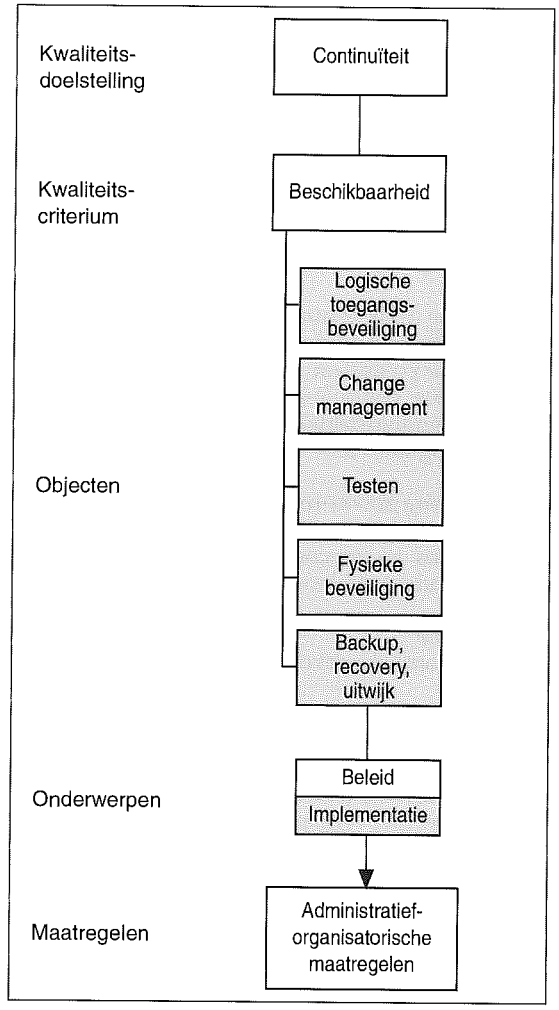
Betrouwbaarheid
Zoals uit figuur 2 blijkt richt de eerste lijns EDP-audit zich op de kwaliteitsdoelstelling betrouwbaarheid. Deze doelstelling vloeit voort uit het met de jaarrekeningcontrole te bereiken doel. Daarmee wordt immers beoogd vast te stellen dat de in de verantwoording opgenomen gegevens overeenstemmen met de werkelijkheid; die verantwoording dient een getrouwe weergave te geven van die werkelijkheid. Het is evident dat een onbetrouwbare geautomatiseerde gegevensbewerking de weergave in de verantwoording kan beïnvloeden.

Continuïteit
Soms wordt de beoordeling van de continuïteit van de geautomatiseerde gegevensbewerking tot de reikwijdte van de jaarrekeningcontrole (en daarmee van de eerste lijns EDP-audit) gerekend. Dit kan bijvoorbeeld uit de bewoordingen van de Wet computercriminaliteit worden afgeleid (zie hiervoor [Moll91] en [NIvRA93]).
In de beschikbare literatuur over de relatie tussen automatisering en jaarrekeningcontrole is echter geen steun te vinden voor deze veronderstelling. Kocks [1986] wijst erop dat 'de continuïteitsproblematiek ten behoeve van de geautomatiseerde gegevensverwerking kan en mag niet tot de controle van de jaarrekening worden gerekend'. Maar ook ander schrijvers wijzen dit expliciet of impliciet af (zie bijvoorbeeld [Frie93] en [Poel93]).

Een en ander betekent dat de kwaliteitsdoelstelling



Figuur 2. Kwaliteitsboom eerste lijns EDP-audit.



Figuur 3. Kwaliteitsboom natuurlijke adviesfunctie

continuïteit niet tot de reikwijdte van de eerste lijns EDP-audit behoort. Met andere woorden, voor het oordeel over de getrouwheid van de jaarrekening sec is het niet noodzakelijk dat de continuïteit van de geautomatiseerde gegevensbewerking in het onderzoek wordt betrokken.
Het bovenstaande betekent echter geenszins dat in de eerste lijns EDP-audit geen aandacht wordt besteed aan de continuïteit van de geautomatiseerde gegevensbewerking. Indien de controle-aanpak gebaseerd is op risico-analyse, zal dat namelijk over het algemeen wel het geval zijn. Alleen vloeien die werkzaamheden dan niet voort uit de controlefunctie van de accountant, maar uit de *natuurlijke adviesfunctie.*

Toelichting
Het doel van de risico-analyse is risico's van het aanwezig zijn van onjuistheden van materieel belang in de te controleren verantwoording te onderkennen, in te schatten en te evalueren [Ontwerp Richtlijnen voor de accountantscontrole (RC) 4.04]. Ten behoeve van de bepaling van het interne-controlerisico moet de accountant onder andere een beoordeling uitvoeren van de opzet van de in de geautomatiseerde gegevensbewerking opgenomen controlemaatregelen. (Dit is uitgewerkt in de paragraaf De eerste lijns EDP-audit in het controleproces.) Beoordeeld worden dan de maatregelen die zich op de betrouwbaarheid richten. Naast de controlefunctie heeft de accountant echter ook een adviesfunctie ten behoeve van de leiding van de organisatie (natuurlijke adviesfunctie). In die hoedanigheid wordt bij deze controle-aanpak van hem verwacht dat hij risico's op het vlak van de continuïteit van de geautomatiseerde gegevensbewerking signaleert en - indien gewenst - adviseert hoe deze risico's het best kunnen worden beheerst [Frie93]. Bij het uitvoeren van de risico-analyse beoordeelt de accountant dus tevens de opzet van de getroffen maatregelen die betrekking hebben op de continuïteit.
In specifieke gevallen is het mogelijk dat de accountant op voorhand een controle-aanpak kiest waarbij hij 'buiten de geautomatiseerde gegevensbewerking om' controleert. Hij voert dan geen evaluatie van de opzet van de in de geautomatiseerde gegevensbewerking opgenomen controlemaatregelen uit. Vanzelfsprekend kan hij dan geen bevin-

dingen rapporteren inzake de betrouwbaarheid en de continuïteit daarvan. Het is zaak dat de accountant - ter vermijding van een verwachtingskloof - in het kader van de opdrachtaanvaarding (zie hierna) geen misverstand laat bestaan over de aard en omvang van zijn werkzaamheden op het terrein van de geautomatiseerde gegevensbewerking.

Computercriminaliteit
Uit het bovenstaande vloeit voort dat de controle-aanpak van invloed is op de rapportering in het kader van de Wet computercriminaliteit. Daarin is bepaald dat de accountant in zijn verslag aan de Raad van Commissarissen en het bestuur 'ten minste melding maakt van zijn bevindingen met betrekking tot de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking.' Een consequente toepassing van de controle-aanpak gebaseerd op risico-analyse leidt daarbij altijd tot bevindingen inzake de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensbewerking. Gelet op de hiervoor vermelde uitzonderingsgevallen verdient het aanbeveling dat de accountant in zijn verslag in ieder geval aan dit onderwerp aandacht besteedt. Hij vermeldt dan of zijn controle-aanpak tot bevindingen heeft geleid en - indien dit het geval is - wat de aard daarvan is.

Logische toegangsbeveiliging
Change management
Testen
Fysieke beveiliging
Geprogrammeerde controles

Figuur 4. Objecten van eerste lijns EDP-audit.

Logische toegangsbeveiliging
Change management
Testen
Fysieke beveiliging
Backup, recovery en uitwijk

Figuur 5. Objecten van de natuurlijke adviesfunctie.

Kwaliteitscriteria

De in de kwaliteitsbomen tot uitdrukking gebrachte criteria zijn een uitwerking van de kwaliteitsdoelstelling. Zij bevatten de kenmerkende elementen waaruit deze doelstelling is opgebouwd. Voor de eerste lijns EDP-audit zijn dit de exclusiviteit, de integriteit en de controleerbaarheid (te zamen de betrouwbaarheid). Ten aanzien van de natuurlijke adviesfunctie is voorts sprake van het kwaliteitscriterium beschikbaarheid (continuïteit). Voor de betekenis van deze kwaliteitscriteria wordt verwezen naar de beschikbare literatuur ter zake (onder andere [NIvRA89] en [Moll89]).

Objecten

De kwaliteitsdoelstelling en de criteria waaruit zij bestaat, richten zich op objecten van geautomatiseerde gegevensbewerking (zie de figuren 4 en 5). De relatie tussen de objecten en de kwaliteitscriteria is weergegeven in de kwaliteitsboom.

De objecten van figuur 4 bestrijken de aandachtsgebieden die minimaal moeten worden beoordeeld om - indien de controle-aanpak dat noodzakelijk maakt - tot een oordeel over de betrouwbaarheid van de geautomatiseerde gegevensbewerking in het kader van de jaarrekeningcontrole te komen. De eerste lijns EDP-audit is daarmee afgegrensd.

De objecten in figuur 5 geven de aandachtsgebieden weer die in het kader van de natuurlijke adviesfunctie ten aanzien van het kwaliteitscriterium beschikbaarheid aan de orde kunnen komen. Het blijkt daarbij dat de objecten die in het kader van de betrouwbaarheid van belang zijn tevens de beschikbaarheid beïnvloeden. Voorts speelt het object 'backup, recovery en uitwijk' daarbij een belangrijke rol.
Aan de keuze van deze objecten liggen de volgende overwegingen ten grondslag.

Logische toegangsbeveiliging
Logische toegangsbeveiliging heeft betrekking op alle organisatorische en softwarematig getroffen maatregelen die erop gericht zijn toegang tot de apparatuur en toepassingen te beschermen tegen benadering door ongeautoriseerde personen [Bruy89]. Als zodanig beïnvloedt de logische toegangsbeveiliging alle criteria en zal zij in de eerste lijns EDP-audit aan een beoordeling worden onderworpen.

Change management
Change management is het proces van evalueren, plannen en coördineren van de implementatie en van wijzigingen in de apparatuur en toepassingen. Elke wijziging kan - wanneer zij niet adequaat wordt uitgevoerd - de kwaliteitscriteria beïnvloeden. In de eerste lijns EDP-audit wordt vastgesteld dat het wijzigingsproces zowel beleidsmatig als qua uitvoering en controle op het verloop daarvan toereikend is ingericht.

Testen
Testen heeft betrekking op de verificatie van apparatuur en toepassingen om vast te stellen of deze gebouwd of onderhouden zijn volgens de vooraf door de gebruikers vastgestelde specificaties. Testen vormt de belangrijkste schakel in het ontwikkelingsproces en vormt een belangrijke waarborg voor een toereikende change management. Bepaalde auteurs (onder andere [Frie93]) menen

dat het in het kader van de jaarrekeningcontrole noodzakelijk is het gehele ontwikkelingsproces te beoordelen. Die mening deel ik echter niet.
De doelstelling van de eerste lijns EDP-audit is het vaststellen van de getrouwheid van de geautomatiseerde gegevensbewerking. Het is dan bij een interne-controlegerichte benadering gewoonlijk toereikend vast te stellen dat:
- de functiescheidingen tussen de ontwikkelings-, test- en produktie-afdelingen voldoende zijn geweest;
- de opzet en werking van de testfunctie voldoende is geweest.

Tijdens de testfase zal blijken of de waarborgen die in het voortraject (probleemanalyse, functioneel ontwerp en technisch ontwerp) zijn gecreëerd, adequaat hebben gewerkt. Onvolkomenheden in het ontwerp die de kwaliteitscriteria (en daarmee de getrouwheid) zouden kunnen aantasten, dienen dan te worden gesignaleerd.

Geprogrammeerde controles
Dit zijn in toepassingsprogramma's opgenomen controles, gericht op het vergelijken van een gegeven met een norm, bij afwijking gevolgd door een signalering aan de gebruiker [Praa92].

Eerste lijns EDP-audit kan op elke organisatie worden toegepast.

Dergelijke controles richten zich vooral op de juistheid, volledigheid en tijdigheid van de bewerkte gegevens. Adequate opzet en werking van geprogrammeerde controles kunnen de gegevensgerichte waarnemingen beperken, hetgeen tot een doelmatiger uitvoering van de algemene controle leidt. De mate waarin de beoordeling van de geprogrammeerde controles deel uitmaakt van de eerste lijns EDP-audit is echter afhankelijk van de controle-aanpak die de accountant voorstaat. Bij een gegevensgerichte aanpak worden het bestaan en de werking daarvan niet in de controle betrokken. (Zie verder hetgeen hieromtrent wordt gezegd in de paragraaf De eerste lijns EDP-audit in het controleproces.)

Fysieke beveiliging
Fysieke beveiliging betreft alle fysieke maatregelen gericht op het selectief aan bepaalde personen toegang verschaffen tot ruimten en apparatuur van de organisatie. Zij beïnvloedt zowel de exclusiviteit als de integriteit en de beschikbaarheid. Een adequate logische toegangsbeveiliging kan onvolkomenheden in de fysieke beveiliging compenseren. Dit geldt echter niet vice versa. Het belang van fysieke beveiliging richt zich dan ook in het bijzonder op het kwaliteitscriterium beschikbaarheid.

Backup, recovery en uitwijk
Hieronder worden alle maatregelen begrepen gericht op het opheffen dan wel compenseren van storingen en calamiteiten [NIvRA89]. De maatregelen richten zich op de beschikbaarheid van de geautomatiseerde gegevensbewerking. De beoordeling die de accountant in dit verband in het kader van de jaarrekeningcontrole uitvoert, verricht hij uit hoofde van zijn natuurlijke adviesfunctie ten behoeve van het management.

Het laatste niveau in de kwaliteitsboom betreffen de maatregelen die in specifieke gevallen getroffen kunnen worden om de kwaliteitscriteria te realiseren. Een onderscheid wordt daarbij gemaakt in beleidsmatige maatregelen en maatregelen die de implementatie betreffen. In het kader van dit artikel worden deze maatregelen echter niet uitgewerkt.

DE EERSTE LIJNS EDP-AUDIT IN HET CONTROLEPROCES

De accountant streeft naar een zo efficiënt mogelijke uitvoering van zijn controle. In dat verband dient hij zich een beeld te vormen van de implicaties van de geautomatiseerde gegevensbewerking op zijn controle(aanpak). Doel daarvan is te bepalen of en zo ja, in welke mate hij voor zijn controle op in de geautomatiseerde gegevensbewerking opgenomen maatregelen van interne controle kan steunen. In de praktijk zal de geautomatiseerde gegevensbewerking dan ook een vast bestanddeel van de controle van de accountant vormen.

De vraag is nu welke rol de geautomatiseerde gegevensbewerking in het - hiervoor uiteengezette gestandaardiseerde - controleproces van de accountant speelt; wat is de inhoud van de eerste lijns EDP-audit? Bij de uitwerking van dit vraagstuk worden de volgende uitgangspunten gehanteerd:

1. Aan de hand van het in de vorige paragraaf geïntroduceerde controleproces zal nu per fase en per onderdeel binnen een fase invulling worden gegeven aan de eerste lijns EDP-audit. De in het kader van de jaarrekeningcontrole te verrichten werkzaamheden die geen betrekking hebben op de geautomatiseerde gegevensbewerking blijven zoveel mogelijk buiten beschouwing.

2. De diepgang van de hierna beschreven werkzaamheden is afhankelijk van de controle-aanpak die de accountant voorstaat. De beschrijving van de eerste lijns EDP-audit is gebaseerd op een risico-analytische benadering (hetgeen door Ontwerp RC 4.04 ook wordt aanbevolen). Voorts worden alle aspecten die in dit kader bij de beoordeling van de geautomatiseerde gegevensbewerking aan de orde kunnen komen, behandeld. Veelal doet zich dit in de praktijk alleen voor in een situatie waarin in belangrijke mate op de in de geautomatiseerde gegevensbewerking opgenomen controles kan worden gesteund. In de beschrijving zal worden aangegeven op welk punt van het controlepro-

ces de controle-aanpak op grond van de bevindingen van karakter kan veranderen.

3. De risico-analytische benadering maakt in zijn algemeenheid geen onderscheid naar typologie en omvang van de te controleren organisatie. Dat betekent tevens dat de eerste lijns EDP-audit in principe op elke organisatie kan worden toegepast. Wel is het zo dat de omvang van de organisatie van invloed is op de controle-aanpak en daarmee op de mate waarin de geautomatiseerde gegevensbewerking aan controle wordt onderworpen.

4. Zoals uit figuur 1 blijkt wordt in twee fasen van het controleproces expliciet aandacht besteed aan de evaluatie van de bevindingen. Daarmee is echter niet gezegd dat de evaluatie zich tot deze fasen zou beperken. Evaluatie van controlebevindingen is een continu proces dat gedurende het hele accountantscontroleproces plaatsvindt. Voortdurend geeft de accountant zich rekenschap van de consequenties die bepaalde bevindingen voor zijn controle hebben en past hij zo nodig zijn controle-aanpak aan.

Voortraject

Acceptatie van de opdracht
Het is van belang dat een accountant - alvorens een opdracht tot controle van de jaarrekening te aanvaarden - zich ervan overtuigt dat geen wezenlijke bezwaren bestaan tegen het aanvaarden van de opdracht. Daartoe zal de accountant - deels na overleg met de potentiële opdrachtgever - een aantal op het bedrijfsgebeuren betrekking hebbende aspecten aan een beoordeling onderwerpen [RC 2.01.2].

Vaktechnisch gezien is van belang dat de accountant zich onder andere een eerste indruk verschaft van de toereikendheid van de administratieve organisatie en het stelsel van maatregelen van interne controle. Belangrijke tekortkomingen op dit gebied kunnen de accountant ervan weerhouden tot een - goedkeurende - verklaring omtrent de getrouwheid van de jaarrekening te komen. In overleg met de opdrachtgever moet dan worden bezien of een controle-opdracht in dat geval nog wel een rationeel doel dient.
In dit verband vormt de accountant zich tevens een eerste indruk van de aard van de geautomatiseerde gegevensbewerking in de te controleren organisatie. Daartoe voert hij één of meer gesprekken met betrokken leidinggevenden en beoordeelt hij zo nodig een beschrijving van het geautomatiseerde systeem van de opdrachtgever.

In het overleg met de potentiële opdrachtgever dat aan het aanvaarden van de opdracht vooraf gaat, dient de accountant duidelijkheid te verschaffen omtrent zijn taak en verantwoordelijkheid ten aanzien van de geautomatiseerde gegevensbewerking in de organisatie. Daarmee moet worden voorkomen dat naderhand bij de opdrachtgever onduidelijkheid zou kunnen bestaan over de aard en de reikwijdte van de uitgevoerde werkzaamheden en de gerapporteerde bevindingen. (Zie ook hetgeen hierover in de paragraaf Kwaliteitsboom eerste lijns EDP-audit is gezegd.)

De accountant maakt de opdrachtgever duidelijk dat zijn verantwoordelijkheid ten aanzien van de controle van de geautomatiseerde gegevensbewerking niet verder reikt dan uit de aard van de jaarrekeningcontrole voortvloeit. Hij geeft daarbij aan dat hij op grond van de Wet computercriminaliteit eventuele bevindingen ten aanzien van de geautomatiseerde gegevensbewerking (voor zover die uit zijn controle voortvloeien) in zijn accountantsverslag zal opnemen.

Vaststellen van de voorwaarden; Opstellen van de opdrachtbevestiging
Specifieke aandachtspunten voor de eerste lijns EDP-audit betreffen de reikwijdte van de op de geautomatiseerde gegevensbewerking betrekking hebbende werkzaamheden. Daarbij gaat de accountant tevens in op de betekenis van de Wet computercriminaliteit voor zijn controle en rapportering. Deze aspecten worden in de opdrachtbevestiging opgenomen.

Controlevoorbereiding

Kennis van de huishouding
In de fase van de controlevoorbereiding dient de accountant zich een duidelijk beeld te vormen van de huishouding en de omgeving waarbinnen de huishouding functioneert [RC 4.01]. Eén van de onderdelen van deze voorbereidingsfase betreft het verkrijgen van inzicht in de relevante gegevens omtrent de te controleren organisatie. In dit kader dient de accountant zich een beeld te vormen van de aard en omvang van de geautomatiseerde gegevensbewerking. Dit beeld richt zich vooralsnog op de samenhang tussen de geautomatiseerde gegevensbewerking en de rest van de organisatie. In een latere fase heeft hij een meer gedetailleerd inzicht nodig om de in de geautomatiseerde gegevensbewerking opgenomen controlemaatregelen te kunnen beoordelen.
De benodigde controle-informatie verkrijgt de accountant door gesprekken te voeren met betrokken leidinggevenden. Voorts maakt hij daarvoor gebruik van in de organisatie aanwezige beschrijvingen van de automatiseringsorganisatie en de belangrijkste in gebruik zijnde systemen (met inbegrip van de functionaliteiten van die systemen). Bij afwezigheid daarvan dient de accountant - noodgedwongen - deze beschrijvingen zelf te vervaardigen.

Initiële cijferbeoordeling
Het uitvoeren van de initiële cijferbeoordeling leidt niet tot specifieke aandachtspunten voor de eerste lijns EDP-audit.

Evaluatie van de controle-omgeving
Richtinggevend voor de aanpak van de controle is de evaluatie van de controle-omgeving. De evalu-

atie is noodzakelijk om een indruk te krijgen van de wijze waarop de leiding omgaat met interne controle.

Ten aanzien van de geautomatiseerde gegevensbewerking dient de accountant inzicht te krijgen in het belang dat de leiding van de organisatie hecht aan de automatisering. In het bijzonder geldt dit voor de betrouwbaarheid van de geautomatiseerde gegevensbewerking, die immers in het kader van het oordeel over de getrouwheid van de verantwoording voor de accountant het meest relevant is. Daartoe voert de accountant een beoordeling uit van de opzet van de in de geautomatiseerde gegevensbewerking opgenomen controlemaatregelen, voor zover die voor zijn controle van belang zijn[2] (processen die voor het oordeel over de getrouwheid van de jaarrekening van mineur belang zijn laat hij buiten beschouwing). Hij maakt daarvoor gebruik van de hiervoor reeds vermelde beschrijvingen van de automatiseringsorganisatie en van de geautomatiseerde systemen. Daarbij richt hij zich op de volgende hiervoor onderkende objecten:

- logische toegangsbeveiliging;
- testen;
- change management.

