KWARTAALBLAD EDP-AUDITING

1995/3

INFORMATIETECHNOLOGIE EN DE ACCOUNTANTSFUNCTIE

COMPACT HERFST

Compact ®
Jaargang 22, nummer 3
Een uitgave van KPMG EDP Auditors NV en Samsom Bedrijfs-Informatie, 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
Drs. P. Veltman RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Prof.dr. J.C. Arnbak
J.H. Buisman RA
Ir. J.C. le Clerq
Mr. P. van Dijken
Prof.mr. H. Franken
Dr. K.Y. Mollema RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Redactiesecretariaat
Mw. I. de Koning,
Samsom Bedrijfsinformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 0172 - 466 746
Fax : 0172 - 466 569
Vormgeving
Bureau Karakter, Delft
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.: 0172 - 466 800
Fax : 0172 - 475 933
Adreswijzigingen - ook tijdelijke - moeten minstens 8 weken voor de verschijningsdatum bekend zijn.
Overname artikelen
Het overnemen en vermenigvuldigen van artikelen en berichten is slechts geoorloofd na schriftelijke toestemming van de uitgever.
Overdrukken artikelen
Overdrukken van artikelen kunnen worden aangevraagd bij het redactiesecretariaat. Prijs per overdruk per artikel (inclusief omslag) f 5,-.
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 EDP Auditors NV.

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 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.

Het gebruik van informatietechnologie in organisaties is niet meer weg te denken; accountants zullen derhalve bij het definiëren van de controle-aanpak ten behoeve van de jaarrekeningcontrole rekening moeten houden met de invloed van het gebruik van informatietechnologie op de inrichting van de administratieve processen. Gaandeweg worden interne administratieve processen, logistieke processen en externe administratieve processen verder geïntegreerd. Het voeren van administraties verandert daardoor van een handmatig proces met vele vastleggingen in een 'high tech' geautomatiseerd proces. Deze omgevingen worden in toenemende mate beheerst door gericht ontworpen interne-controlemaatregelen ter vervanging van de klassiek algemeen geldende uitgangspunten van functiescheiding en dubbele registratie.

De vraag die het verantwoordelijke management, en daarvan afgeleid de accountant, zich zal stellen is 'op welke wijze worden de routinematige processen binnen onze organisatie onder controle gehouden'. Gezien het efficiency-streven bij het integreren van administraties met de aanleverende systemen is het niet waarschijnlijk dat het proces zodanig is ingericht dat de betrouwbaarheid van het proces steunt op werkverdeling, dubbelwerk en detailcontroles. Vanuit de accountantswerkzaamheden bezien vindt een verschuiving plaats van 'checken' naar 'beoordelen'. In feite is er sprake van een substitutie van min of meer eenvoudige werkzaamheden uitgevoerd door assistent-accountants naar werk dat wordt uitgevoerd door EDP-auditors. Past de accountant zijn controle-aanpak niet aan dan zal het management van de organisatie niet begrijpen waarom de accountant geen gebruik maakt van de aanwezige controlemechanismen. Immers, de managers die zich hebben verdiept in de beheersing van de kwaliteit van de informatievoorziening op basis van geautomatiseerde systemen, verwachten dat de accountant dit ook zal doen en hieraan een belangrijk deel van zijn controlebewijs zal ontlenen.

In efficiënt georganiseerde organisaties steunt het management voor wat betreft de kwaliteit van de processen op de toereikendheid van de combinatie van geprogrammeerde controles en door mensen uitgevoerde controles, te zamen de application controls. De kwaliteit van de technische infrastructuur (general IT controls) is hierbij een basisvoorwaarde voor het management om de organisatie te kunnen beheersen. De accountant, in complexe situaties ondersteund door de EDP-auditor, stelt vast of de situatie daadwerkelijk wordt beheerst