De diepgang van beoordelen van 'general controls' is afhankelijk van de controle-aanpak.

De maatregelen die de accountant in dat verband beoordeelt worden wel omschreven als 'general controls'. Dit zijn de maatregelen van interne controle in de automatiseringsorganisatie en in de toepassingsprogramma's, die ervoor zorgen dat de 'application controls' blijvend en juist functioneren. 'Application controls' zijn in de toepassingsprogramma's opgenomen maatregelen van interne controle. De opzet van de 'application controls' komt eerst in de fase 'controle-aanpak' aan de orde. Daarin kiest de accountant de processen die hij interne-controlegericht wenst te controleren. Om die keuze te kunnen maken dient hij de eventueel in de toepassingsprogramma's opgenomen controlemaatregelen te beoordelen.
De diepgang waarmee de accountant de hiervoor bedoelde 'general controls' beoordeelt is afhankelijk van de controle-aanpak die hij voorstaat. Dit kan als volgt worden geïllustreerd.

Toelichting
De in de onderdelen 'acceptatie van de opdracht' en 'kennis van de huishouding' verkregen informatie over het functioneren van de huishouding kan de accountant tot het inzicht brengen dat een interne-controlegerichte aanpak (waarbij hij in belangrijke mate steunt op de in de geautomatiseerde gegevensbewerking opgenomen maatregelen van interne controle) tot de meest efficiënte uitvoering van de controle leidt. In dat geval voert hij in dit onderdeel van het controleproces een diepgaande beoordeling van de 'general controls' uit. Daarbij richt hij zich in het bijzonder op die delen van het gegevensbewerkend proces waarop hij wenst te steunen.

Dit is echter anders indien de accountant het inzicht heeft dat de kwaliteit van de geautomatiseerde gegevensbewerking niet van dien aard is dat hij daarop kan steunen. De beoordeling van de 'general controls' is dan meer globaal en dient ter ondersteuning van zijn inzichten. De aanpak van de controle kan dan:

- interne-controlegericht zijn,

onder voorwaarde dat:

- de kwaliteit van de administratieve organisatie en interne controle overigens - afgezien van de geautomatiseerde gegevensbewerking - toereikend is;
- de aard en de omvang van de processen van de gecontroleerde een controle-aanpak buiten de geautomatiseerde gegevensbewerking toelaten;

of:

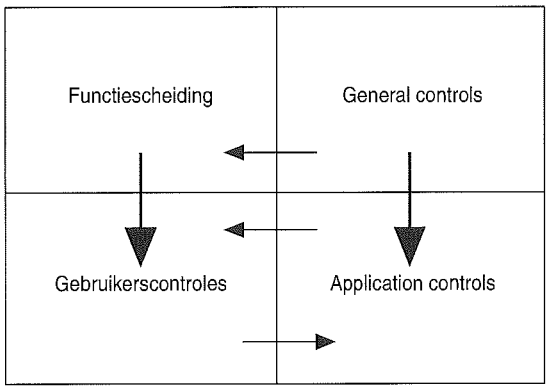
- gegevensgericht zijn,

en wel indien de kwaliteit van de administratieve organisatie en interne controle overigens niet toereikend is voor een interne-controlegerichte aanpak, maar wel voldoende is om de voor de controle minimaal noodzakelijke functiescheidingen te waarborgen.

Toelichting
Zo kan door onvoldoende scheiding tussen de ontwikkel-, test/acceptatie- en produktie-omgevingen onvoldoende aanwijzing bestaan voor de goede werking van geprogrammeerde controles. Bezien moet dan worden of een interne-controlegerichte benadering op de buiten de geautomatiseerde gegevensbewerking opgenomen controlemaatregelen mogelijk is, of dat - indien dit niet mogelijk is - de controle meer gegevensgericht uitgevoerd kan worden door meer op het cijfermateriaal gerichte controlewerkzaamheden. (Voor een uitvoeriger beschouwing over mogelijke tekortkomingen in de controlemaatregelen in de geautomatiseerde gegevensbewerking en de invloed daarvan op de controle-aanpak, wordt verwezen naar Van der Poel en Waardenburg [MAB93].) Indien echter de geautomatiseerde gegevensbewerking vergaand geïntegreerd en complex is, zodat een andere aanpak voor onmogelijk moet worden gehouden, dan zullen de bevindingen invloed hebben op het oordeel en de verklaring van de accountant.

Aangezien dit 'getrapte' keuzeproces regelmatig aanleiding geeft tot discussies, is in figuur 6 een schematisch overzicht opgenomen van de relaties tussen de verschillende elementen van het in een huishouding functionerende interne-controlestelsel. De pijltjes geven die relaties weer.

2 *In figuur 7 is een opsomming opgenomen van de relatie tussen de op de administratieve organisatie en daarmee samenhangende maatregelen van interne controle gerichte werkzaamheden en de eerste lijns EDP-audit.*



Figuur 6. Verhouding AO/IC-maatregelen buiten en binnen de geautomatiseerde gegevensbewerking.

Toelichting
Het rechter gedeelte van de afbeelding heeft betrekking op de maatregelen van interne controle die in de automatiseringsorganisatie worden getroffen. Het linker gedeelte heeft betrekking op de maatregelen die buiten de automatiseringsorganisatie worden getroffen. Zoals uit het schema blijkt, kunnen onvolkomenheden in de 'general controls' in bepaalde gevallen (zie hiervoor) gecompenseerd worden door een adequaat stelsel van functiescheiding buiten de automatiseringsorganisatie. Een interne-controlegerichte aanpak blijft dan mogelijk.

Onder functiescheiding wordt in dit verband verstaan het toedelen van functies aan verschillende personen, zodat een belangentegenstelling ontstaat. Een gebruikerscontrole is een organisatorische maatregel van interne controle die buiten de automatiseringsorganisatie wordt getroffen.
Voorts kunnen manco's in de 'application controls' worden gecompenseerd door gebruikerscontroles (en vice versa). Als de functiescheidingen niet gerealiseerd zijn, kan niet worden gesteund op het blijvend juist functioneren van de gebruikerscontroles. Zoals hiervoor al werd gesteld, zorgen de 'general controls' ervoor dat de 'application controls' blijvend en juist functioneren.

Deze fase van het controleproces (evaluatie van de controle-omgeving) geeft de accountant een eerste indicatie van de mate waarin de in de geautomatiseerde processen opgenomen controlemaatregelen van invloed zijn op zijn controle. Een goed systeem van interne controle leidt dan veelal tot een interne-controlegerichte aanpak, waarbij in belangrijke mate gesteund wordt op de geautomatiseerde gegevensbewerking. Het controleren van het bestaan en de effectieve werking van de daarin opgenomen controlemaatregelen staat dan centraal.

Werkzaamheden uit hoofde van de natuurlijke adviesfunctie
In deze fase van het controleproces besteedt de accountant tevens aandacht aan de opzet van de controlemaatregelen van de objecten die niet direct van invloed zijn op de te controleren verantwoording. Het betreft hier:
- fysieke beveiliging;
- backup, recovery en uitwijk.

Onvolkomenheden hierin die een zeker risico inhouden voor de continuïteit van de geautomatiseerde gegevensbewerking zullen in de managementletter aan de leiding van de organisatie worden gerapporteerd. Voorts zullen deze bevindingen - indien zij daarvoor voldoende relevant zijn - in het kader van de Wet computercriminaliteit worden meegenomen in het accountantsverslag.

Vaststellen controletolerantie
Dit onderdeel van het controleproces levert geen specifieke aandachtspunten voor de eerste lijns EDP-audit.

Identificatie kritische controledoelstellingen
In dit onderdeel van de voorbereidingsfase wordt vastgesteld welke posten en processen en daarbinnen welke getrouwheidsaspecten (juistheid, volledigheid, tijdigheid, eigendom, etc.) kritisch zijn voor het beeld van de jaarrekening: de kritische controledoelstellingen. Deze beoordeling kan zich - afhankelijk van de voorgestane controle-aanpak - tevens op de geautomatiseerde gegevensbewerkende processen richten. De wijze waarop deze beoordeling in dat geval moet worden verricht, vertoont echter geen aanmerkelijke verschillen met de beoordeling van niet-geautomatiseerde processen.

Opstellen van het planningmemorandum
De bevindingen uit de voorgaande stappen worden op systematische wijze vastgelegd. Voor wat betreft de geautomatiseerde gegevensbewerking wordt onder andere aangegeven welke geautomatiseerde systemen bij de gecontroleerde aanwezig zijn en welke invloed daarvan uitgaat op de controle. In het memorandum wordt aandacht besteed aan de in de geautomatiseerde gegevensbewerking opgenomen functiescheidingen en andere controlemaatregelen, alsmede de mogelijkheden die een en ander biedt voor een interne-controlegerichte aanpak. Tot slot moet worden aangegeven of en zo ja, in welke mate de ondersteuning van een EDP-auditor wenselijk wordt geacht. Factoren die de wenselijkheid daarvan bepalen zijn onder andere:
- de mate waarin de accountant denkt te kunnen steunen op de in de geautomatiseerde gegevensbewerking opgenomen controlemaatregelen, in relatie tot de aard en omvang van deze geautomatiseerde gegevensbewerking;
- verwachtingen bij de opdrachtgever;
- kennis en ervaring van de accountant.

Bepaling controle-aanpak

Inzicht in de gegevensbewerkende processen
De evaluatie van de controle-omgeving kan tot de conclusie leiden dat de opzet van de 'general controls' van voldoende niveau is om op te steunen. In deze fase van het controleproces gaat de accoun-

tant vervolgens na of het ook mogelijk is te steunen op de in de processen opgenomen 'application controls'. Daartoe voert hij (zo nodig met hulp van een EDP-auditor) een diepgaande beoordeling uit van de eventueel in de organisatie aanwezige proces- en systeembeschrijvingen. Voorts voert hij interviews uit met gebruikers en beheerders van die systemen.

Inschatting inherent risico
Bij de inschatting van het inherent risico per gegevensbewerkend proces spelen de aard en de omvang van de geautomatiseerde gegevensbewerking een rol. Processen die worden uitgevoerd met behulp van bijvoorbeeld verouderde systemen die tevens slecht onderhouden of storingsgevoelig zijn, leiden tot een hoger inherent risico voor het betreffende te controleren proces.
De accountant baseert zijn beslissing ter zake veelal op interviews met gebruikers en beheerders, alsmede op de uitkomsten van zijn initiële cijferbeoordeling. Voorts zal hij zo nodig zijn inzichten onderbouwen door beoordeling van bescheiden (bijvoorbeeld onderhoudscontracten).

Een controle
waarbij de accountant in belangrijke mate steunt op
de in de geautomatiseerde gegevensbewerking
opgenomen controlemaatregelen,
eist dat hij
het bestaan en de werking daarvan controleert.

Per routinematig proces initiële keuze: interne-controlegerichte of gegevensgerichte controle-aanpak
Op basis van de in de voorgaande fasen van het controleproces uitgevoerde werkzaamheden dient de accountant nu per proces een keuze te maken tussen een interne-controlegerichte en een gegevensgerichte controle-aanpak. In het bijzonder maakt hij hiervoor gebruik van zijn bevindingen omtrent de opzet van de genomen controlemaatregelen, zoals vastgesteld bij de stappen 'evaluatie controle-omgeving' en 'inzicht in de gegevensbewerkende processen'.
Ten aanzien van de geautomatiseerde gegevensbewerking is van belang dat de accountant moet aangeven op welke geautomatiseerde processen hij wil steunen. Zijn conclusies daarover baseert hij op de in het onderdeel 'inzicht in de gegevensbewerkende processen' uitgevoerde beoordelingen.

Inschatting interne-controlerisico
De bevindingen uit de voorgaande fasen van het controleproces, te zamen met de resultaten van de beoordeling van de opzet van de in de geautomatiseerde processen opgenomen controlemaatregelen, maken het de accountant mogelijk een inschatting te maken van het interne-controlerisico. Te zamen met de inschatting van het cijferanalyserisico kan dan gefundeerd - in het controleplan en in het werkprogramma - worden aangegeven in welke mate interne-controletests en gegevensgerichte controlewerkzaamheden nodig zijn om een deugdelijke grondslag voor de verklaring te leggen.

Inschatting cijferanalyserisico
Voor wat betreft de geautomatiseerde gegevensbewerking doen zich met betrekking tot dit onderdeel van het controleproces geen specifieke problemen voor.

Opstellen controleplan en werkprogramma
Voor wat betreft de geautomatiseerde gegevensbewerking vermeldt de accountant in het controleplan op basis van de risico-inschattingen, welke en hoeveel in de geautomatiseerde gegevensbewerking opgenomen interne controles op bestaan en werking moeten worden gecontroleerd. Deze controle strekt zich uit over zowel de 'application controls' als de 'general controls'.
Een en ander leidt tot een gedetailleerde weergave van de aard en omvang van de uit te voeren lijncontroles en proceduretests.
Voorts bepaalt hij welke en hoeveel gegevensgerichte waarnemingen moeten worden verricht om de vereiste controlezekerheid te krijgen.

Uitvoering interne-controletests en gegevensgerichte controle

Lijncontroles en proceduretests
Een controle waarbij de accountant in belangrijke mate steunt op de in de geautomatiseerde gegevensbewerking opgenomen controlemaatregelen, eist dat hij het bestaan en de werking daarvan controleert. Van belang is te onderkennen dat in de voorgaande stappen van het controleproces al een beoordeling heeft plaatsgevonden van de opzet van de in de automatiseringsorganisatie en toepassingsprogramma's opgenomen controlemaatregelen. In dit onderdeel van het controleproces richt de beoordeling zich dan ook op het bestaan en de werking daarvan. Lijncontroles worden uitgevoerd om het bestaan vast te stellen. Proceduretests richten zich op de werking van de controlemaatregelen.
De bevindingen kunnen eventueel leiden tot bijstelling van de inschatting van de uit te voeren gegevensgerichte controleverrichtingen.

Voorbeeld
Het controleren van het bestaan van adequate testprocedures ('general control') kan geschieden door een lijncontrole uit te voeren waarbij de afhandeling van een concreet opgeleverd systeem aan de hand van beschikbare testrapporten wordt nagegaan. De werking van de testprocedure stelt de accountant vast door een beoordeling van testverslagen. Daarbij zal hij zich onder andere richten op de

inhoud van de door de ontwikkelings-, gebruikers- en verwerkingsorganisatie gemaakte opmerkingen en de afwerking daarvan.
Het controleren van het bestaan en de werking van 'application controls' is veelal geen losstaande activiteit. Zij vindt plaats door gebruik te maken van de waarborgen die de automatiseringsorganisatie biedt. Daarbij is vooral de werking van adequate testprocedures en een adequaat werkend change management-proces van belang.

Cijferbeoordelingen, verbandscontroles en detailwaarnemingen
De vorige fasen van het controleproces kunnen voldoende controle-informatie hebben opgeleverd over de effectieve opzet, bestaan en werking van de geautomatiseerde gegevensbewerking. In dat geval kan voor het uitvoeren van cijferbeoordelingen en verbandscontroles gebruik worden gemaakt van door middel van de geautomatiseerde gegevensbewerking verkregen cijfers. Voorts maakt deze controlebenadering het noodzakelijk dat de accountant aandacht besteedt aan de werking van de maatregelen die de continuïteit van de geautomatiseerde gegevensbewerking waarborgen. Hij doet dit uit hoofde van zijn natuurlijke adviesfunctie.

Evaluatie uitkomsten

Evaluatie controlebevindingen
Op zich heeft de evaluatie van de controlebevindingen in dit onderdeel van het controleproces geen specifieke elementen ten aanzien van de geautomatiseerde gegevensbewerking in zich. Eerder is namelijk de invloed van de bevindingen over de opzet, het bestaan en de werking van de in de automatiseringsorganisatie en toepassingsprogramma's opgenomen controlemaatregelen op de verdere controle-aanpak van de accountant al afgewogen. Deze bevindingen kunnen ertoe leiden dat de voorgestelde aanpak van de controle moet worden heroverwogen.

Afsluitende cijferbeoordeling
Voor wat betreft de geautomatiseerde gegevensbewerking doen zich met betrekking tot dit onderdeel van het controleproces geen specifieke problemen voor.

Rapportering

Gebeurtenissen na balansdatum; Beoordeling van de jaarrekening
Voor wat betreft de geautomatiseerde gegevensbewerking doen zich met betrekking tot deze onderdelen van het controleproces geen specifieke problemen voor.

Accountantsrapport met verklaring
Hiervoor is al stilgestaan bij de invloed van de bevindingen van de beoordeling van de geautomatiseerde gegevensbewerking op het oordeel en de verklaring van de accountant. In ieder geval verplichten wettelijke bepalingen (BW2, titel 9, artikel 393, vierde lid) de accountant in zijn aan het bestuur van de gecontroleerde organisatie uitgebrachte accountantsverslag melding te maken van zijn bevindingen inzake de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensbewerking, voor zover die uit de jaarrekeningcontrole voortvloeien.

Onderdeel	Activiteit	Maatregelen	Soort
Controle-voorbereiding	Evaluatie controle-omgeving	Opzet van de in de geautomatiseerde gegevensbewerking opgenomen maatregelen, voor zover van belang voor de algemene controle: - logische toegangsbeveiliging; - change management; - testen. Uit hoofde van de adviserende functie: de opzet van de maatregelen ten aanzien van - fysieke beveiliging; - backup, recovery en uitwijk.	General controls
Bepaling controle-aanpak	Inzicht in gegevensbewerkende processen	De opzet van de in de geautomatiseerde gegevensbewerkende processen opgenomen maatregelen: - geprogrammeerde controles.	Application controls
Interne-controletests en gegevensgerichte controle	Lijncontroles en proceduretests	Het bestaan en de werking van de in de processen en automatiseringsorganisatie opgenomen maatregelen.	General en Application controls

Figuur 7. Op de AO/IC gerichte werkzaamheden en eerste lijns EDP-audit.

Managementletter
Naast het accountantsverslag stelt de accountant veelal tevens een managementletter voor de directie op. Daarin gaat hij voornamelijk meer in detail in op de uit de controle voortvloeiende bevindingen die op de interne organisatie van de gecontroleerde betrekking hebben.
Ten aanzien van de geautomatiseerde gegevensbewerking biedt de managementletter de accountant de mogelijkheid de directie te attenderen op onvolkomenheden op dat punt en eventueel voorstellen

R.A. Jonker RA
Is research-medewerker bij het Directoraat Vaktechniek van het NIvRA.
Een woord van dank gaat uit naar de leden van de werkgroep Standaarden en Normen, zonder wier inbreng dit artikel niet geschreven had kunnen worden. Het artikel is op persoonlijke titel geschreven.

te doen tot opheffing daarvan. Een en ander past binnen de uit de controlefunctie voortvloeiende natuurlijke adviesfunctie van de accountant.

TOT SLOT

In deze beschouwing is inhoud gegeven aan de zogenaamde eerste lijns EDP-audit. Dit is gebeurd aan de hand van het op risico-analyse gebaseerde accountantscontroleproces, zoals dit inmiddels op ruime schaal in het kader van de jaarrekeningcontrole wordt toegepast. Dat betekent dat het geschetste theoretische referentiekader voor de eerste lijns EDP-audit ook kan worden toegepast bij organisaties van geringe omvang waar de automatisering een minder prominente rol vervult. De risicoanalytische benadering maakt immers in haar opzet geen onderscheid in de omvang van de te controleren organisatie en leidt bij consequente toepassing daarvan tot de geschikte controle-aanpak.

LITERATUUR

[Bruy89] P. Bruyninckx en J.P.G. Frints, *Toegangsbeveiliging*, in: Automatisering onder controle, 1989.

[Dele90] G.P.A.J. Delen en D.B.B. Rijsenbrij, *Kwaliteitsattributen van automatiseringsprojecten en informatiesystemen*, Informatie nr. 1 1990.

[Frie93] A.B. Frielink en H. de Heer, *Leerboek Accountantscontrole*, deel 3B, Stenfert Kroese, 1993.

[Jenk92] Brian Jenkins et al., *An Audit Approach to computers*, The Institute of Chartered Accountants in England and Wales, 1992.

[Kock86] H.C. Kocks, *Accountant - automatisering en continuïteit*, in: 24 over EDP-auditing, Samsom, 1986.

[Moll89] K. IJ. Mollema, *Controle van de informatieverwerking*, Samsom, 1989.

[Moll91] K.IJ. Mollema en H. Franken, *Jaarrekening en computerbeveiliging*, De Accountant, november 1991.

[NIvRA89] NIvRA, *Automatisering en controle, deel VII 'Kwaliteitsoordelen over informatievoorziening'*, NIvRA-geschrift 53, Kluwer, 1989.

[NIvRA93] NIvRA, *Computercriminaliteit*, NIvRA-geschrift 62, Kluwer, 1993.

[Poel93] W.G. van der Poel en J. Waardenburg, *Jaarrekeningcontrole en EDP audit*, MAB, mei 1993.

[Praa92] Jan van Praat en Hans Suerink, *Inleiding EDP-auditing: kwaliteitscontrole en beveiliging van informatiesystemen*, Kluwer Bedrijfswetenschappen, 1992.

[RC 2.01.2] Richtlijnen voor de accountantscontrole, *Aanvaarding en bevestiging van opdrachten tot controle van verantwoordingen*, NIvRA, 1987.

[Ontwerp RC 4.04] Richtlijnen voor de accountantscontrole, *Risico-analyse*, NIvRA, 1992.

De invloed van informatietechnologie op de interne-controle-principes

J.C. Boer RE RA

Informatietechnologie begint een steeds grotere invloed te krijgen op de wijze waarop ondernemingen hun administratie inrichten. Het stempel dat zij op de administratieve organisatie drukt heeft zijn invloed op de interne-controlemaatregelen. Klassieke maatregelen als de controletechnische functiescheiding bieden in vele gevallen niet langer een oplossing. Maatregelen in de vorm van in de gebruikte informatietechnologie opgenomen betrouwbaarheidswaarborgen komen hiervoor in de plaats. Creativiteit en oog voor het auditaspect moeten de individuele accountant helpen zich een weg te banen door dit grotendeels onontgonnen gebied.

INLEIDING

De beïnvloeding van de administratieve organisatie door toegepaste informatietechnologie (IT) is geen nieuw fenomeen. De wisselwerking tussen de inrichting van informatiesystemen en de administratieve organisatie bestaat al vanaf het ontstaan van de eerste administratieve toepassing van computers. Door de toenemende mogelijkheden en lagere prijs/prestatie-verhouding neemt het aandeel van informatietechnologie in het gehele registratieve en administratieve proces ten opzichte van de door mensen uitgevoerde procedures toe. Niet alleen in het grootbedrijf maar ook in het MKB-segment van het bedrijfsleven. De thans voorhanden zijnde mogelijkheden tot het gebruik van informatietechnologie hebben hun invloed op de administratieve organisatie en de daarin opgenomen maatregelen van interne controle.

Dit artikel gaat slechts zijdelings in op de invloed van informatietechnologie op de administratieve organisatie. Vandaag de dag wordt tegen automatisering over het algemeen breder aangekeken dan in de zin van alleen het geautomatiseerde systeem. De veranderingen in de informatieverwerking zijn gericht op een optimalisatie van de bedrijfsprocessen gebruik makend van de mogelijkheden die door informatietechnologie worden geboden. De verschuiving van handmatige processen naar geautomatiseerde processen heeft haar invloed op de wijze waarop de processen door interne-controlemaatregelen worden beheerst. Het gebruik van informatietechnologie vraagt om andere beheersingsmaatregelen dan een handmatige omgeving.

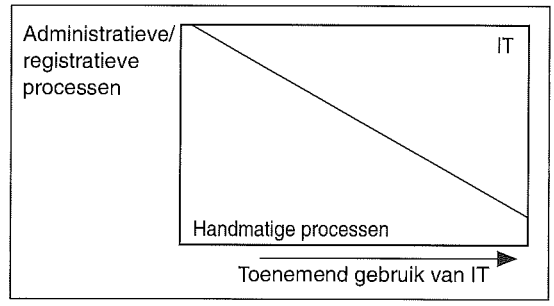
Een aanloopje tot het onderwerp wordt gevormd door een korte beschouwing van de opkomst van informatietechnologie. Hierbij wordt niet zozeer ingegaan op de technische kanten. Vooral door de ontwikkeling van informatietechnologie mogelijk gemaakte veranderingen in de inrichting van administratieve processen worden belicht. Een intensief gebruik van de mogelijkheden die informatietechnologie biedt voor het optimaliseren van de bedrijfsprocessen heeft zijn invloed op de wijze waarop de organisatie door het verantwoordelijk management kan worden beheerst. Een veranderende organisatie, maar vooral veranderingen in de interne-controleprocessen stellen nieuwe eisen ten aanzien van de kennis van een accountant. Deze kennis is noodzakelijk om de betrouwbaarheid van administratieve processen te kunnen beoordelen en om invulling te kunnen geven aan zijn adviesfunctie op het terrein van registratieve en administratieve processen.

In het grootbedrijf is deze kennis onontbeerlijk voor een beoordeling van de mate waarin de bedrijfsleiding de complexe processen beheerst. Daarnaast wordt het vooral in het MKB-segment als vanzelfsprekend beschouwd dat de accountant de deskundige adviseur is met betrekking tot de beheersing van de betrouwbaarheid van de registratieve administratieve processen.

ONTWIKKELINGEN IN DE GEAUTOMATISEERDE GEGEVENSVERWERKING

In de afgelopen veertig jaar heeft de geautomatiseerde gegevensverwerking een snelle ontwikkeling doorgemaakt. De nieuwe IT-middelen bleken uitstekend te voldoen als hulpmiddel voor de verbetering van de efficiëntie van de informatieverwerking binnen bedrijven. Het eerste voordeel voor bedrijfshuishoudingen lag niet zozeer in kostenbesparingen, maar in een betere informatievoorziening tegen gelijke of relatief gering hogere kosten. Het terugdringen van de kosten van de gegevensverwerking wordt bij de bedrijven die de informatievoorziening op het gewenste peil hebben, actueel. Wijzigingen worden dan ingegeven door de wens processen efficiënter (sneller en goedkoper) te laten verlopen. Dit laatste kan worden gerealiseerd door een herontwerp van het informatieverwerkende proces (figuur 1). De snelheidswinst en de kostenbesparing worden hierbij in het algemeen bereikt door:

- het integreren van processen waardoor tussenstappen en logische tussenbestanden vervallen;
- verkleining van de verwerkingsstapels (batches), waardoor een doorlopende realtimeverwerking ontstaat.



Figuur 1. IT-aandeel in processen.

Het gevolg hiervan is arbeidsbesparing en korte doorlooptijden, hetgeen echter leidt tot een toename van de complexiteit van de informatiesystemen en de afhankelijkheid van informatietechnologie.

Integratie

Integratie leidt ertoe dat nog slechts sprake is van een enkelvoudige vastlegging. Registraties ten behoeve van de produktiesturing resulteren direct in mutaties van voorraden en onderhanden werk. Vastleggingen door de afdeling personeelszaken behoeven, voor zover zij invloed hebben op de salarisuitbetaling, geen tweede invoer; het personeelsinformatiesysteem zorgt voor de invoer van de mutatie in de geautomatiseerde salarisadministratie. Dit zijn slechts enkele voorbeelden.

De integratietendens grijpt echter verder om zich heen. De bedrijfsgrenzen vervagen doordat afnemers de data entry in de bedrijfsinformatiesystemen gaan verzorgen (EDI). Denk hierbij aan het elektronisch bestellen en aan toepassingen als electronic banking. Ook de uitgaande informatiestroom kan de vorm hebben van datacommunicatie (bijvoorbeeld elektronisch factureren). Bezien vanuit een administratief-organisatorisch gezichtspunt is niet de datacommunicatie een fundamentele wijziging, maar het vervallen van handelingen gericht op de eerste vastlegging en de autorisatie door middel van een fysieke handeling.

Integratie leidt tot het vervallen van dubbele registratie van gegevens voor verschillende doelen, waardoor tevens de mogelijkheid vervalt tot controle door het vergelijken van twee door verschillende bedrijfsfuncties onderhouden administraties. Administratief-organisatorisch gezien is de grote verandering die door EDI ontstaat de directe koppeling tussen externe informatie aanleverende of informatie accepterende systemen zonder dat dit op transactieniveau vergezeld gaat van direct tastbare acceptaties en autorisaties. De toepassing van informatietechnologie gaat een steeds groter stempel drukken op de inrichting van administratieve en registratieve processen binnen ondernemingen en instellingen. Het gevolg van de verandering van de administratieve processen is dat ook de wijze waarop de processen beheerst worden, zal veranderen. De oude maatregelen passen niet meer, nieuwe mogelijkheden liggen in het verschiet.

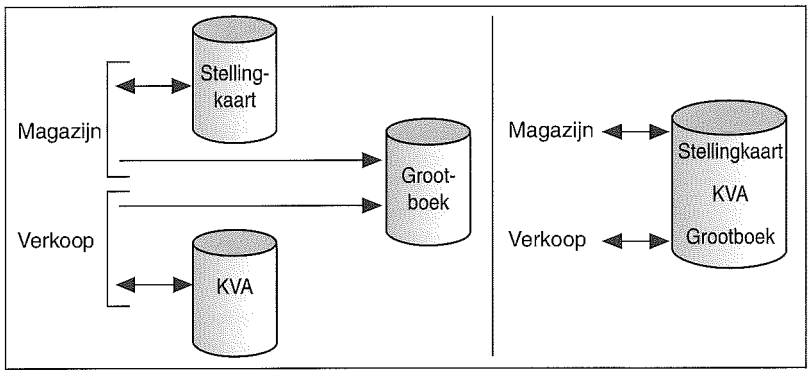
Verkleining verwerkingsstapels

Door verkleining van de verwerkingsstapels (batch) wordt de snelheid van het informatieproces en daarmee de bedrijfsvoering aanzienlijk verhoogd. Dit sluit aan bij de in de maatschappij aanwezige tendens om transactiecyclussen te versnellen. Klanten accepteren het niet meer om weken op een uitkering van een ziektekostenverzekering te moeten wachten. De typologie van de logistiek van het administratieve proces verschuift van een partijgewijze (discrete) organisatie naar een procesorganisatie.
Een ander niet altijd direct gesignaleerd gevolg van de verkleining van de verwerkingsstapels is een toename van de massaliteit. Het aantal transacties zal ten opzichte van het totale transactievolume toenemen. Met andere woorden, de omvang van de gemiddelde transactie neemt af. Deze ontwikkeling is mogelijk door de directe beschikbaarheid van het transactieverwerkende proces; uit oogpunt van efficiëntie is het samenvoegen van transacties niet meer nodig.

ADMINISTRATIEVE ORGANISATIE INCLUSIEF INFORMATIETECHNOLOGIE

Klassiek is het begrip administratieve organisatie inclusief interne controle. In het vakgebied is dikwijls de discussie gevoerd of de toevoeging 'interne controle' niet een herhaling is omdat dit al begrepen is in 'administratieve organisatie'. De toe-

voeging heeft mijns inziens stand gehouden om te accentueren dat de beheersingsmaatregelen deel uitmaken van het geheel van procedures. De vraag is of dit accent nog wel nodig is. De beheersing is thans vooral gelegen in de betrouwbaarheid van de gebruikte IT-hulpmiddelen en de opvolging door functionarissen van door de informatiesystemen afgegeven signalen. Om informatietechnologie als bepalend element in de opzet en werking van de administratieve organisatie te accentueren wordt voorgesteld voortaan te spreken van AO/IT.



Figuur 2. Integratie registraties.

Klassieke interne controle

De administratieve organisatie is gericht op een betrouwbare, tijdige informatieverwerking en de beveiliging van de bezittingen van de organisatie door een stringente registratie en periodieke inventarisatie. Waar mensen werken worden fouten gemaakt. Interne-controlemaatregelen moeten ervoor zorgen dat deze fouten niet onopgemerkt blijven. De efficiency stond in de klassieke leerboeken over de bestuurlijke informatieverzorging op de tweede plaats. De hoeveelheid door mensen te verrichten handelingen was toentertijd een onbeïnvloedbaar gegeven.

De belangrijkste beheersingsmaatregelen berusten op functiescheiding. Hierbij wordt gebruik gemaakt van de benodigde personele capaciteit voor het uitvoeren van de registratieve en administratieve processen. De veelheid van taken die door medewerkers worden uitgevoerd, maakte een werkverdeling noodzakelijk. De beheersing van de administratieve processen kon eenvoudig worden bereikt met een zodanige verdeling van taken dat een situatie ontstond waarin medewerkers tegengestelde belangen hadden. Om de vele betrokkenen efficiënt te laten werken bouwden zij uit hun eigen bronnen registraties op. Deze registraties (bijvoorbeeld kantoorvoorraadadministratie en stellingkaarten) waren in eerste instantie niet opgebouwd voor interne-controledoeleinden. Het waren hulpmiddelen voor de betreffende functionarissen om hun werk uit te voeren.
De uit de administratieve logistiek voortkomende dubbele registraties gaven de bedrijfsleiding een mogelijkheid om door een afstemming van beide registraties vast te stellen dat de administratie een betrouwbare weergave van de werkelijkheid is.

Van AO/IC naar AO/IT

Informatietechnologie neemt in steeds grotere mate taken over die voorheen door mensen werden vervuld. Door het gebruik van geïntegreerde informatietechnologie kan worden volstaan met een gemeenschappelijke registratie die door verschillende bedrijfsfuncties wordt gebruikt. Het voeren van dubbele administraties is niet meer nodig omdat vanaf verschillende werkplekken dezelfde gegevens in een eigen presentatie kunnen worden gebruikt (figuur 2).

De mogelijkheden tot fysieke functiescheiding worden minder omdat opeenvolgende stappen in het registratieve en administratieve proces door informatiesystemen worden uitgevoerd. De administratieve grenzen van de eigen onderneming en de buitenwereld vervagen door de directe gegevensontvangst en -verzending van en naar derden. Wat zijn nu de gevolgen voor de beheersing van de informatievoorziening binnen een bedrijf? Om een antwoord op deze vraag te vinden moeten we teruggaan naar de doelstelling van de controletechnische functiescheidingen en de overige daaraan ondergeschikte maatregelen van interne controle, namelijk het tijdig signaleren van fouten tijdens het verwerkingsproces en het waarborgen van de autorisatie van beschikbare handelingen. Als de werkzaamheden niet meer door personen worden uitgevoerd, vervalt de noodzaak van interne controle op de door hen uitgevoerde werkzaamheden. Hetzelfde geldt voor de dubbele registraties. Deze worden over het algemeen vervangen door één registratie, waardoor een belangrijke foutenbron, een accuratessefout in één van beide registraties, komt te vervallen.

Nu de controletechnische functiescheidingen en dubbele registratie aan betekenis inboeten, moet naar andere middelen worden gezocht die de betrouwbaarheid van de administratieve processen kunnen waarborgen. In tegenstelling tot de maatregel controletechnische functiescheiding bestaat er in de administratieve organisatie jammer genoeg geen tweede algemeen toepasbaar principe. De oplossing is gelegen in het ontwerp van een doordacht stelsel van geprogrammeerde maatregelen in samenhang met door de verantwoordelijke functionarissen uit te voeren autorisatie-, controle- en correctietaken. Het specifieke is erin gelegen dat het IC-stelsel moet aansluiten met de logistiek van het administratieve proces.

Binnen de kaders van dit algemeen signalerend artikel gaat het te ver om aan te geven hoe in een geïntegreerd administratief proces het aspect van interne controle moet worden uitgewerkt. Belangrijk is dat de gekozen interne-controlestructuur aansluit op de structuur van het verwerkingsproces. Deze eis wordt eens te meer ingegeven omdat bij het opzetten van administratieve procedures, met als criterium een optimale administratieve logistiek, de interne-controlemaatregelen niet belemmerend mogen zijn. De kostenbeperking en

versnelling staan dikwijls hoger in het vaandel dan interne controle. Het vreemde is echter dat betrouwbaarheid een aspect is waar informatici als vanzelfsprekend van uitgaan. Deze vanzelfsprekendheid is ingegeven door de betrouwbaarheidswaarborgen die de informatietechnologie biedt. Informatietechnologie kent geen accuratessefouten. Het kenmerk is dat het geautomatiseerde proces systematisch goed of systematisch fout verloopt. Een aantekening die hierbij meestal niet wordt gemaakt, is dat deze stelling slechts geldt voor de geteste situaties. Onvoorziene omstandigheden (programmawijziging, storing in de verwerking, een bijzondere transactie, etc.) kunnen tot onbedoelde effecten leiden.

De moeilijke taak van de voor de informatieverwerking verantwoordelijke functionaris (dikwijls de controller) is om een ieder te overtuigen dat de betrouwbare werking een juiste stelling is, maar wel één die doorlopend moet worden aangetoond. Er mag geen sprake zijn van blind vertrouwen. De acceptatie van binnenkomende informatie (orders, rekeningen, etc.) en de autorisatie van uitgaande stromen (bestellingen, betalingen) moeten gewaarborgd zijn. Aantoonbaar moet worden vastgesteld dat het informatiesysteem een juist en volledig beeld geeft van de werkelijkheid en dat geen ongeautoriseerde in- en uitvoer van gegevens plaatsvindt. Dit kan in een administratief proces waarbij efficiency een belangrijke ontwerpvariabele is, alleen worden gerealiseerd als het ontwerpen van de interne-controlemaatregel een geïntegreerd onderdeel van het ontwerp van de applicatie en van het voorschrijven van menselijke procedures is. Bij het ontwerpen van een IC-maatregel moet de ontwerper zich realiseren dat de geautomatiseerde processen andere risico's kennen dan de handmatige processen en daardoor vragen om andere controlemaatregelen.

GEVOLGEN VOOR DE ACCOUNTANT

De werkzaamheden van een controlerend accountant zijn er in de eerste plaats op gericht de betrouwbaarheid van (financiële) verantwoordingsverslagen vast te stellen. Naast zijn controlerende taak zal de accountant in de praktijk geconfronteerd worden met vragen van zijn opdrachtgever over het gebruik van informatietechnologie ter ondersteuning van de registratieve en administratieve processen. Beide aspecten vragen in het tijdperk van de administratieve organisatie inclusief het gebruik van informatietechnologie bijzondere vaardigheden.

Controle-aanpak

Door de algemene beschikbaarheid van de verworvenheden van de IT-hulpmiddelen is er geen bedrijf meer voor te stellen dat geen gebruik maakt van informatietechnologie. De bedrijfsleiding is er over het algemeen alles aan gelegen de basisprocessen (de routineprocessen) efficiënt en vlekkeloos te laten verlopen. Veel fouten leiden tot stijging van de kosten, vertragingen en een teruglopend vertrouwen bij de opdrachtgevers. De beheersing van de administratieve routineprocessen wordt niet meer bereikt door functiescheiding maar door betrouwbare informatiesystemen. In situaties waarin de cliënt zijn uiterste best doet om het administratieve proces te beheersen door een combinatie van in de technische infrastructuur opgenomen controles en enkele gerichte gebruikerscontroles, ligt een systeemgerichte controle-aanpak voor de hand. Hiervoor is kennis van de maatregelen die de verwerkingsomgeving in stand houden en van de interactie tussen de informatiesystemen en de gebruiker noodzakelijk. Wil de accountant zijn positie als deskundige op het terrein van de administratieve processen handhaven, dan zal hij/zij dit terrein zich eigen moeten maken.
Op niet al te lange termijn zal de accountant ten aanzien van de verwerking van routinetransacties in belangrijke mate zijn conclusie omtrent de betrouwbaarheid van de uit deze processen afkomstige gegevens baseren op zijn oordeel over de wijze waarop de organisatie deze processen onder controle heeft, zo is mijn stellige overtuiging. Bij grote organisaties en ook bij door de bedrijfsleiding als complex ervaren geautomatiseerde processen zal de klant de inzet van specialisten (EDP-auditors) begrijpen. Bij middelgrote cliënten en in minder complexe situaties is het budgettechnisch niet verantwoord het controleteam structureel uit te breiden met een EDP-auditor, en ook zal de klant niet begrijpen waarom de accountant direct met een specialist komt voor situaties die door de organisatie als gewoon worden ervaren.

Door de voortschrijdende integratie en toenemende massaliteit zal de accountant in steeds meer situaties niet langer om een systeemgerichte aanpak heen kunnen. Argumenten zijn:
- de fysieke brondocumenten bestaan niet meer of zijn moeilijk toegankelijk;
- de klant verwacht een systeemgerichte aanpak omdat hij een groot vertrouwen in het systeem stelt.

Afkeer door onbekendheid mag voor de accountant geen argument zijn om na een herinrichting van een bedrijfsproces, waarbij informatietechnologie een integraal onderdeel uitmaakt van het administratieve proces, aan deze verandering voorbij te gaan. Wellicht lukt het vaktechnisch met wat kunst en vliegwerk om de controle gegevensgericht uit te voeren. Het zal echter niet lang duren of de cliënt zal de vraag stellen waarom de accountant het allemaal zo omslachtig controleert. De integratie van informatietechnologie in de administratieve organisatie leidt er vanuit het gezichtspunt van het management toe dat de kwaliteit van het administratieve proces op een hoger niveau is komen te liggen. Het management verwacht dat de accountant in deze ontwikkeling mee gaat of er ten minste, als deskundige op het terrein van interne controle, zijn reactie op geeft.

Vereiste kennis accountant

Om in staat te zijn de routinematige basisprocessen systeemgericht te controleren zal de accountant

kennis moeten hebben van de applicatie, toegangsautorisaties en de betrouwbaarheidsmaatregelen binnen de automatiseringsafdeling.

Kennis nemen van de applicatie komt erop neer dat de accountant zijn inventarisatie en beoordeling van de administratieve organisatie niet kan beperken tot de gebruikersprocedures. Een belangrijk deel van de beheersingsmaatregelen is immers opgenomen in de geautomatiseerde gegevensverwerking. Dit lijkt in het begin complex, maar in de praktijk zien we dat verschillende bedrijven in de kern van de gegevensverwerking niet veel van elkaar verschillen. Ook door het gebruik van standaardpakketten treedt een zekere standaardisatie op. De accountant van vandaag zal kennis moeten hebben van de veelgebruikte pakketten. Deze kennis is nodig voor de controle alsmede voor de invulling van zijn adviesfunctie naar de klant toe.

Geautomatiseerde toegangsautorisatieprocedures geven een goed beeld van de wijze waarop de klant omgaat met bevoegdheden. Veel accountants lopen hier met een grote boog omheen omdat zij bang zijn tegen onoplosbare vragen op te lopen. De toegangsbeveiligingssoftware wordt echter met de dag gebruikersvriendelijker. Als de klant in staat is hier zonder bijzondere automatiseringskennis mee om te gaan, moet dit ook tot de bagage van de accountant horen. In de situaties die thans als gemeengoed beschouwd worden (NOVELL, OS 400, populaire standaardsoftware), moet de accountant samen met de systeembeheerder in staat zijn vast te stellen wie tot wat bevoegd is en op welke wijze door de cliënt de toegangsbevoegdheden worden onderhouden.

De mate waarin sprake is van een systematisch werkend systeem wordt voor een belangrijk deel bepaald door de opzet van de procedures met betrekking tot de IT-hulpmiddelen. Belangrijk zijn hierbij de procedures voor het in produktie nemen van nieuwe programma's en het ingrijpen in de produktie ter oplossing van acute produktieproblemen. Ook hier geldt weer dat in de gemiddelde situatie waarin een dergelijke procedure ook bij de cliënt niet ingevuld is door specialisten, dit door de accountant kan worden beoordeeld. Het inroepen van specialisten is noodzakelijk in geval van een complexiteit die ook door de cliënt slechts door (eigen) specialisten kan worden beheerst.
Door steeds verdergaande automatisering van de automatisering is de tendens aanwezig dat het beheer van de computersystemen in een gemiddelde situatie na installatie geen bijzondere specialistische kennis meer vereist.
In een middelgrote tot kleine omgeving waarin informatietechnologie geen strategisch element is, komen de specialisten eraan te pas wanneer ingrijpende veranderingen plaatsvinden. De ervaring leert, dat ingrijpende wijzigingen zich bij bedrijven in de MKB-sector tot eens in de paar jaar beperken. Dit kan het moment zijn dat de accountant tijdelijk ondersteuning vraagt van een EDP-auditor; waarna hij na stabilisatie van de nieuwe situatie weer zelfstandig de noodzakelijke systeemgerichte controlewerkzaamheden moet kunnen uitvoeren. Indien dit niet mogelijk is, ligt het probleem in de eerste plaats bij het management. Het betekent namelijk dat ook dit niet in staat is zelfstandig het proces te beheersen, waarmee de accountant direct een aardig onderwerp heeft voor de invulling van zijn 'natuurlijke' 'ongevraagde' adviesfunctie.

SAMENVATTING EN CONCLUSIE

Informatiesystemen verzorgen thans vele onderdelen van het administratieve verwerkingsproces. Voor de registratieve en administratieve routineprocessen beperkt de menselijke betrokkenheid zich tot het autoriseren van de transacties en het toezien op de juiste en volledige verwerking. De accuratesse van routineprocessen wordt bepaald door de kwaliteit van de informatietechnologie en in mindere mate door menselijk handelen. Dit betekent een verandering in de vorm van maatregelen van interne controle.

Klassieke maatregelen als de controletechnische functiescheiding worden verdrongen door geprogrammeerde procedures (application controls), gerichte controleprocedures door de verantwoordelijke functionarissen (user controls) en een systematisch werkende verwerkingsomgeving (general IT controls). Door de verschuiving van de verwerkingstaken van functionarissen naar door informatietechnologie beheerste processen ontstaan nieuwe risico's die het hoofd moeten worden geboden. Hierbij mag echter niet uit het oog worden verloren dat foutrisico's die bestonden in een klassieke organisatie, voor een belangrijk deel weggenomen zijn door het gebruik van informatietechnologie. De informaticus en de organisatie-adviseur zijn in mindere mate historisch belast met het interne-controlemiddel functiescheiding en hebben dikwijls op creatieve wijze maatregelen getroffen om de kwaliteit van de informatieverwerking te bewaken. Hun eerste belang is een efficiënt en een betrouwbaar proces; de controleerbaarheid komt hierbij over het algemeen op het tweede plan.

Wil de accountant in staat blijven de betrouwbaarheidswaarborgen van geïntegreerde informatiesystemen te doorgronden, dan zal hij er oog voor moeten hebben dat de processen in een geautomatiseerde omgeving op een andere wijze door het management worden beheerst. De controlerend accountant zal, ook al is hij alleen betrokken bij de controle van bedrijven in de MKB-sector, kennis en ervaring moeten hebben van de administratieve logistiek van de verwerking van routinetransacties. De beoordeling van de combinatie van applicatie-, gebruikers- en algemene IT-controles is een voor de hand liggend controlemiddel in een omgeving waarin het management ernaar streeft de verwerking van deze dikwijls massale transactiestromen door middel van het gebruik van informatietechnologie vlekkeloos te laten verlopen. Alle opmerkingen die de accountant maakt over de kwaliteit van de administratie en de opgeleverde cijfers moeten aansluiten bij de benaderingswijze van het management. Is dit niet het geval, dan zal het management dat gewend is te vertrouwen op het proces, zijn opmerkingen als niet (kosten)efficiënt naast zich neerleggen.

J.C. Boer RE RA
Is lid van de maatschap KPMG Klynveld EDP Auditors. Hij is verantwoordelijk voor een regionaal opererend EDP-auditing-team. Op grond van zijn in 1978 gestarte EDP-auditing-loopbaan bezit hij een lange en ruime ervaring op alle terreinen van de EDP-auditing.

Audit van een logistiek systeem

Drs. J.A.C. van Geel, ing. A.P.J. Mouwen en
drs. E.P.R. van Vroenhoven RE RA

Wordt mijn logistieke besturing optimaal ondersteund door automatisering?
Indien dit niet het geval is, ligt dat dan aan de wijze waarop een softwarepakket wordt gebruikt of aan de (on)mogelijkheden van dit pakket?
Moet als gevolg van een verandering in de logistieke besturing het logistieke softwarepakket anders worden ingericht of moet zelfs een ander pakket worden aangeschaft?
Dit zijn voorbeelden van vragen die via een gestructureerde auditaanpak kunnen worden beantwoord.

INLEIDING

In de wereld van de industriële bedrijven is sprake van ontwikkelingen zoals internationalisering, sterke produktdifferentiatie en focus op core processen.

Industriële bedrijven opereren steeds meer internationaal en kunnen bovendien concurrentie uit vrijwel alle delen van de wereld verwachten. De produktlevenscyclus wordt over het algemeen korter en de variatie in produkten groter. Nam een bedrijf voorheen vrijwel het volledige industriële proces voor zijn rekening om tot een produkt te komen, op dit moment wordt veelvuldig gebruik gemaakt van toeleveranciers, die gespecialiseerd zijn in wat door het bedrijf als 'non-core processen' worden beschouwd.

De bekende kritieke succesfactoren prijs en kwaliteit, maar ook levertijd, leverbetrouwbaarheid en flexibiliteit, worden als gevolg van bovenstaande ontwikkelingen steeds 'kritieker'.
Verbetering van de kritieke succesfactoren wordt bereikt door een optimale besturing van het bedrijf. In veel situaties is sprake van een complexe besturing, waarbij besturingsbeslissingen zijn gebaseerd op een enorme hoeveelheid informatie. In een dergelijke situatie is de verwerkingskracht van automatisering onmisbaar geworden. De juiste keuze en het juiste gebruik van logistieke software zijn zelfs uitgegroeid tot een kritieke succesfactor in industriële bedrijven. Een logistieke systeem-audit kan ondersteunen bij de oordeelsvorming over de mate waarin een logistiek systeem deze kritieke succesfactor vervult.

REDENEN VOOR EEN LOGISTIEKE AUDIT

Logistieke software voorziet in de behoefte aan geautomatiseerde hulpmiddelen voor produktieplanning en -besturing, maar ook voor processen als inkoop, voorraadbeheer, verkoop, engineering/werkvoorbereiding, onderhoud, produktontwikkeling en dergelijke.
Logistieke besturing en daarmee de benodigde logistieke software is bedrijfsspecifiek. De variëteit in logistieke software is groot[1] en de complexiteit van implementatie en gebruik is hoog.
Om te kunnen voldoen aan de bedrijfsspecifieke besturingseisen, maken pakketten veelvuldig gebruik van parameters om het pakket in te stellen (het pakket SAP is waarschijnlijk 'kampioen parameters' met meer dan 1400 tabellen met pakketinstellingen). De noodzaak tot en het belang van het juist instellen van het pakket, te zamen met de enorme functionaliteit van logistieke software, maken de implementatie tot een complex en moeilijk beheersbaar project.
In de praktijk blijkt vaak dat ook als het juiste pakket al is gekozen, de implementatie en daarmee het gebruik van het pakket te wensen overlaten. Vandaar dat een audit is ontwikkeld waarmee de geschiktheid van een logistiek pakket voor de organisatie alsmede de effectiviteit van het gebruik kan worden vastgesteld. Met de audit wordt antwoord gegeven op managementvragen zoals:
- 'Wordt onze logistieke besturing optimaal ondersteund door automatisering?'
- 'Indien dit niet het geval is, ligt dat dan aan de wijze waarop ons pakket wordt gebruikt of aan de (on)mogelijkheden van ons pakket?'
- 'Wij hebben onze logistieke besturing veranderd. Moeten wij ons pakket anders inrichten of zelfs tot aanschaf van een ander pakket overgaan?'

De audit van een logistiek systeem, LOSA (Logistieke Systeem Audit) genaamd, is een quick scanmethode. Dit houdt in dat in korte tijd (gemiddelde doorlooptijd twee à drie weken) een antwoord op bovenstaande vragen wordt gegeven.
De logistieke audit bestaat uit de volgende fasen:

1. *Vooronderzoek*
- Understanding the business
- Vaststellen besturingsconcept
- Globale beoordeling besturingsconcept

2. *Definitie systeemeisen*
- Definitie eisen aan logistiek systeem
- Definitie wijze waarop het systeem zou moeten worden gebruikt

3. *Inventarisatie*
- Inventarisatie systeemmogelijkheden
- Inventarisatie wijze van gebruik

4. *Analyse en rapportage*
- Analyse systeemeisen versus systeemmogelijkheden
- Analyse wijze van gebruik
- Rapportage

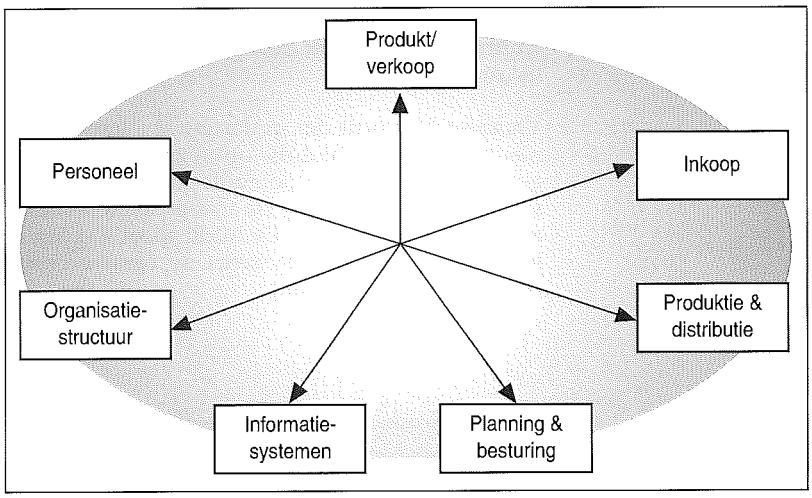
Gegeven de bovenstaande fasering zal in het vervolg van dit artikel per fase een beschrijving worden gegeven van de inhoud en de bijbehorende hulpmiddelen van de logistieke audit.

FASE 1 VOORONDERZOEK

De logistiek in een industrieel bedrijf dient integraal te worden benaderd. Problemen worden namelijk niet door één onderdeel uit de logistiek veroorzaakt en succes zal ook niet worden bereikt door enkel aandacht te schenken aan één bepaald onderdeel.

In een situatie waarin bijvoorbeeld sprake is van een groot produktassortiment, weinig standaardisatie, vele kleine, vaak spoedorders met veel orderwijzigingen en -annuleringen, kan alle aandacht op de besturing en de bijbehorende (automatiserings)hulpmiddelen worden gericht. Een betere oplossing is echter een combinatie van aandacht voor besturing én aandacht voor verlaging van de besturingslast (minder breed assortiment, standaardisatie van verpakkingen, klanten laten betalen voor spoedorders, etc.).

Om het te onderzoeken bedrijf op dergelijke zaken attent te maken wordt in het vooronderzoek, naast de voor de logistieke systeem-audit primaire aandachtsgebieden 'Planning en besturing' en 'Informatiesystemen', aandacht besteed aan alle overige aandachtsgebieden van integrale logistiek (zie figuur 1).



Figuur 1. Aandachtsgebieden integrale logistiek.

Per onderdeel wordt door middel van vragen in een pre-auditlijst (zie voorbeeld in figuur 2) getracht een indruk te krijgen van het verbeteringspotentieel. Natuurlijk geeft beantwoording van de pre-auditvragen en het in korte tijd bespreken van deze antwoorden met de logistieke medewerkers van het bedrijf, geen absolute zekerheid over de

1 *Zo worden in het rapport van Berenschot [BERE92] over het onderzoek naar logistieke software, 61 (!) MRP-systemen en 20 elektronische planbordsystemen aan de orde gesteld.*

Logistieke prestaties	
• Leverbetrouwbaarheid (per klantgroep, produktgroep)	%
• Gemiddelde doorlooptijd, variantie doorlooptijd	# dagen
• Gemiddelde verhouding bewerkingstijd/wachttijd	x/x
• Etc.	
Produkt/verkoop	
• Aantal eindprodukten (voor verpakking, na verpakking)	#
• Klantspecifieke aanpassingen? (% van alle orders)	%
• Vaak wijziging produktspecificaties na orderacceptatie?	Ja/Nee
• % orders met seriegrootte < gemiddelde seriegrootte	%
• % orders met orderwijzigingen na orderacceptatie	%
• Gemiddelde orderomvang, % orders < gemiddelde orderomvang	#, %
• Etc.	

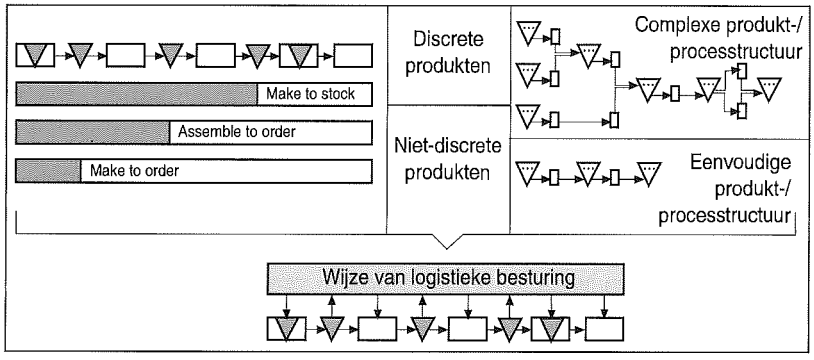
Figuur 2. Voorbeeld pre-auditlijst I.

juistheid en volledigheid van de verbeteringsvoorstellen.
De verbeteringsvoorstellen moeten worden gezien als attentiepunten voor het management. De attentiepunten worden zonder verder onderzoek opgenomen in de rapportage.

Een ander belangrijk onderdeel van het vooronderzoek is het kennis nemen van de wijze waarop het bedrijf zijn logistieke planning en besturing heeft ingericht en tevens het nagaan of zwaar wegende bezwaren tegen de wijze van besturing bestaan.
Indien sprake is van een besturingsfilosofie die absoluut niet past bij het logistieke proces van het bedrijf (bijvoorbeeld materiaalgeoriënteerde planning bij een volledig capaciteitgericht bedrijf), heeft gedetailleerd onderzoek naar de wijze waarop het logistieke pakket aansluit op deze besturingsfilosofie, geen zin. De resultaten alsmede aanbevelingen voor verandering van de logistieke besturing worden in dat geval teruggekoppeld naar het management.

Voorgesteld wordt om in dat geval allereerst een nieuwe besturingsfilosofie op te zetten en vervolgens op basis hiervan de audit van het logistieke systeem voort te zetten. De vraagstelling voor de audit verandert hierbij. De audit moet nagaan of het huidige logistieke systeem de nieuwe besturingsfilosofie ondersteunt.

Figuur 3. Bepalen van de besturingsfilosofie.



Om inzicht te krijgen in de wijze van besturing en tevens een globale beoordeling van de besturingsfilosofie uit te voeren, zijn wederom pre-auditvragen geformuleerd. Uitgangspunt hierbij is dat het klantenorder-ontkoppelpunt en de produkt-/proceskenmerken de besturingsfilosofie bepalen (zie figuur 3).

Een high tech printplaatfabriek wordt bijvoorbeeld vaak gekenmerkt door een volledig 'make to order' klantenorder-ontkoppelpunt. De klant bestelt printplaten in klantspecifieke maten en vormen en bepaalt het aantal lagen, de spoorbreedte, het patroon en dergelijke. Het produkt, de printplaat, is een discreet produkt bestaande uit een beperkt aantal materialen. Het proces is bijzonder complex. De fabriek kenmerkt zich door een job shop-produktie, met vele en vaak iteratieve bewerkingen. Bewerkingstijden zijn volledig produkt- en dus orderspecifiek.

Op basis van het klantenorder-ontkoppelpunt en de produkt-/proceskenmerken zal de besturingsfilosofie voor de printplaatfabriek gekenmerkt worden door onder meer een capaciteitgerichte planning, sterke aandacht voor werkvoorbereiding en fijnplanning op de werkvloer.

Een voorbeeld van vragen uit de pre-auditlijst bevindt zich in figuur 4.

Als derde onderdeel van het vooronderzoek wordt ingegaan op proceskenmerken die bepalen in welke mate de functionaliteiten van een logistiek systeem van toepassing zijn. De antwoorden op de hiervoor geformuleerde pre-auditvragen (zie voorbeeld in figuur 5) zijn van belang voor de definitie van de systeemeisen in de volgende fase van het onderzoek.

De antwoorden op de pre-auditvragen uit de lijsten I, II en III worden besproken met de logistieke medewerkers van het te onderzoeken bedrijf. De gesprekspartners worden afhankelijk van de situatie gekozen. Denk hierbij aan de algemeen directeur en managers van de afdelingen produktie, logistiek/bedrijfsbureau, inkoop, verkoop, engineering/werkvoorbereiding, administratie en onderhoud.

De antwoorden op de pre-auditvragen, te zamen met een algemene bedrijfs- en produktbeschrijving en indrukken die opgedaan zijn tijdens een bedrijfsrondleiding, leiden in de volgende fase tot systeemeisen aan het logistieke systeem.

FASE 2
DEFINITIE SYSTEEMEISEN

Fase 2 van LOSA is erop gericht een raamwerk van systeemeisen op te zetten, waarmee in fase 3 een beoordeling kan worden uitgevoerd van de geschiktheid van het logistieke systeem alsmede van het gebruik van het systeem in de organisatie.
Het opzetten van het raamwerk van systeemeisen

wordt ondersteund met referentiemodellen, opgenomen in een geautomatiseerd hulpmiddel, genaamd PaperClip.
Om via de referentiemodellen tot de juiste systeemeisen te komen, is een drietal sleutels gedefinieerd (zie figuur 6), te weten:
- logistieke besturingsfilosofie;
- klantenorder-ontkoppelpunt;
- produkt-/proceskenmerken.

De logistieke besturingsfilosofie (MRP II, JIT, OPT, en dergelijke) bepaalt het basisreferentiemodel. Het basisreferentiemodel is onderverdeeld in eisen met betrekking tot:
- *basisgegevens:* stuklijst, routing, artikelen, klanten, leveranciers, etc.;
- *systeemfuncties:* demand planning, produktieplanning, shop floor control, engineering, inkoop, verkoop, voorraadbeheer, etc.;
- *algemene eisen:* interne controle/beveiliging, onderhoudbaarheid, etc.

De systeemfuncties en de invulling van de eisen per onderdeel verschillen per besturingsfilosofie. Zo zijn de eisen voor capaciteitsplanning bij OPT (knelpuntgerichte besturingsfilosofie) veel uitgebreider dan bij MRP II.
Vervolgens wordt het basisreferentiemodel uitgebreid met eisen uit referentiemodellen per klantenorder-ontkoppelpunt en eisen uit hoofde van bepaalde produkt-/proceskenmerken (zie figuur 7).

In het geval van het klantenorder-ontkoppelpunt 'assemble to stock' (dat is halffabrikaten op voorraad produceren en eindbewerking/verpakking klantspecifiek uitvoeren) worden bijvoorbeeld eisen voor een final assembly schedule (dat is separate planning voor de klantspecifieke eindbewerking/verpakking van halffabrikaten) toegevoegd. Mogelijkheden tot uitbesteding (proceskenmerk) leiden bijvoorbeeld eveneens tot extra eisen.
De inhoud van de drie sleutels - besturingsfilosofie, klantenorder-ontkoppelpunt en produkt-/proceskenmerken - wordt bepaald op basis van de antwoorden op de pre-auditvragen in het vooronderzoek.

In de referentiemodellen in PaperClip is per eis een gewicht meegegeven. Dit gewicht geeft het belang van de betreffende eis weer. Het wordt gebruikt om op basis van in fase 3 toe te kennen scores aan eisen, een totaalscore per systeemfunctie en uiteindelijk voor het totale logistieke systeem uit te rekenen. De gewichten verschillen wederom per besturingsfilosofie, klantenorder-ontkoppelpunt en produkt-/proceskenmerken.

Het via de sleutels opgebouwde raamwerk van eisen wordt met de opdrachtgever besproken. Indien van toepassing kunnen bedrijfsspecifieke eisen worden toegevoegd dan wel niet-relevante eisen vervallen.

Een ander belangrijk aspect dat met de opdrachtgever wordt besproken, is de zogenaamde *opportunity coverage*. Indien sprake is van volledige afdekking van de systeemeisen door het logistieke systeem wordt de zogenaamde maximum coverage (100%) bereikt. Op basis van kenmerken of keuzes

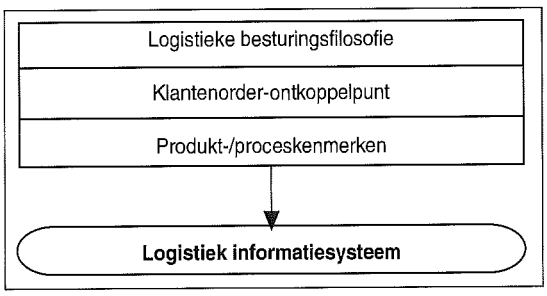
Klantenorder-ontkoppelpunt	
• Zijn produkten klantspecifiek? (verpakking/produkt zelf)	Ja/Nee
• Is sprake van voorraad halffabrikaat/eindprodukt? (omvang?)	HF __ EP __
• Etc.	
Produkt-/proceskenmerken	
• Aantal elementen/niveaus in stuklijst?	#/#
• Produkten niet discreet/discreet (vanaf welk moment)?	ND/D __
• Aantal bewerkingen tot eindprodukt (per produktgroep)?	#
• Iteratieve bewerkingen? Parallelle bewerkingen?	Ja/Nee
• Etc.	
Besturingsfilosofie	
• Besturingsfilosofie (MRP I, MRP II, OPT, JIT, etc.)	MRP I/II/OPT/JIT
• Produktie volgens pull- of push-principe?	Pull/Push __
• Planninghorizon Hoofd Produktie Plan, Fijnplanning	HPP __ /FP __
• Voorraadbehoeftebepaling via MRP I, SIC, EOQ, minimumvoorraad	MRPI/SIC/EOQ/MV
• Etc.	

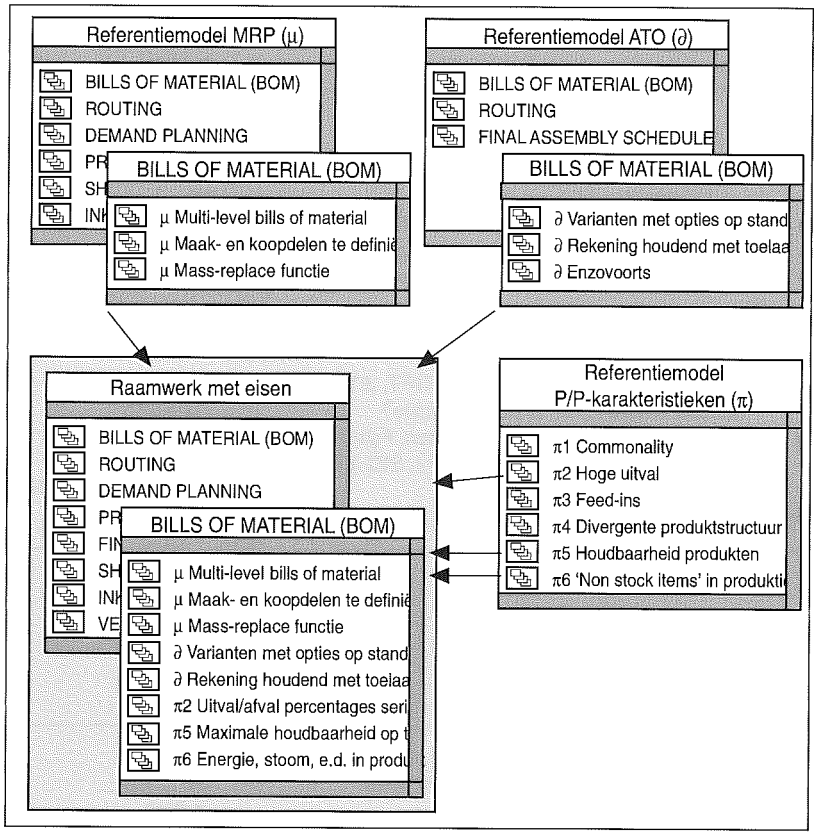
Figuur 4. Voorbeeld pre-auditlijst II.

Voorraad	
• Partijregistratie (grondstoffen/eindprodukt)?	GS__ /EP__
• Gevaarlijke goederen?	Ja/Nee
• Aantal magazijnen, vrije/vaste locaties?	# - Vast/Vrij
• Etc.	
Inkoop	
• Aantal leveranciers, orders, gemiddeld aantal orderregels?	#/#/#
• Raamcontracten (prijs/hoeveelheid/kwaliteit)?	PR/HOEV/KW
• Buitenlandse leveranciers, facturering in vreemde valuta	Ja/Nee
• Etc.	
Produktie	
• Uitbesteding mogelijk?	Ja/Nee
• Knelpunten (mens/machine)?	Mens/Machine
• Materiaal feed ins bij bewerkingen?	Ja/Nee
• Nevenprodukten?	Ja/Nee
• Gereedschappen?	Ja/Nee
• Etc.	

Figuur 5. Voorbeeld pre-auditlijst III.

Figuur 6. Factoren bepalend voor de definitie van systeemeisen.





Figuur 7. Referentiemodellen.

van de organisatie kan in onderling overleg tussen de EDP-auditor en de opdrachtgever worden besloten niet te streven naar maximum coverage, maar naar een lagere afdekking van de systeemeisen, de opportunity coverage. Aanleiding kan bijvoorbeeld onvoldoende kennis en ervaring voor automatisering van een bepaalde functie (bijvoorbeeld afdelingsplanning) zijn. De opportunity coverage wordt per hoofdonderwerp in het raamwerk van eisen vastgesteld.

FASE 3
INVENTARISATIE

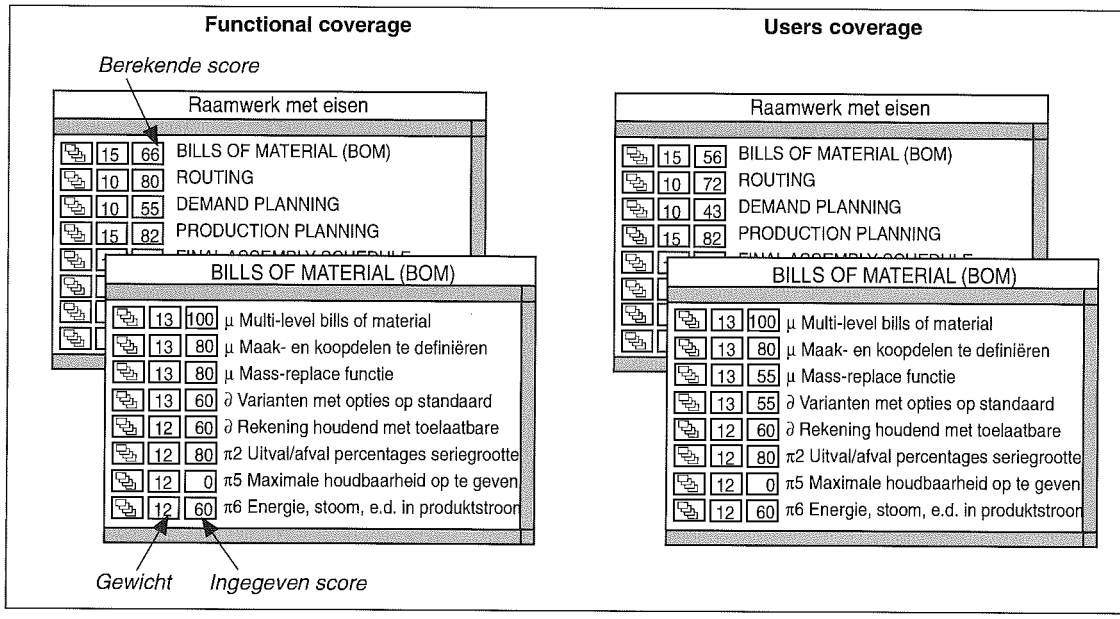
Aan de hand van gesprekken met logistieke medewerkers, beperkte bestudering van de systeemdocumentatie en een korte demonstratie van het systeem, wordt in fase 3 geïnventariseerd of:

- het logistieke systeem functioneel voldoet aan het raamwerk van eisen opgesteld in fase 2 (functional coverage);

- de in het logistieke systeem aanwezige functionaliteiten door de organisatie op de juiste wijze worden gebruikt (users coverage).

Met behulp van PaperClip worden per eis in het in fase 2 opgestelde raamwerk van eisen, scores (0-100) voor functional en users coverage ingegeven (zie figuur 8).
Op basis van de gewichten en scores berekent PaperClip de functional en users coverage op het niveau van systeemfunctie en uiteindelijk van het totale logistieke systeem (zie figuur 9).

Figuur 8. Inventarisatie systeemeisen.



FASE 4
ANALYSE EN RAPPORTAGE

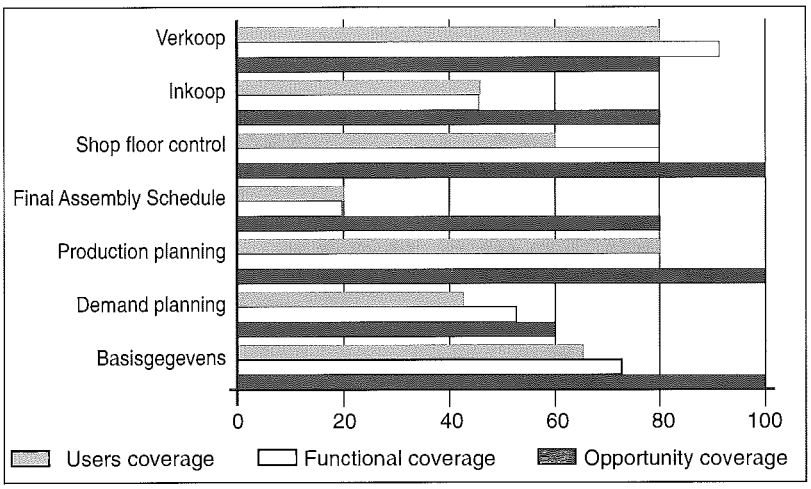
In fase 4 worden de resultaten van de inventarisatie in fase 3 geanalyseerd en wordt een rapport aan de opdrachtgever uitgebracht. Uitgangspunt is de beantwoording van de door het management gestelde vragen, zoals:
'Wordt onze logistieke besturing optimaal ondersteund door automatisering?'
'Indien dit niet het geval is, ligt dat dan aan de wijze waarop ons pakket wordt gebruikt of aan de (on)mogelijkheden van ons pakket?'

Indien het logistieke systeem gebaseerd is op een andere besturingsfilosofie dan die van het bedrijf, de functional coverage bijzonder laag is en de opportunity coverage voldoende mogelijkheden biedt, zal aanschaf van een nieuw logistiek systeem worden aanbevolen. Bij het selectietraject voor een nieuw logistiek systeem kan gebruik worden gemaakt van het in fase 2 opgestelde raamwerk van eisen.

Als sprake is van een redelijk goed logistiek systeem met een beperkte functional coverage op bepaalde, voor het bedrijf belangrijke gebieden, zal maatwerk worden aanbevolen. Aandachtspunt hierbij is de blijvende onderhoudbaarheid van het logistieke systeem.

Indien de in het logistieke systeem opgenomen functionaliteiten in onvoldoende mate of verkeerd worden gebruikt (lage users coverage), worden aanbevelingen omtrent het juiste gebruik gegeven. Hernieuwde implementatie van bepaalde functionaliteiten, bijscholing en aanpassing van gebruikershandleiding en procedures zijn in een dergelijk geval noodzakelijk.

Naast functionele aspecten wordt ook rekening gehouden met andere kwaliteitsaspecten, zoals onderhoudbaarheid en interne controle/beveiliging. Potentiële problemen ten aanzien van bijvoorbeeld onderhoudbaarheid (de leverancier ondersteunt bijvoorbeeld het pakket niet meer) spelen een belangrijke rol bij de richting van de adviezen (maatwerk/ander pakket).
De rapportage bevat daarnaast, zoals aangegeven bij het vooronderzoek, verbeteringsmogelijkheden voor andere aandachtsgebieden van integrale logistiek dan 'Planning en besturing' en 'Informatiesystemen'.



Figuur 9. Resultaten fase 3 afgezet tegen de opportunity coverage.

CONCLUSIE

Gezien het toenemende belang van logistieke pakketten voor een goede besturing van industriële ondernemingen, is het belangrijk om regelmatig de effectiviteit van het logistieke pakket te toetsen. Door veranderingen in de besturing van de organisatie is het mogelijk dat het pakket niet meer aansluit bij de organisatie. Daarnaast blijkt in de praktijk dat in veel gevallen de mogelijkheden van de logistieke pakketten niet maximaal worden benut. Met behulp van de in dit artikel beschreven methode LOSA wordt onderzocht of het logistieke pakket past bij de wijze van logistieke besturing en of de organisatie in voldoende mate gebruik maakt van de mogelijkheden van het pakket. De benadering van integrale logistiek staat daarbij centraal. Door gebruik van hulpmiddelen als pre-auditlijsten en referentiemodellen wordt de doorlooptijd van de audit aanzienlijk verkort.

LITERATUUR

[BERE92] *Software pakketten voor produktiebesturing*, Logiplan Berenschot, 1992.

Drs. J.A.C. van Geel
Is in 1991 in dienst getreden bij KPMG Klynveld EDP Auditors. Naast de studie Bestuurlijke Informatiekunde heeft hij de post-doctorale opleiding EDP-auditing voltooid, beide aan de Katholieke Universiteit Brabant. Hij heeft als belangrijk werkterrein het beoordelen, selecteren en implementeren van applicaties. Hij heeft zich onder meer gespecialiseerd in de beoordeling en selectie van logistieke pakketten.

Ing. A.P.J. Mouwen
Is in 1991 na afronding van de studie informatica aan de Hogeschool Eindhoven de studie Bestuurlijke Informatiekunde aan de Katholieke Universiteit Brabant gaan volgen. Ter afsluiting van deze studie heeft hij in 1994 een stageopdracht bij KPMG Klynveld EDP Auditors te Eindhoven uitgevoerd. De opdracht bestond uit het ontwikkelen van tools ter ondersteuning van een onderzoek naar de effectiviteit van logistieke informatiesystemen.

Drs. E.P.R. van Vroenhoeven RE RA
Is sinds 1989 werkzaam bij KPMG Klynveld EDP Auditors. Naast de studie Bestuurlijke Informatiekunde heeft hij de post-doctorale studie Accountancy voltooid, beide aan de Katholieke Universiteit Brabant. Zijn auditervaring ligt met name bij pakketselecties, implementaties van software en beoordelingen op het gebied van logistiek.

Informatiebeveiliging van theorie naar praktijk

Drs. P. Veltman RE RA

De evolutie van theorie- en modelvorming tot standaarden, die zich op het gebied van de informatiebeveiliging heeft voltrokken, is van belang voor het evalueren en certificeren van beveiligingsprodukten. Pragmatische invalshoeken (baseline-benadering) resulteren ook in de totstandkoming van, wellicht minder strikte, standaarden. Het verschil tussen de theorie- en baseline-benadering vergt een verschil in attitude van de EDP-auditor.

INLEIDING

Halverwege de jaren zeventig, in de periode dat in Nederland de eerste aanzet werd gegeven tot het afbakenen en definiëren van het vakgebied EDP-auditing, werd in de Verenigde Staten de basis gelegd voor een wetenschappelijke benadering van informatiebeveiliging.
Hoewel afkomstig uit twee geheel verschillende werelden - accountancy respectievelijk 'the military' - zijn EDP-auditing en informatiebeveiliging onlosmakelijk met elkaar verbonden. Het zijn immers vooral de beveiligingsmaatregelen die moeten waarborgen dat de informatievoorziening aan bepaalde kwaliteitseisen voldoet, hetgeen het object van onderzoek is van de EDP-auditor.

Het onderwerp van dit artikel is informatiebeveiliging, de evolutie van theorie- en modelvorming tot standaarden die kunnen worden toegepast voor het evalueren en certificeren van beveiligingsprodukten. Tevens wordt ingegaan op alternatieve, meer pragmatische benaderingen, gebaseerd op 'baselines'.

Het belang van beveiligingsstandaarden voor de EDP-auditor is evident; concrete normen, wettelijk of door de organisatie bepaald, waaraan de informatiebeveiliging in een specifieke situatie kan worden getoetst, zijn veelal niet voorhanden. Door aansluiting te zoeken bij theoretisch onderbouwde, internationaal aanvaarde en de facto-standaarden kan de subjectiviteit in het oordeel van de EDP-auditor worden teruggebracht.

Van nog groter belang zijn de standaarden voor het management dat verantwoordelijkheid draagt voor informatiebeveiliging. De materie is complex, de technologische ontwikkelingen gaan snel en een ongeluk zit in een klein hoekje, zodat het moeilijk is de juiste balans te vinden tussen risico's en beveiligingsmaatregelen. Beveiligingsstandaarden kunnen het management bij het zoeken van deze balans ondersteuning bieden doordat zij, met de woorden van het in deze bijdrage te behandelen Orange Book, een maatstaf verschaffen waarmee informatiebeveiliging en het vertrouwen dat hierin kan worden gesteld, kunnen worden gemeten, en waarmee beveiligingsspecificaties kunnen worden opgesteld bij investeringen in informatietechnologie.
In hoeverre de thans ontwikkelde informatiebeveiligingstheorieën, -standaarden en -produkten invulling geven aan dit perspectief wordt in dit artikel geanalyseerd.

THEORIEVORMING

De theoretische benadering van informatiebeveiliging heeft geresulteerd in de ontwikkeling van een aantal min of meer formele modellen. In deze paragraaf worden een geheimhoudingsmodel en een integriteitsmodel behandeld.

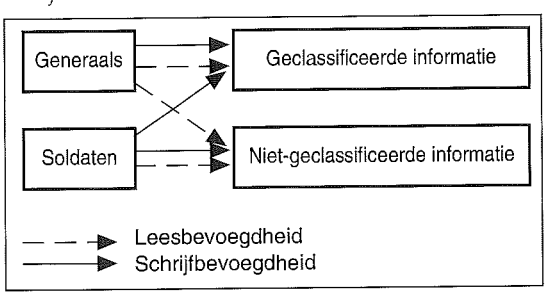
Het Bell/LaPadula-model - focus op geheimhouding

Uitgangspunt voor de modelmatige benadering van informatiebeveiliging is het onderzoekswerk van Bell en LaPadula in de Verenigde Staten eind jaren zestig en begin jaren zeventig, dat resulteerde in het *Bell/LaPadula-model* ([Bell73], [Bell76]).

Het Bell/LaPadula-model (BLM) is gericht op de geheimhouding van geclassificeerde (militaire) informatie. De doelstelling is dat geclassificeerde informatie niet bekend mag raken bij onbevoegden. Op het eerste gezicht kan deze doelstelling op een eenvoudige manier worden bereikt door aan het lezen van geclassificeerde informatie restricties te verbinden. Een dergelijke simpele beveiligingsmaatregel biedt echter geen bescherming tegen het al dan niet opzettelijk 'declassificeren' van informatie door een op zichzelf bevoegde persoon, met als gevolg dat de geclassificeerde informatie toch bekend raakt bij onbevoegden. Om dit te voorkomen moet ook het schrijven van informatie worden beperkt. Aldus is het BLM gebaseerd op twee principes, die kunnen worden samengevat als: 'niet hoger lezen, niet lager schrijven'. Deze principes (in het model 'Simple Security Condition' respectievelijk '*-Property' genoemd) worden aan de hand van een voorbeeld toegelicht.

> In een bepaalde militaire omgeving bestaat het onderscheid tussen generaals en soldaten, waarbij de generaals bevoegd zijn om geclassificeerde informatie te lezen, en soldaten niet. Soldaten zijn wel bevoegd tot het lezen van niet-geclassificeerde informatie, evenals de generaals (zie figuur 1).
>
> Om te voorkomen dat de soldaten kennis nemen van de geclassificeerde informatie geldt het principe van 'niet hoger lezen'. Het principe van 'niet lager schrijven' verhindert dat een generaal geclassificeerde informatie ter kennis brengt van een soldaat.
> In een geautomatiseerde omgeving kan de informatie bestaan uit een computerprogramma, dat bij 'lezing' tot uitvoering wordt gebracht. Een soldaat zou misbruik kunnen maken van zijn schrijfbevoegdheid door aan een aantrekkelijk ogend programma (een computerspelletje, zeg 'War games') verborgen functionaliteit toe te voegen, bijvoorbeeld het lezen en vervolgens wegschrijven van geclassificeerde informatie. Door het principe van 'niet hoger lezen' is de soldaat niet in staat zelf met het programma de geclassificeerde informatie te lezen. Maar als een generaal, onbewust van de verborgen functionaliteit, War games speelt wordt het programma uitgevoerd met zijn bevoegdheden en kan het de geclassificeerde informatie lezen. Het principe van 'niet lager schrijven' verhindert nu dat het programma de geclassificeerde informatie wegschrijft als niet-geclassificeerde informatie, waartoe de soldaat toegang heeft.
> Op deze manier biedt de schrijfrestrictie niet alleen bescherming tegen misbruik van bevoegdheden door een generaal, maar ook tegen een 'Trojan horse'.[1]

Figuur 1. Principes van 'niet hoger lezen, niet lager schrijven'.



Vanzelfsprekend kan dit voorbeeld worden uitgebreid door meerdere bevoegdheidsniveaus ('clearance levels') en meerdere classificatieniveaus te onderscheiden. Ook kunnen verdere restricties in de bevoegdheden worden aangebracht, die bijvoorbeeld verhinderen dat personen met op zichzelf voldoende clearance inzage krijgen in bepaalde informatie. Deze nadere restricties zijn in feite de traditionele beveiligingsmaatregelen, bedoeld om het principe van 'need to know' (of meer algemeen 'least privilege') af te dwingen. In verband met het risico van misbruik van bevoegdheden en van Trojan horses dienen deze least privilege-beveiligingsmaatregelen geen afbreuk te doen aan de principes van het BLM.

Welke bevoegdheden een persoon bij least privilege nodig heeft valt niet op voorhand aan te geven. Dit moet, afhankelijk van de specifieke situatie, worden vastgesteld door of namens de eigenaar van het beveiligde object. Daarom duidt men logische toegangsbeveiliging op basis van least privilege wel aan als 'Discretionary Access Control' (DAC). Toegangsbeveiliging volgens het BLM, waaraan ook eigenaars zich verplicht moeten houden, heet dan 'Mandatory Access Control' (MAC). Dit onderscheid tussen DAC en MAC is overigens minder principieel dan wel wordt voorgesteld. Ook bij MAC moeten door of namens daartoe bevoegde personen, zoals eigenaars, bevoegdheids- en classificatieniveaus worden vastgesteld en geïmplementeerd. In dit opzicht is MAC net zo discretionary als DAC.

Het BLM is in werkelijkheid complexer dan hier wordt gesuggereerd. Het is een wiskundig model, gebaseerd op de verzamelingenleer, waarin bijvoorbeeld het bewijs wordt geleverd van het 'Basic Security Theorem'. Dit theorema houdt in dat een systeem in een beveiligde toestand na het ondergaan van een willekeurige volgorde van operaties

1 *Een Trojan horse kan worden gedefinieerd als een computerprogramma met een schijnbare of werkelijke nuttige functie, dat additionele (verborgen) functies bevat en dat op clandestiene wijze gebruik maakt van de (gelegaliseerde) autorisaties van het initiërende proces (definitie ontleend aan [Berg92]).*

die in het model zijn beschreven, weer in een beveiligde toestand verkeert. Door deze formele benadering is het model echter ook tamelijk ontoegankelijk.
Ondanks de grote invloed die het BLM heeft gehad op beveiligingsstandaardisatie en de ontwikkeling van beveiligde computersystemen, heeft het model een aantal belangrijke beperkingen. Deze beperkingen vloeien voort uit de doelstelling van geheimhouding van (militaire) informatie. Zo komt het principe van 'niet lager schrijven' wat merkwaardig over indien de integriteit van informatie als uitgangspunt wordt genomen.
'Niet lager schrijven', dat wil zeggen 'gelijk of hoger schrijven', houdt immers in dat een persoon met een lage clearance geclassificeerde informatie mag schrijven. Op zich is de ratio van dit principe duidelijk: een soldaat of een ondergeschikte in het algemeen moet een rapport aan zijn of haar meerdere kunnen schrijven. Het houdt echter tevens in dat de ondergeschikte geclassificeerde programma's kan schrijven; het verhoogd risico van niet-integere informatie dat dit tot gevolg heeft, is voor militaire omgevingen van minder belang dan het risico van uitlekken van geclassificeerde informatie. Voor de meeste commerciële omgevingen geldt echter het omgekeerde.

Het Bell/LaPadula-model is een belangrijk theoretisch beveiligingsmodel.

De publikaties van Bell en LaPadula hebben een stimulans betekend voor onderzoekswerk naar beveiligingsmodellen gericht op de integriteit van informatie. Het bekendste voorbeeld daarvan is het *Clark/Wilson-model.*

Het Clark/Wilson-model - focus op integriteit

In 1987 publiceren Clark en Wilson hun 'A Comparison of Commercial and Military Computer Security Policies' [Clar87]. In dit artikel gaan zij in op het militaire informatiebeveiligingsbeleid zoals dat is geïncorporeerd in het Orange Book, oorspronkelijk uitgebracht in 1983. Dit Orange Book, dat in de volgende paragraaf wordt behandeld, is gebaseerd op het Bell/LaPadula-model.

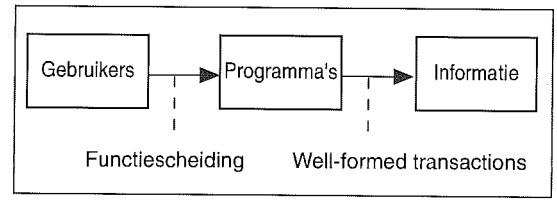
De auteurs beargumenteren dat voor een commercieel informatiebeveiligingsbeleid geheimhouding weliswaar niet onbelangrijk is, maar dat de eerste zorg moet uitgaan naar integriteit. Voor handhaving van de integriteit zijn deels andere modellen en andere beveiligingsmechanismen noodzakelijk. In een militaire omgeving is de doelstelling van informatiebeveiliging dat geclassificeerde informatie niet mag worden gelezen door onbevoegden ('niet hoger lezen') en niet mag worden gedeclassificeerd ('niet lager schrijven'). Voor commerciële omgevingen zou de primaire doelstelling moeten zijn dat geen enkele gebruiker, ook niet een op zichzelf bevoegde gebruiker, al dan niet opzettelijk informatie zodanig kan wijzigen dat bedrijfsmiddelen of verantwoordingsregistraties verloren gaan of gemanipuleerd worden.

Traditioneel, ook in een handmatige omgeving, zijn er twee principes om de doelstelling van commerciële informatiebeveiliging te bereiken. Deze zijn de vormvoorschriften bij het registreren van transacties (met de woorden van Clark en Wilson 'well-formed transactions') en functiescheiding. Vormvoorschriften zijn bijvoorbeeld de regels van het dubbel boekhouden en de eis dat een foutieve transactieregistratie wordt tegengeboekt in plaats van verwijderd. Deze vormvoorschriften zijn vooral gericht op de interne consistentie van de informatie.
Functiescheiding heeft vooral tot doel te waarborgen dat de informatie in overeenstemming is met het afgebeelde deel van de werkelijkheid (externe consistentie). Door activiteiten die een verandering in de werkelijkheid tot gevolg hebben, zoals het uitvoeren van een verkooptransactie, aan verschillende personen toe te wijzen, worden waarborgen verkregen dat de informatie over deze transactie integer is.

Om de twee principes van het Clark/Wilson-model (CWM) te realiseren zijn beveiligingsmechanismen nodig die deels identiek zijn aan de beveiligingsmechanismen om het BLM te ondersteunen. Deze zijn bijvoorbeeld de mechanismen om de identiteit van een gebruiker vast te stellen en te verifiëren, en om de activiteiten van gebruikers vast te leggen. Voor een belangrijk deel zijn deze mechanismen echter verschillend. Het BLM is in essentie binair van opzet en richt zich op de relatie tussen gebruikers en informatie. Het CWM is een ternair model, met als componenten gebruikers, informatie en activiteiten om informatie te bewerken (in een geautomatiseerde omgeving zijn dat de programma's). Het principe van functiescheiding heeft vooral betrekking op de relatie tussen gebruikers en programma's. Het principe van well-formed transactions betreft de relatie tussen programma's en informatie (zie figuur 2).

Clark en Wilson hebben de twee principes verder uitgewerkt in een model bestaande uit een aantal certificatie- en handhavingsregels. De certificatieregels dienen ter vaststelling dat informatieverwerkende programma's voldoen aan de eisen van well-formed transactions, waaronder de eis van

Figuur 2. Principes van het Clark/Wilson-model.



een audit-trail, en dat de relaties tussen gebruikers, programma's en informatie voldoen aan de eisen van functiescheiding. De handhavingsregels moeten onder andere waarborgen dat informatie alleen wordt verwerkt met de gecertificeerde programma's en volgens de gecertificeerde relaties, en dat de gebruikersidentiteit wordt geverifieerd voordat een programma wordt uitgevoerd.
Als kritiek op het CWM is onder meer naar voren gebracht dat het geen of onvoldoende ondersteuning biedt voor rolafhankelijke functiescheiding (Role Based Access Control - RBAC) (zie onder andere [Abra93], [Berg92]). Rolafhankelijke functiescheiding wordt bijvoorbeeld toegepast bij electronic banking-systemen: een gebruiker mag betalingstransacties zowel invoeren als verifiëren, maar hij mag niet de betalingstransacties verifiëren die hij zelf heeft ingevoerd.[2] Belangrijker is echter de kritiek dat het model voorbij gaat aan de inherente complexiteit van de derde component die wordt geïntroduceerd: de programma's. In de praktijk zal het nauwelijks mogelijk zijn het geheel aan (applicatie)programmatuur, waaronder standaardpakketten, parametergestuurde programma's, utilities, opvraagtalen, etc., te certificeren op de wijze als Clark en Wilson voorstaan (zie hiervoor verder [NGI90]).

Over de vraag in hoeverre de certificatie- en handhavingsregels mandatory van aard zijn kan men twisten. Door het instellen van adequate 'general IT controls', waaronder functiescheiding tussen het vaststellen en onderhouden van de regels enerzijds en het gebruiken van het systeem anderzijds, krijgen de regels voor de systeemgebruikers een mandatory werking. De certificatieregels, zoals de geprogrammeerde invoer- en verwerkingscontroles ('application controls') en de vereiste functiescheidingen, zullen echter veelal situatie-afhankelijk zijn, hetgeen de discretion van de eigenaar noodzakelijk maakt.

Bovendien leveren Clark en Wilson geen formeel bewijs dat de certificatie- en handhavingsregels de beoogde informatie-integriteit daadwerkelijk afdwingen. In het model van Bell en LaPadula wordt bijvoorbeeld aangetoond dat het principe van 'niet lager schrijven' voldoende voorwaarde is om te voorkomen dat informatie wordt gecompromitteerd door een Trojan horse-aanval. Doordat er (nog) geen algemeen geldende methoden bekend zijn om de correctheid van programmatuur te bewijzen, zal ook het (formele) bewijs dat de regels van CWM bestand zijn tegen bijvoorbeeld een Trojan horse, nog wel even op zich laten wachten.
Het CWM is een quasi-formeel model, hetgeen overigens de leesbaarheid en toegankelijkheid ten goede komt.

Naast het model van Clark/Wilson zijn in de literatuur alternatieve integriteitsmodellen beschreven. Tot op heden hebben deze modellen echter nog niet geleid tot concrete beveiligingsstandaarden, laat staan tot beveiligingsprodukten. Zolang het aan deze standaarden ontbreekt zullen de computerleveranciers zich richten op de standaarden die wel beschikbaar zijn, en dat zijn standaarden gebaseerd op het geheimhoudingsmodel, waarvan het Orange Book het meest gezaghebbend is.

BEVEILIGINGSSTANDAARDEN

Beveiligingsstandaardisatie is ontstaan vanuit de militaire behoefte aan zekerheid dat de geheimhouding van geclassificeerde informatie is gewaarborgd. Dit heeft geleid tot de ontwikkeling van het befaamde Orange Book, waarvan de effecten moeilijk kunnen worden overschat.

Het 'Orange Book' poogt beveiliging meetbaar te maken op basis van operationele criteria.

De laatste jaren hebben in vervolg op het Orange Book een stortvloed van nieuwe initiatieven te zien gegeven, niet alleen in de Verenigde Staten maar ook in Europa, Canada en Japan. Op enkele van deze ontwikkelingen wordt ingegaan.

De eerste standaard: het Orange Book

Het eerste initiatief om te komen tot praktisch toepasbare en certificeerbare beveiligingsstandaarden is afkomstig van het Amerikaanse Ministerie van Defensie en dateert van 1977. In 1983 resulteerde dit in het uitbrengen van de 'Trusted Computer System Evaluation Criteria' (TCSEC ofwel het Orange Book). De huidige versie verscheen in 1985 [DoD85].
In het Orange Book worden beveiligingsklassen beschreven, en leveranciers van computersystemen kunnen hun produkten aanbieden voor evaluatie en certificatie volgens een bepaalde klasse.
De doelstelling van het Orange Book is om informatiebeveiliging 'meetbaar' te maken aan de hand van operationele criteria. De informatiebeveiliging is gericht op de geheimhouding van informatie en gebaseerd op het model van Bell en LaPadula.

Een centraal element in het Orange Book is de 'Trusted Computing Base' (TCB). De TCB is een variatie op het 'reference monitor'-concept, een mechanisme om autorisatieregels af te dwingen. Aan een dergelijk mechanisme worden de volgende eisen gesteld:
- het moet bestand zijn tegen manipulatie ('knoeibestendig' of 'tamperproof');
- het moet altijd worden aangeroepen (ook wel 'volledige bemiddeling' of 'complete mediation' genoemd);
- het moet klein genoeg zijn om te kunnen worden geanalyseerd en getest, opdat de volledigheid kan worden vastgesteld.

De eerste implementaties van het reference monitor-concept, in de vorm van hardware en software, stonden bekend als 'security kernels'.
Om tegemoet te komen aan de praktijk behoeft de TCB, waarvan de softwarecomponent bestaat uit delen van besturingsprogrammatuur of applicatie-

2 *RBAC wordt ook wel gedefinieerd als de toepassing van functionele gebruikersprofielen, waaraan enerzijds een gebruikersidentiteit is gekoppeld en anderzijds een verzameling bevoegdheidsregels, passend bij een bepaalde functie-omschrijving. Deze opzet vereenvoudigt het onderhoud van bevoegdheidsregels, doordat bij een functieverandering slechts de relatie tussen gebruikersidentiteit en functioneel profiel behoeft te worden gewijzigd, en niet het geheel van bevoegdheidsregels.*

programmatuur, niet noodzakelijkerwijs geheel aan de reference monitor-eisen te voldoen.

In het Orange Book worden drie beveiligingsdoelstellingen onderkend, die worden uitgewerkt in zes meer concrete beveiligingseisen. De evaluatie geschiedt op basis van zevenentwintig evaluatiecriteria, die een nadere uitwerking zijn van de beveiligingseisen en een documentatie-eis.

Op grond van de evaluatiecriteria kunnen computersystemen in drie klassen worden ingedeeld, afgezien van een restklasse voor systemen die niet aan de criteria voldoen om in een hogere klasse te worden ingedeeld. Binnen de drie klassen worden nog enkele subklassen onderkend. De drie klassen zijn:

Discretionary Protection (C)
Aan deze klasse wordt de eis gesteld dat de TCB beveiligingsvoorzieningen bevat in de vorm van bijvoorbeeld 'access control lists' waarmee de toegang van gebruikers tot informatie kan worden afgeschermd. Voorts moet het systeem over een faciliteit beschikken voor het identificeren en authenticeren van gebruikers, en moeten de authenticatiegegevens, zoals passwords, beschermd zijn tegen ongeautoriseerde toegang.

Bij executie in het interne geheugen moet de TCB zelf beschermd zijn tegen manipulatie. Via een test moet aantoonbaar zijn dat er geen voor de hand liggende manieren zijn om de werking van de TCB te omzeilen.

Binnen deze klasse worden twee subklassen onderkend (C1 en C2). Aan C2 worden onder meer de volgende aanvullende eisen gesteld:

- Er moet een mechanisme zijn om het 'propageren' van toegangsrechten aan restricties te kunnen verbinden. Hiermee kan dus de discretion van eigenaars worden beperkt.

- Voordat geheugenmedia aan een subject beschikbaar worden gesteld, moeten eventueel nog bestaande toegangsrechten worden ingetrokken en moet eventueel nog aanwezige informatie worden verwijderd.

- De TCB moet een audit-trail kunnen bijhouden van gebruikersactiviteiten.

Figuur 3. Beveiliging op basis van hiërarchische classificaties en niet-hiërarchische categorieën.

Object / Subject	Kantoorinformatie (2, KMF)	Magazijninformatie (1,M)	Fabrieksinformatie (3,F)
Algemeen directeur (3, KMF)	L[1]	L[2]	L[3]
Kantoormedewerker (2, KMF)	L, S	L[2]	–[4]
Magazijnmedewerker (1,M)	S[5]	L, S	–[6]
Fabrieksmedewerker (3,F)	–[7]	–[8]	L, S

Toelichting:
L = Leesbevoegdheid
S = Schrijfbevoegdheid
De karakters tussen haakjes geven de labels weer, waarbij de cijfers de hiërarchische classificaties voorstellen en de letters de niet-hiërarchische categorieën.
1. De hiërarchische classificatie verhindert schrijfbevoegdheid.
2. De hiërarchische classificatie en de niet-hiërarchische categorieën verhinderen schrijfbevoegdheid.
3. De niet-hiërarchische categorieën verhinderen schrijfbevoegdheid.
4. De hiërarchische classificatie verhindert leesbevoegdheid en de niet-hiërarchische categorieën verhinderen schrijfbevoegdheid.
5. De hiërarchische classificatie en de niet-hiërarchische categorieën verhinderen leesbevoegdheid.
6. De hiërarchische classificatie verhindert leesbevoegdheid en de niet-hiërarchische categorieën verhinderen lees- en schrijfbevoegdheid.
7. De hiërarchische classificatie verhindert schrijfbevoegdheid en de niet-hiërarchische categorieën verhinderen leesbevoegdheid.
8. De hiërarchische classificatie verhindert schrijfbevoegdheid en de niet-hiërarchische categorieën verhinderen lees- en schrijfbevoegdheid.

Mandatory Protection (B)
De belangrijkste eis aan deze klasse is dat de TCB met behulp van labels een verzameling mandatory toegangsregels kan handhaven.

De labels worden toegekend aan 'subjecten' (processen die de gebruikers vertegenwoordigen) en 'objecten' (bestanden, randapparaten en dergelijke). De labels bestaan uit twee componenten: een hiërarchische classificatie en één of meer niet-hiërarchische categorieën. Met behulp van deze categorieën kunnen, net als met het discretionary-mechanisme van access control lists, nadere restricties in bevoegdheden worden aangebracht, maar nu met een mandatory werking. In een commerciële omgeving kan men bijvoorbeeld onderscheid maken tussen de categorieën Kantoor, Magazijn en Fabriek, waarbij een fabrieksmedewerker alleen fabrieksinformatie mag lezen, ongeacht zijn (hiërarchische) clearance. Met deze categoriebeveiliging kan echter niet dezelfde verfijning worden aangebracht als met access control lists.
Ook de categoriebeveiliging voldoet aan de principes van 'niet hoger lezen, niet lager schrijven', waarbij 'lager' moet worden geïnterpreteerd als zijnde een deelverzameling van 'hoger'. Leestoegang wordt verleend indien de hiërarchische classificaties van subject en object voldoen aan het principe van 'niet hoger lezen', én de niet-hiërarchische categorieën van het subject die van het object omvatten. Voor schrijftoegang is vereist dat de hiërarchische classificaties voldoen aan het principe van 'niet lager schrijven', én dat de niet-hiërarchische categorieën van het *object* die van het *subject* omvatten.
Een voorbeeld van de classificatie- en categoriebeveiliging wordt gegeven in figuur 3 (vrij naar [Paan91), waarbij men kan denken aan een autofabrikant, met geheime fabrieksinformatie.

De B-klasse is nader ingedeeld in de subklassen B1, B2 en B3, met oplopende eisen. Het belangrijkste verschil tussen B1 en B2 is het werkingsgebied; bij B1 vallen de subjecten en objecten *die worden beheerst door de TCB* onder de werking, maar bij B2 *alle* subjecten en objecten. Bij B3 moet de TCB voldoen aan de reference monitor-vereisten.

Verified Protection (A)
Aan deze klasse worden geen verdere eisen gesteld op het gebied van beveiligingsfunctionaliteit. Het verschil met B3 is dat het ontwerp van de TCB formele verificatie van de beveiligingsfunctionaliteit mogelijk moet maken.

Hoewel het Orange Book is gericht op de geheimhouding van informatie en de evaluatiecriteria bedoeld zijn voor toepassing in een militaire omgeving, streven leveranciers van computersystemen voor commercieel gebruik ernaar een zo hoog mogelijk Orange Book-certificaat te verkrijgen. Beveiliging geldt als marketinginstrument en het Orange Book als het meest gezaghebbend.
Op dit punt is de stand van zaken momenteel dat voor IBM-mainframe-omgevingen beveiligingsprodukten met een B1-classificatie standaard zijn, terwijl voor midrange-produkten C2 gangbaar is. Wel zijn vaak speciale beveiligde versies van midrange-besturingsprogrammatuur beschikbaar of in ontwikkeling die voldoen of moeten voldoen aan de B1-criteria. Voor besturingsprogrammatuur van Local Area Networks zijn binnenkort de eerste C2-certificaten te verwachten.[3]

Men kan zich afvragen wat het belang van deze certificaten is voor het bedrijfsleven. Ontegenzeggelijk biedt een Orange Book-certificaat bepaalde waarborgen over de aanwezige beveiligingsfunctionaliteit en de werking daarvan. Maar niet alle functionaliteit is van evenveel nut voor het bedrijfsleven. Slechts weinig organisaties zullen bijvoorbeeld de behoefte hebben 'system wide' te voldoen aan de C2-eis aangaande het schonen van geheugenmedia voordat zij beschikbaar worden gesteld voor hergebruik.

Voorts kan worden betwijfeld of er in het bedrijfsleven grote behoefte bestaat aan mandatory beveiliging zoals die in het Orange Book is uitgewerkt. Deze beveiliging is gericht op de geheimhouding en waarborgt daartoe een eenrichtingsverkeer van informatie van beneden naar boven. Het bedrijfsleven heeft er juist behoefte aan te *verhinderen* dat informatie van beneden naar boven gaat, dat wil zeggen als hiervan de integriteit niet vaststaat.[4]
Daadwerkelijke implementatie van B-beveiliging heeft voor het bedrijfsleven in het algemeen pas zin als de labels en het bijbehorende mandatory mechanisme kunnen worden aangewend of 'misbruikt' voor integriteitshandhaving. Ondanks onderzoek (zie bijvoorbeeld [Berg92]) biedt de theorie nog onvoldoende aanknopingspunten over hoe dit zou kunnen worden gerealiseerd. Daarbij komt dat het definiëren en onderhouden van de labels een grote inspanning zullen vergen, vooral door de complexiteit, zoals uit figuur 3 moge blijken.

Een praktisch, maar wel fundamenteel, punt van kritiek op het Orange Book is overigens nog dat geen enkele klasse voldoende bescherming biedt tegen misbruik van bevoegdheden door de 'security administrator', degene die belast is met het onderhouden van de autorisatieregels en labels.

Het bedrijfsleven onderkent dat niet alle Orange Book-certificaten van evengroot belang zijn.

Een toegekend Orange Book-certificaat houdt niet in dat een willekeurig systeem ook aan de eisen voldoet. Veel van de beveiligingsmechanismen moeten via optie-instellingen worden geactiveerd en bovendien zal de feitelijke systeemconfiguratie afwijkend zijn van het gecertificeerde produkt. Met name in IBM-mainframe-omgevingen zal er daarnaast sprake zijn van lokale modificaties van de besturingsprogrammatuur.

Het Orange Book is gevolgd door een reeks van publikaties die een nadere toelichting geven op bepaalde onderwerpen. Zo bestaan er nadere interpretaties van het Orange Book voor netwerk- en database-omgevingen ([NCSC87] respectievelijk [NCSC91]), uitgebracht door het National Computer Security Center. Vanwege de steeds andere kleur van de omslag wordt gesproken van de regenboogreeks.
Daarnaast is het Orange Book de aanleiding geweest tot een reeks van initiatieven in andere landen, waaronder Nederland.

Ontwikkelingen in Europa

Enige jaren na het verschijnen van het Orange Book werd ongeveer tegelijkertijd in Duitsland en in Groot-Brittannië de aanzet gegeven tot het ontwikkelen van eigen richtlijnen voor het beveiligen van geautomatiseerde systemen en het evalueren van produkten. Als spoedig mondde dit uit in een gezamenlijk initiatief, waarbij ook Frankrijk en Nederland zich aansloten. Dit initiatief werd vervolgens overgenomen door de Raad van de Europese Gemeenschappen en culmineerde in 1991 in de publikatie van de 'Information Technology Security Evaluation Criteria' (ITSEC) [CEC91].

De ITSEC-standaard borduurt voort op het Orange Book, maar is erop gericht een aantal tekortkomingen hiervan weg te nemen. De belangrijkste verschillen zijn de volgende:

- In het Orange Book wordt voor wat de classificatie betreft geen onderscheid gemaakt tussen beveiligingsfunctionaliteit als zodanig en de zekerheid dat het beveiligingsmechanisme goed werkt ('assurance'). De oplopende eisen die aan de C- en B-(sub)klassen worden gesteld, hebben betrekking op zowel de functionaliteit als de assurance. Alleen

3 *Overigens werd al in 1985 aan een besturingssysteem het B2(!)-certificaat toegekend. Dit betrof Honeywell Multics, waarbij Multics staat voor Multiplexed Information and Computing Service.*
Dit besturingssysteem heeft een vanuit beveiligingsoogpunt interessante architectuur, gekenmerkt door 'protection rings' en toegangscontrole gebaseerd op 'capabilities'. Deze architectuur is bij uitstek geschikt om ook integriteitsregels te handhaven. Helaas is dit besturingssysteem niet commercieel levensvatbaar gebleken. Wel heeft het geleid tot de ontwikkeling van een besturingssysteem dat momenteel een grote commerciële bloei doormaakt: Unix, aanvankelijk Unics gedoopt (Uniplexed Information and Computing Service) [Lith94].

4 *Op dit uitgangspunt is het model van Biba [Biba77] gebaseerd. Dit model is een inversie van het Bell/LaPadula-model, dat wil zeggen dat de lees- en schrijfregels zijn omgekeerd. Doordat integriteit geen inversie is van geheimhouding is deze ingreep te rigoureus.*

aan de overgang van B naar A worden uitsluitend assurance-eisen gesteld.
In de ITSEC-standaard worden afzonderlijke klassen onderscheiden voor functionaliteit en assurance.

– De ITSEC-standaard gaat in dit opzicht nog verder. Het staat de aanbieder binnen zekere grenzen vrij om zelf aan te geven welke beveiligingsfunctionaliteit moet worden geëvalueerd. Voor het specificeren van de te evalueren functionaliteit, 'Target Of Evaluation' (TOE) genoemd, is een speciale, semi-formele 'claims language' ontwikkeld.[5] Wel zijn in de standaard enkele functionaliteitsklassen voorgedefinieerd, waaronder de vijf Orange Book-functionaliteitsklassen.

– De ITSEC-standaard is niet alleen gericht op de geheimhouding van informatie, maar ook op de integriteit en de beschikbaarheid. Hiervoor zijn zelfs aparte functionaliteitsklassen voorgedefinieerd. Deze klassen zijn echter onvoldoende uitgewerkt om van praktisch nut te zijn.

Daarnaast zijn er verschillen in de organisatie van de evaluatie en de certificatie, en in de wijze waarop de kosten van evaluatie en certificatie worden gedragen.

Besturingssystemen met een ITSEC-certificaat zijn er nog niet veel, en zo ze er wel zijn is er niet veel bekendheid aan gegeven. Opmerkelijk in dit verband is de aankondiging van Novell dat voor het produkt Netware (versie 4.x) niet alleen een aanvraag is ingediend voor een Orange Book (C2)-certificaat, maar ook voor een overeenkomstig ITSEC-certificaat (zie Automatisering Gids/GKE/22-04-'94).[6]
De ITSEC-standaard is een voorlopige standaard, met in eerste instantie een werkingsduur van twee jaar. Inmiddels is besloten geen nieuwe versies meer uit te brengen maar de inspanningen te richten op een gezamenlijk initiatief met de Verenigde Staten en Canada. Of ook Japan, dat een eigen standaard heeft ontwikkeld, zich hierbij zal aansluiten, is niet bekend.

Intussen mag een ander Europees initiatief hier niet onvermeld blijven. In maart 1992 nam de Raad van de Europese Gemeenschappen het besluit om een algemeen raamwerk te creëren waarbinnen vraagstukken op het gebied van informatiebeveiliging kunnen worden geadresseerd en oplossingen kunnen worden ontwikkeld. In dit kader werd een comité ingesteld bestaande uit een groep van hoge ambtenaren (Senior Officials Group for Information Systems Security - SOG-IS) [REG92].
Dit besluit leidde tot het opstellen van een actieplan voor 1992 (Infosec '92), waarin veertien deelprojecten werden beschreven, waaronder een viertal met betrekking tot de ITSEC-standaard.
Infosec '92 werd gevolgd door Infosec '93, waarin veertien vervolgprojecten zijn gedefinieerd [CEC 93-1]. Eén van deze projecten heeft geresulteerd in het uitbrengen van een Green Book, een brede verkenning van het terrein van informatiebeveiliging, waarin wordt ingegaan op zulke uiteenlopende onderwerpen als de globalisering van de economie, de mensenrechten in relatie tot communicatiebescherming en veiligheid, economische aspecten van beveiliging, 'Trusted Third Parties' (TTP's), evaluaties van beveiligingsprodukten en beveiligingsmaatregelen [CEC93-3]. Per onderwerp worden in het Groenboek risico's of aandachtspunten en te ondernemen acties geïdentificeerd.
Infosec '93 is inmiddels opgevolgd door Infosec '94, met als hoofdthema elektronische handtekening en TTP's [CEC94].

Verdere harmonisatie

Waren de ITSEC al 'harmonised' (binnen Europa), inmiddels is besloten tot een verdere internationale harmonisatie door de inspanningen in Europa, de Verenigde Staten en Canada te bundelen.

Eén van de aanleidingen tot deze harmonisatie was het uitbrengen in december 1992 van het eerste, voorlopige concept van de 'Federal Criteria for Information Technology Security', een gezamenlijk project van NIST en NSA (zie [NIST92]; het 'definitieve' concept, bedoeld om publiek commentaar uit te lokken, verscheen in januari 1993). Het was de bedoeling dat deze criteria zouden uitgroeien tot een 'Federal Information Processing Standard' (FIPS) en het Orange Book zouden vervangen.
De Federal Criteria (FC) zijn gericht op de aspecten vertrouwelijkheid, integriteit en beschikbaarheid, en bevatten elementen van het Orange Book, de Europese ITSEC en de Canadese CTCPEC ('Canadian Trusted Computer Product Evaluation Criteria').
De FC bestaan uit twee delen. In deel 1 worden de componenten waaruit de beveiligingsfunctionaliteit bestaat geanalyseerd en worden de evaluatiecriteria behandeld. Deel 2 bevat een beschrijving van een aantal voorgedefinieerde functionaliteitsklassen ('protection profiles' genoemd), waaronder klassen die overeenstemmen met de Orange Book-classificatie.
Evenals bij de ITSEC is bij de FC onderscheid gemaakt tussen functionaliteit en assurance. De assurance valt uiteen in 'development assurance' en 'evaluation assurance'.

De kennelijke doublure die de FC inhielden met inspanningen elders in de wereld leidde tot het gezamenlijk initiatief van Europa (Europese Commissie), de Verenigde Staten (NIST en NSA) en Canada (Communications Security Establishment (CSE)). Dit initiatief beoogt de ontwikkeling van Common Criteria (CC), die 'achterwaarts compatibel' dienen te zijn met de bestaande standaarden. Als eerste actie is in februari 1994 een studie gestart naar de mogelijkheden om aan development assurance een hoge mate van zekerheid te ontlenen over de werking van de beveiligingsfunctionaliteit. Dit is nodig in verband met de steeds korter wordende 'time to market' van IT-produkten, waardoor het evaluatieproces zo efficiënt mogelijk moet worden ingericht.

De harmonisatie is nog niet volmaakt. Zo zijn er nog problemen met de wederzijdse erkenning van beveiligingscertificaten, niet alleen tussen Europa en Noord-Amerika maar ook binnen Europa. Voorts wordt in de vertegenwoordiging van de

5 *Dit is duidelijk in afwijking met het Orange Book, waarin, overigens zonder nadere argumentatie, wordt gesteld dat 'it is highly desirable that there be only a small number of overall evaluation classes' [DoD85].*

6 *Waarschijnlijk hebben de kraakprogramma's die in Nederland zijn ontwikkeld, onder andere door de hackersgroep die ook het blad Hack-Tic uitgeeft, hiertoe mede aanleiding geven. Door deze kraakprogramma's (KNOCK.EXE en HACK.EXE) werd het vertrouwen in de beveiliging van Novell ernstig ondermijnd. Een Europees beveiligingscertificaat kan ertoe bijdragen het vertrouwen terug te winnen. (Zie hiervoor ook [Ramo93].)*

Verenigde Staten het NCSC gemist, de hoeder van de Orange Book-standaarden en de instantie die de desbetreffende evaluaties uitvoert. Niet uitgesloten is dat het Amerikaanse Ministerie van Defensie vasthoudt aan haar eigen standaard, hetgeen zou kunnen leiden tot een afzonderlijke standaard voor (Amerikaanse) militaire omgevingen naast een standaard voor commerciële omgevingen. Vooral voor leveranciers van IT-produkten is dit een ongewenste situatie.

Andere standaarden

Op automatiseringsgebied zijn wereldwijd behalve de reeds genoemde nog talloze andere standaardisatie-instanties actief. Te denken is aan ANSI[7], CCITT[8], IEEE[9], ISO[10] en de Verenigde Naties (met Edifact). Deze instanties hebben inmiddels een respectabel aantal beveiligingsstandaarden ontwikkeld, die meestal van toepassing zijn op deelgebieden en die elkaar deels overlappen. Een voorbeeld is het bekende DES-encryptie-algoritme, gespecificeerd in ANSI X3.92 en FIPS-PUB-46/1.
Het voert te ver om hierop in dit artikel nader in te gaan. Verwezen wordt naar [NGI93]. Wel is nog te vermelden dat het de bedoeling is de Common Criteria na completering in te brengen in ISO (zie [Scho93]).

ALTERNATIEVE BENADERINGEN: DE BASELINE APPROACH

Zoals ook de teneur is van de uitkomsten van één van de Infosec-deelprojecten, bestaat er in het bedrijfsleven vooral behoefte aan praktische regels die een basisniveau van beveiliging beschrijven.
In deze paragraaf wordt ingegaan op drie pragmatische benaderingen van informatiebeveiliging.

Baseline approach van SRI/I-4

De bekende Donn Parker van het Stanford Research Institute houdt zich al sedert het begin van de jaren zeventig bezig met informatiebeveiliging. Ten behoeve van de leden van de I-4 startte het SRI in de jaren tachtig een project voor het identificeren van 'baseline controls' voor informatiebeveiliging. De leden van de I-4 (International Information Integrity Institute) zijn grote ondernemingen en overheidsinstanties. De geïdentificeerde baseline controls zijn mede gebaseerd op de praktijk bij zestig van deze leden.

De baseline-benadering berust op de inzichten die in vijfentwintig jaar denken over informatiebeveiliging zijn gegroeid, de communis opinio van beveiligingsexperts, de beschikbaarheid van beveiligingsprodukten en de 'controls' die in de praktijk daadwerkelijk worden toegepast.
De acceptatiegraad van baselines wordt bepaald door de mate waarin zij algemeen in de praktijk worden toegepast. In dit opzicht verschillen zij van standaarden, die hun gezag vooral ontlenen aan het standaardisatie-instituut, en die soms dwingend kunnen worden opgelegd.
De voordelen van de baseline-benadering zijn met name gelegen in efficiëntie; het instellen van baseline controls bespaart de kosten van een uitvoerige analyse van bedreigingen, mogelijke schade, kwetsbare plekken en mogelijke maatregelen, terwijl toch een aanvaardbaar basisniveau van informatiebeveiliging wordt gerealiseerd.

De baseline-benadering wordt gekenmerkt door pragmatisme.

De meest recente versie van de SRI/I-4-baselines dateert van 1993 [SRI93]. De totaal circa driehonderd baselines zijn ingedeeld in zeventien groepen, waaronder beveiligingsbeleid, organisatie, 'security audits', fysieke beveiliging, netwerkbeveiliging, beveiliging van gedistribueerde omgevingen, gebruikersidentificatie en -authenticatie, backup en recovery, systeemontwikkeling, operations en werkstationbeveiliging. Bij elke baseline control is onder meer aangegeven de mate van toepassing bij I-4-leden en een indicatie van kosten en effectiviteit.

Code of Practice

De 'Code of Practice' is ontwikkeld door het Britse Department of Trade and Industry met medewerking van het British Standards Institution en een groep vooraanstaande bedrijven, waaronder Midland Bank, Shell en Unilever [BSI93]. De doelstelling is om ondernemingen een gemeenschappelijke basis te verschaffen voor het ontwikkelen, implementeren en meten van effectieve informatiebeveiliging, en om vertrouwen te verschaffen bij handelsverkeer tussen ondernemingen.

Zowel de opzet als de inhoud van de Code of Practice vertoont sterke overeenkomsten met de I-4-benadering. De mogelijk te treffen maatregelen zijn ingedeeld in tien groepen, die vergelijkbaar zijn met de zeventien I-4-groepen. Een verschil is wel dat in de code een tiental maatregelen als 'key controls' wordt aangemerkt, ofwel omdat zij op grond van wettelijke vereisten een verplicht karakter hebben, ofwel omdat zij gelden als fundamentele bouwstenen (bijvoorbeeld ter bevordering van het beveiligingsbewustzijn). Deze key controls zijn van toepassing op alle organisaties en alle omgevingen[11].

De Code of Practice is algemeen geldend van opzet en daarmee onafhankelijk van specifieke IT-omgevingen. Hetzelfde geldt voor de I-4-baselines. Deze algemene toepasbaarheid brengt met zich mee dat de beschreven maatregelen een weinig concreet karakter hebben. De controls zijn vooral organisa-

7 *American National Standards Institute.*
8 *Comité Consultatif International pour le Télégraphique et le Téléphonique.*
9 *Institute of Electrical and Electronics Engineers.*
10 *International Organization for Standardization.*
11 *November jl. heeft het Nederlands Normalisatie-instituut de Code in Nederlandse vertaling uitgebracht, met als titel: Code voor Informatiebeveiliging. Een leidraad voor beleid en implementatie.*

torisch van aard en geven geen antwoord op de vraag hoe in een specifieke situatie bepaalde beveiligingsopties van een bepaald beveiligingsprodukt moeten worden ingesteld. Nu is dit ook niet te verwachten van een benadering gericht op het realiseren van een basisniveau van beveiliging. Vooral de meer concrete, technische beveiligingsmaatregelen moeten worden vastgesteld door de betrokken organisatie, afhankelijk van de specifieke situatie. Een voorbeeld van een dergelijke uitwerking is de IBM-benadering.

IBM-benadering

Mede uit onvrede over de geringe toegevoegde waarde van internationale beveiligingsstandaarden als het Orange Book en ITSEC voor de informatiebeveiliging in een operationele omgeving, stelde IBM begin jaren negentig een internationale werkgroep in met als opdracht het inventariseren van bestaande beveiligingsnormen, het onderkennen van als bureaucratisch ervaren maatregelen en het opstellen van normen die passen binnen de organisatie en aansluiten op de stand van de techniek (zie [Paan93]). Dit resulteerde in het uitbrengen van een IBM-beveiligingsstandaard [IBM93], op basis waarvan beveiligingsprodukten werden ontwikkeld en nieuwe procedures werden geïmplementeerd. Daarnaast geldt de standaard als toetsingsnorm bij EDP-audits.

De standaard omvat de fysieke en logische beveiliging van mainframes, middelgrote systemen, externe netwerkverbindingen en decentrale LAN's. De te realiseren beveiliging is gebaseerd op een classificatie van de systemen, met als criteria de vertrouwelijkheid van de informatie, de waarde voor de zakelijke processen en de waarde van de apparatuur. Op grond van de classificatie worden concrete normen geformuleerd voor de fysieke toegangsbeveiliging, logische toegangsbeveiliging en netwerkbeveiliging. In de bijlagen bij de standaard wordt aangegeven hoe deze systeem-onafhankelijke normen moeten worden geïmplementeerd in de besturingsprogrammatuur (zie hiervoor verder [Paan93]).

De IBM-benadering is niet zonder meer toepasbaar voor andere organisaties. Men kan ervan uitgaan dat de voorschriften zullen leiden tot een adequaat niveau van informatiebeveiliging, maar zij kunnen conflicteren met een beleid van decentralisatie. De vorming van zelfstandige business units, met een zekere vrijheid om een eigen IT-beleid te voeren, verhoudt zich slecht met het voorschrijven van gedetailleerde beveiligingsnormen. In een dergelijke situatie moet een middenweg worden gevonden tussen assurance over het niveau van informatiebeveiliging enerzijds en beleidsvrijheid van de gedecentraliseerde bedrijfsonderdelen anderzijds.

TOT BESLUIT

Het theoretisch onderzoek naar informatiebeveiliging heeft belangwekkende inzichten opgeleverd over basisprincipes om kwaliteitsaspecten van informatie - vooral vertrouwelijkheid, in mindere mate integriteit en nog nauwelijks beschikbaarheid - te waarborgen. Op dit moment lijkt de theorie een beetje op dood spoor te zijn beland; het wachten is op een nieuw soort Bell/LaPadula-model, waarin de tot dusver onderbelichte kwaliteitsaspecten beter tot hun recht komen.

De standaarden die zijn voortgekomen uit het BLM hebben vooral betrekking op centrale, batchgewijze verwerkingsomgevingen en betreffen de hardware, besturingsprogrammatuur en applicaties. Zij zijn gericht op het evalueren en certificeren van een bepaald produkt zoals dat voor evaluatie wordt aangeboden, en niet op het certificeren van een operationele omgeving, bestaande uit meerdere produkten en een organisatie daar omheen.
Wel zijn de standaarden in zekere mate aangepast of nader toegelicht om toepasbaar te zijn in database- en netwerkomgevingen.

De alternatieve baseline-benadering richt zich juist op de operationele omgeving en de organisatorische maatregelen. Als bezwaar tegen de baselines kan echter naar voren worden gebracht dat zij het karakter hebben van een checklist-benadering, en de elegantie ontberen van een axiomatisch beveiligingsmodel.

De spanning tussen theorie en praktijk van informatiebeveiliging is te vertalen als de wisselwerking tussen een mechanische, op mathematische principes gebaseerde benadering en een benadering gebaseerd op 'professional judgement'. Dit spanningsveld doet zich tevens voor op het gebied van bijvoorbeeld risico-analyse.
Ook in de accountancy is een slingerbeweging waarneembaar tussen de mathematische benadering, gebaseerd op kwantitatieve risico-analyse, en de benadering die het menselijke oordeel vooropstelt.

Op het gebied van informatiebeveiliging zijn twee tendensen te onderkennen. Enerzijds voldoen de beveiligingsprodukten steeds meer aan de theorie van de beveiligingsmodellen, anderzijds blijkt uit de praktijk een toenemende belangstelling voor baseline-benaderingen.
Bij de tweede tendens is een grotere rol van het professional judgement van de EDP-auditor te verwachten.

LITERATUUR

[Abra93] M.D. Abrams et al., *Report of an integrity research study group*, Computers & Security, Vol. 12, No. 7, 1993.

[Bell73] D.E. Bell and L.J. LaPadula, *Secure Computer Systems: Mathematical Foundations and Model*, The MITRE Corporation, 1973.

[Bell76] D.E. Bell and L.J. LaPadula, *Secure Computer Systems: Unified Exposition and Multics Interpretation*, The MITRE Corporation, 1976.

[Berg92] M. van den Bergh, *Geheimhouding en integriteit van computergegevens, Concepten voor een effectieve en controleerbare beveiliging*, ongepubliceerd manuscript, 1992.

[Biba77] K.J. Biba, *Integrity Considerations for Secure Computer Systems*, ESD-TR-76-372, Air Force Electronic Systems Division, 1977.

[BSI93] British Standards Institution, *A Code of Practice for Information Security Management*, DISC PD0003, 1993.

[CEC91] Commission of the European Communities, Directorate-General XIII, Directorate F, *Information Technology Security Evaluation Criteria (ITSEC)*, Provisional Harmonised Criteria, 1991.

[CEC93-1] Commission of the European Communities, Directorate-General XIII, Directorate B, *Infosec '93, Security Investigations, The Security of Information Systems*, 1993.

[CEC93-2] Commission of the European Communities, Directorate-General XIII, Directorate B, *Information Technology Security Evaluation Manual (ITSEM)*, Provisional Harmonized Criteria, 1993.

[CEC93-3] Commission of the European Communities, Directorate-General XIII, Directorate B, *Green Book on the Security of Information Systems*, Draft 4.0, 1993.

[CEC94] Commission of the European Communities, Directorate-General XIII, Directorate B, *Infosec '94, Security Investigations, The Security of Information Systems*, 1994.

[Clar87] D.D. Clark and D.R. Wilson, *A Comparison of Commercial and Military Policies*, Proceedings of the 1987 IEEE Symposium on Security and Privacy, 1987.

[DoD85] Department of Defense, *Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, 1985.

[IBM93] IBM Europe, *ISS EMEA: Information Processing Security Standards*, Draft version 0.2, 1993.

[Lith94] M.C. van Lith, *Beveiliging van Unix*, Compact 1994/2.

[NCSC87] National Computer Security Center, *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria*, NCSC-TG-005, Version-1, 1987.

[NCSC91] National Computer Security Center, *Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria*, NCSC-TG-021, Version-1, 1991.

[NIST92] National Institute of Standards and Technology & National Security Agency, *Federal Criteria for Information Technology Security*, Volume I and II, Version 1.0, 1992.

[NGI90] NGI, Sectie EDP Auditing, Werkgroep Beveiligingssystemen, *Beveiligingssystemen - een visie op toegang, toegang tot een visie*, 1990.

[Paan91] R. Paans, *With MVS/ESA Labels Towards B1*, Computers & Security, Vol. 10, 1991.

[Paan93] R. Paans, *Beveiligingsstandaard voor informatiesystemen*, Compact 1993/2.

[Pfle89] C. B. Pfleeger, *Security in Computing*, Prentice Hall International, 1989.

[Ramo93] J.L. Ramos Najera, *Beveiligingsperikelen rondom Novell Netware*, Compact 1993/1.

[REG92] Raad van de Europese Gemeenschappen, *Besluit van 31 maart 1992 betreffende de beveiliging van informatiesystemen*, 92/242/EEG, Publikatieblad van de Europese Gemeenschappen, Nr. L 123/19, 1992.

[Scho94] H. Schoone, *NIST Workshop on Federal Criteria*, NGI Nieuwsbrief, Afdeling Beveiliging, december 1993.

[SRI93] SRI International, *The Baseline Approach*, rapport ten behoeve van de leden van het International Information Integrity Institute (I-4), 1993.

[Stro93] L.A.M. Strous (red.) et al., *Standaardisatie van informatiebeveiliging*, een inventarisatie, NGI Afdeling Beveiliging, 1993.

Drs. P. Veltman RE RA
Is sedert 1983 werkzaam bij KPMG Klynveld, gedurende een aantal jaren in de controlepraktijk, thans in de functie van senior EDP-auditor. Zijn auditervaring ligt op het terrein van besturingssystemen en beveiligingspakketten, informatiesystemen en automatiseringsorganisaties. Hij heeft een aantal artikelen over deze onderwerpen gepubliceerd.

Informatie(beveiligings) beleid in concernverband

Prof. A.W. Neisingh RE RA

Het topmanagement is verantwoordelijk voor definiëring van en besluitvorming over een safety- en security-beleid. De afweging van centrale versus decentrale belangen in dezen is van cruciaal belang. Begripsvorming over de reikwijdte van dergelijk beleid gerelateerd aan de omvang van investeringen in informatietechnologie in een organisatie is op managementniveau een noodzaak.

INLEIDING

In dit artikel[1] wordt ingegaan op de rol van het management van een concern waarbinnen business units (BU's) of resultaatverantwoordelijke eenheden opereren met betrekking tot het informatiserings- en automatiseringsbeleid zoals dat door de organisatie-onderdelen zal zijn gedefinieerd. Investeringen in informatietechnologie vergen vaak grote bedragen, zodat besluitvorming door het hoogste orgaan in een organisatie in de lijn der verwachtingen ligt. Het concern-management vaardigt richtlijnen uit en dient verder over toetsingscriteria te kunnen beschikken om de aard en omvang van deze investeringen te kunnen beoordelen op aspecten als: past investering binnen de totale begroting, return-on-investment, produktiviteitsverbetering en verhoging van de kwaliteit van de informatievoorziening.
Ter ondersteuning van het topmanagement kan een afzonderlijke functie, de informatiemanager op concernniveau, grote diensten bewijzen.

Vanzelfsprekend geldt deze verantwoordelijkheid ook voor het informatiebeveiligingsbeleid als onderdeel van een safety- en security-beleid (veiligheid en beveiliging).
Het concern-management dient de uitgangspunten, uitgewerkt in richtlijnen, voor de betrouwbaarheid, vertrouwelijkheid en continuïteit van de geautomatiseerde gegevensverwerking vast te stellen. Steeds vaker laat het topmanagement zich bijstaan door een op safety- en security-gebied gespecialiseerde staffunctie. Dit neemt niet weg dat het topmanagement verantwoordelijk blijft voor definiëring en besluitvorming ter zake van zo'n beleid.

Achtereenvolgens zal op vorenstaande problematiek worden ingegaan.

INFORMATISERING: BELEID

Bij het vaststellen van het ondernemingsbeleid zal de leiding mede een visie hebben op de rol van de informatievoorziening en de wijze waarop men deze wenst vorm te geven en te benutten voor de bedrijfsvoering. Deze visie betreft onder andere de rol van de informatievoorziening bij de toekomstige bedrijfsvoering, de kwaliteit van de informatievoorziening en de vorm van de informatieverstrekking. Bedoelde visie wordt wel aangeduid met de term informatiebeleid. Concreet betreft dit het deel van het totale beleid dat relevant is voor de informatievoorziening.

In het kader van het informatiebeleid zal het management op conceptueel niveau keuzes maken. Zo kan de visie van de ondernemingsleiding gericht zijn op een verdere uitbouw van de informatievoorziening met de nadruk op het verhelpen van knelpunten in de huidige informatievoorziening, doch ook op een verdergaand integreren van informatietechnologie in logistieke, financiële en andere processen.

De benadering van een onderneming kan echter ook gericht zijn op kansen (opportunities). Men gaat hierbij voorbij aan knelpunten in de huidige informatievoorziening en richt zich op nieuwe organisatiestructuren en besturingsmodellen waarvoor de toekomstige informatievoorziening ondersteuning moet bieden. Dit kan vooral gericht zijn op die bedrijfsonderdelen waar volgens de leiding de toekomstige groeimogelijkheden voor de onderneming liggen.

Op basis van het informatiebeleid - de visie van de leiding met betrekking tot de informatievoorziening - is het mogelijk een meerjarenplan vast te stellen. In de praktijk wordt dit plan vaak opgesplitst in een strategisch gericht lange-termijnplan en een meer technisch gericht middellange-termijnplan (uitvoeringssfeer). Deze plannen worden wel aangeduid met de termen informatieplan en automatiseringsplan. Hierbij is het automatiseringsplan een nadere concretisering van het informatieplan voor zover het de automatisering betreft. In voorkomende gevallen worden van het automatiseringsplan afgeleide, meer gedetailleerde plannen opgesteld, zoals het apparatuurplan en het plan voor infrastructurele projecten. De voor informatieplanning gekozen benaderingswijze (knelpunten of kansen) speelt bij het vervolgens automatiseren geen rol van betekenis meer.

De vraag of alle genoemde plannen separaat moeten worden opgesteld, is van ondergeschikt belang in het proces waarbij het informatiebeleid wordt vertaald in een concreet plan. Van belang is dat het beleid wordt vertaald tot op detailniveau, zodat daardoor de uitvoering voldoende kan worden gestuurd en bewaakt. Wel is in het genoemde vertaalproces een scheiding gewenst tussen projecten enerzijds en investeringen in de technische infrastructuur anderzijds. Een onderscheid kan worden gemaakt tussen het informatieplan en als nadere concretisering daarvan een projectenplan en een automatiseringshulpmiddelenplan. Als eindprodukt van de vertaalslag van het informatiebeleid kunnen de drie genoemde plannen als hoofdstukken in een geïntegreerd plan worden opgenomen.

De per business unit gedefinieerde beleidsplannen zullen ter goedkeuring aan het concern-management worden voorgelegd. Zijn leden zullen immers willen toetsen of het gebruik en de toepassing van informatietechnologie past in, respectievelijk aansluit op de informatiebehoeften van dit topmanagement zelf.
Verder vergt realisatie van het gedefinieerde informatiebeleid belangrijke investeringen in computer- en randapparatuur, datacommunicatie- en telefonievoorzieningen, in software en dergelijke.

Samenhang tussen centrale en decentrale plannen is een heikel punt.

De plannen dienen niet incidenteel te worden opgesteld, maar hebben een continu karakter en dienen dus ook voortdurend te worden beoordeeld op actualiteit en zo nodig te worden aangepast.
Op deze wijze passen jaarlijkse investeringen in informatietechnologie binnen een logisch en te voorzien geheel.

Gewenste aanpassingen in de meerjarenplannen en concretiseringen in de jaarplannen zullen altijd door een daartoe bevoegde functie moeten worden beoordeeld op hun nut, noodzaak en kosten. Om zo'n beoordeling te kunnen geven is het vaak noodzakelijk dat door de aanvrager gemotiveerd wordt aangegeven waarom zo'n aanpassing of aanvulling nodig is.
Het blijkt uit praktijkervaringen dat de opstellers van dergelijke voorstellen zich primair hebben geconcentreerd op de beschrijving van de huidige knelpunten en op de gewenste toekomstige situatie. Het is daarom soms moeilijk vanuit de voorgelegde plannen zich een oordeel te vormen omtrent het nut, de noodzaak en de omvang van de vereiste investering.

INFORMATISERING: FINANCIËLE CONSEQUENTIES

Het is doelmatig en effectief dat ten behoeve van de beoordeling van de plannen in het voorstel een afzonderlijke paragraaf wordt opgenomen. In deze paragraaf kunnen alle relevante informatie en de financiële consequenties van de investering worden opgenomen c.q. worden samengevat.

Hierna zijn enkele aandachtspunten opgenomen voor de invulling van zo'n paragraaf Investerings-

1 *Het artikel werd eerder gepubliceerd in Account Dossier 'Onderneming en Concern', 1994.*

aanvraag. De eisen die aan deze paragraaf zijn gesteld, zijn globaal weergegeven en zullen van situatie tot situatie kunnen worden aangepast, omdat de aard en de omvang van de inspanning zeer verschillend kunnen zijn.

Voor het beoordelen van een investering is het van belang de consequenties op een aantal terreinen te voorzien. Sommige van deze terreinen zijn niet te overzien door de aanvrager, wel door degene die de investering beoordeelt, andere zijn door het topmanagement moeilijk te beoordelen op realiteitsgehalte.

De IT-investeringsaanvraag dient onder meer de volgende gegevens te bevatten:

a. Aansluiting bij bestaand informatie- en automatiserings/IT-beleid
Aangegeven dient te worden in hoeverre het voorstel aansluit bij c.q. een uitwerking is van reeds vastgesteld informatie- en/of automatiserings/IT-beleid. Afwijkingen hiervan kunnen consequenties hebben voor overige projecten en zullen herziening van prioriteiten en dergelijke noodzakelijk kunnen maken. Zo zal het afwijken van bestaande apparatuur- en besturingsprogrammatuurlijnen gevolgen kunnen hebben voor de bestaande applicatieprogrammatuur en wellicht ook voor procedures inzake betrouwbaarheid en beveiliging. Ook binnen het bestaande beleid kan een investering wijzigingen noodzakelijk maken. Dit dient dan gemotiveerd te worden aangegeven.

b. De omvang van de investering
De omvang kan worden gemeten in geld en in arbeidsuren.

Investeringen dienen tastbaar te worden gemaakt.

Natuurlijk is het vaak moeilijk aan te geven wat de precieze kosten zullen zijn en zal moeten worden volstaan met schattingen. Indien dit laatste noodzakelijk is, moet worden aangegeven hoe hard deze schattingen zijn en welke de risicogebieden met betrekking tot overschrijding zijn.
De arbeidsuren dienen per discipline te worden weergegeven en tevens dient te worden vermeld of zich daarbij knelpunten zullen voordoen, zoals in verband met overbelasting van bepaalde functies (bijvoorbeeld de zeer bezette lijnfunctionaris die tevens dient mee te draaien in het project vanwege zijn specifieke deskundigheid). Bij dergelijke knelpunten moet een oplossing worden aangegeven (alsmede natuurlijk eventuele organisatorische en financiële consequenties).
Naast deze gegevens dienen ook de looptijd van de investering en de momenten van investering te worden aangeduid, teneinde de investering op financieel-economische gronden te kunnen inschatten. Hierop aansluitend dient ook duidelijk te worden aangegeven of en zo ja, in welke mate vervolginvesteringen (ook buiten het tijdvak van de onderhavige aanvraag) noodzakelijk zullen zijn teneinde de op termijn beoogde voordelen te kunnen bereiken.

c. De noodzaak of wens voor de investering
Het is bekend dat het vaak heel moeilijk is een kosten/baten-analyse te maken, vooral omdat de baten vooraf zo moeilijk te meten zijn.
Toch is inzicht in het nut van de investering noodzakelijk.
Altijd is een motivering in financiële termen zeer wenselijk. Zo kunnen moderniseringsprojecten, waarbij de functionaliteit ten minste gelijk blijft, vaak in financiële termen worden gemotiveerd; de vergelijking met de huidige kosten is immers te maken.
Ook voor volledig nieuwe projecten is het noodzakelijk de investering tevens in financiële termen uit te drukken. Een concrete financiële motivering is dan beslist niet eenvoudig, maar uitsluitend motiveren in termen als concurrentievoordeel en voordelen inzake organisatorische en personele aspecten is niet voldoende.
Het vermelden van deze imponderabilia blijft natuurlijk noodzakelijk. Getracht moet worden de onzekerheid zoveel mogelijk te beperken en er dient gemotiveerd te worden aangegeven welke informatie onderhevig is aan belangrijke onzekerheid.

Tot slot van dit onderdeel wordt opgemerkt dat de mogelijkheden moeten worden onderzocht of in concernverband synergetische voordelen te behalen zijn.
In dit verband valt te denken aan gemeenschappelijk gebruik van een concern-datacommunicatienetwerk, profiteren van quantumkortingen op apparatuur en licenties door gezamenlijke inkoop, het vastleggen van concernstandaarden met betrekking tot ontwikkeling van informatiesystemen, kwaliteitsbewaking en niet in het minst informatiebeveiligingsbeleid.
Een belangrijke rol kan zijn weggelegd voor een corporate informatiemanager.

CONCERN-INFORMATIEBEVEILIGINGSBELEID

Concernverbanden opereren in de praktijk nogal eens verschillend. Soms zijn de verschillende concernonderdelen zeer zelfstandig, in andere gevallen zijn duidelijke onderlinge structuren en afhankelijkheden herkenbaar. In het eerste geval zullen de concernonderdelen tamelijk zelfstandig zorg dragen voor informatiebeleid en het daaraan gerelateerde informatiebeveiligingsbeleid, en slechts zeer beperkt sturing op dit terrein door de concernleiding accepteren. Met name tijdens de laatste fusiegolf is gebleken hoe lastig het is om bedrijven

of bedrijfsonderdelen in een concern te integreren, indien binnen dat concern strakke richtlijnen bestaan inzake informatievoorziening c.q. informatiebeveiliging. Vaak gaat dat gepaard met desinvesteringen in de bestaande informatietechnologie. Daarbij bestaat een groot risico van verstoring van de kwaliteit van de informatievoorziening en van inbreuken op het getroffen stelsel van controle- en beveiligingsmaatregelen.

Concerns waar tussen de bedrijfsonderdelen slechts in beperkte mate uitwisseling van informatie plaatsvindt, doen er dus goed aan niet te veel 'van boven af' te sturen. De sturing die met het oog op een gelijkwaardig informatiebeveiligingsbeleid wel dient plaats te vinden betreft vooral de standaardisatie ten aanzien van niveau van beveiligingsmaatregelen tussen de concernonderdelen. Deze standaardisatie houdt met name in voorschriften inzake de eenduidige betekenis van gegevensdefinities, afspraken in verband met noodvoorzieningen en uitwijk, backup van gegevens en programmatuur, en dergelijke.

Voor concerns waarbij de onderlinge relaties sterker zijn, is door de concernleiding voordeel te behalen bij meer eenduidige voorschriften voor de concernonderdelen, zonder daarbij de eigen verantwoordelijkheid van het management van die onderdelen geweld aan te doen. Op het gebied van informatiebeleid is voordeel te behalen door het beperken van verschillende IT-infrastructuren en informatiesystemen, waardoor onderlinge communicatie eenvoudiger wordt, gesteund kan worden op elkaars kennis of ervaring en financieel voordeel door schaalgrootte te bereiken is. Niet voor niets is de laatste jaren weer een duidelijke tendens waarneembaar naar rekencentra op concernniveau, waarbij landsgrenzen geen beperkingen meer blijken te zijn. Na de tegengestelde beweging van 'downsizing' is juist nu het begrip 'outsourcing' actueel, waarbij het vaak blijkt te gaan om concentratie van de gegevensverwerking op één plaats binnen het concern. Van belang is ook in die situaties een en ander contractueel te regelen, hetgeen kan geschieden door het afsluiten van een service level agreement.

Op het gebied van het informatiebeveiligingsbeleid zal het verschil in opereren van concernverbanden zich op uiteenlopende wijze uiten. Voor de eerste categorie concerns zal de concernleiding zich veelal beperken tot het definiëren van beperkte 'mission statements', waarna de concernonderdelen ieder voor zich een beveiligingsbeleid opstellen en uitwerken.
Voor de meer samenhangende concerns stelt de concernleiding een (strategisch) informatiebeveiligingsbeleid op. De concernonderdelen zullen dit uitwerken in beveiligingsnormen op tactisch niveau, waarna de organisatie vervolgens maatregelen zal treffen om aan die normen te voldoen. Daarbij is het de taak van de concernleiding te zorgen dat de beveiligingsnormen tussen de concerns volgens dezelfde maatlat (namelijk het strategisch concernbeleid) worden vastgesteld. Voorschriften voor gegevensclassificatie, gekoppeld aan een categorie voor beveiligingsnormen, kunnen daarbij zeer effectief zijn.

IT-BELEID VAN DE HOLDING

Ook de holding zelf zal moeten definiëren welke informatiebehoefte noodzakelijk wordt geacht. Het proces om tot vastlegging en realisatie ervan te komen verschilt in principe niet van dat zoals besproken voor de afzonderlijke business units.
Bijzondere toepassingen dienen echter te worden overdacht. Zo kan gebruik worden gemaakt van executive information systems (EIS) om op eenvoudige en snelle wijze gegevens te extraheren uit BU-systemen.
Wanneer betalingsstromen centraal worden geleid, dienen informatiesystemen voor cash management en electronic banking in de beschouwing te worden betrokken. Over het algemeen worden daarmee risicovolle toepassingen (fraude) geïntroduceerd, die operationeel zijn in (zeer) kleinschalige automatiseringsomgevingen. Het holding-management dient zich dan ook te realiseren dat het op dit punt een eigen verantwoordelijkheid draagt.

STAFFUNCTIES OP CONCERNNIVEAU

In dit artikel zijn twee bijzondere functies aan de orde geweest, te weten:
- de informatiemanager op concernniveau; en
- de verantwoordelijke functionaris voor safety en security.

Vanuit hun verantwoordelijkheid en specialisme kunnen zij het concern-management bijstaan, zowel bij beleidsvoorbereiding als bij controle op daadwerkelijke implementatie.
Voor wat betreft de deskundigheid op het gebied van informatiebeveiligingsbeleid, normen en standaarden geldend voor de geautomatiseerde gegevensverwerking en dergelijke, alsmede beoordeling van kwaliteitsaspecten van automatisering (betrouwbaarheid, vertrouwelijkheid, continuïteit, efficiency en effectiviteit) kan een beroep worden gedaan op (interne en/of externe) EDP-auditors. Zij zijn bij uitstek in staat op het onderhavige terrein als auditors en adviseurs op te treden.

Kijken wij terug naar het onderwerp van dit artikel, dan kan naast de reeds genoemde kwaliteitsaspecten worden gedacht aan beoordeling van het investeringsplan, van de volledigheid van het informatieplan en van het gehele ontwikkelingstraject in de vorm van quality engineering/quality assurance.

Prof. A.W. Neisingh RE RA Is lid van de maatschap KPMG Klynveld EDP Auditors en deeltijd-hoogleraar betrouwbaarheidsaspecten van geautomatiseerde informatiesystemen aan de Rijksuniversiteit Groningen (vakgroep Accountancy). Zijn werkzaamheden liggen op het terrein van beoordeling en advies met betrekking tot kwaliteitsaspecten van het gebruik van informatietechnologie in organisaties. Verder is hij buitengewoon lid van de Registratiekamer, hoofdredacteur van Compact en lid van de adviesraad van het Handboek Informatiebeveiliging.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact
Een compilatie van artikelen over informatica en recht die in eerdere Compacts zijn verschenen, is, aangevuld met actuele bijdragen over dit onderwerp, opgenomen in *Twintig over Informatietechnologie en recht*. Twintig auteurs behandelen een breed spectrum van aspecten van de raakvlakken van informatietechnologie en recht op voor EDP-auditor, manager, adviseur, jurist en accountant toegankelijke wijze.
Het boek is verkrijgbaar via de boekhandel onder nummer: ISBN 90 14 04634 0.

3 20e jaargang 93/3 herfst 1993

De toegevoegde waarde van EDP-auditing bij systeemontwikkeling
Ir. J.A. Verstelle

Normenstelsels voor systeemontwikkeling: hoe bruikbaar zijn deze?
Mw.drs. C.D.M. van der Veen

Projectbeheersing en -audit: contingency-benadering vereist
Ir. B.A.W.M. Bruns

De toegevoegde waarde van inspectietechnieken tijdens het ontwikkeltraject
B. Rooth

Invoering van informatiesystemen
Drs. Th.H. van Hesteren

Twintig vuistregels voor 'foutloos' onderhoud
E. Bergler

4 20e jaargang 93/4 winter 1993

Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving
Drs. R.G.A. Fijneman RE RA

Aandacht voor interne controle tijdens systeemontwikkeling
Drs. J.J. van Beek RE RA

Audit automation
Drs. L.H. Dam RA en drs. P. Veltman RE RA

Operational auditing en EDP-auditing; is hier sprake van een begripsverwarring?
J.C. Boer RE RA

Accountant, EDP-auditor en jurist: een multidisciplinaire samenwerking
Mw.mr.drs. A.W. Duthler

Automatiseringsrisico's, verzekeringen en de rol van de accountant
Drs. G.J.W.C. Vankan

Geautomatiseerde betalingen
Drs. R. Oudega en drs. P. Veltman RE RA

1 21e jaargang 94/1 lente 1994

De invloed van informatietechnologie op de beheersing van organisaties
Prof. A.W. Neisingh RE RA

Rekencentra: normen voor menskracht
Prof.dr.ir. R. Paans RE

Accountant en de kosten- en batenbeheersing van informatietechnologie
Prof. H.B. Moonen RE RA

Informatiebeveiliging: de tijd is rijp
Drs. H.G.Th. van Gils RE RA

Het beoordelen van het testen van systemen
P. van Berge

2 21e jaargang 94/2 zomer 1994

Audit van een SNA-netwerk
M.M. Buijs RI en E.J.M. Ridderbeekx RE RI

Beveiliging van analoge kieslijnen
Drs.ing. D. Brouwer RE

Beveiliging van UNIX
Mw.drs. M.C. van Lith RE

Typologie van workflow-managementsystemen
Drs. D.J.P.Witte

3 21e jaargang 94/3 herfst 1994

Inleiding tot op TCP/IP gebaseerde netwerken
Ir. P. Kornelisse

Internet? Maar dan wel met een firewall!
H. van Hulst

Netwerkverbindingen in een OpenVMS-omgeving
Ir. J.H. Lie-Tjauw

Enige juridische wegwijzers voor de elektronische snelweg
Mw. mr. G.P. van Duijvenvoorde

Betrouwbaarheid en beveiliging van een CICS-omgeving
Ing. G.H.M. Meijer RE en mw. J.A.M. Holla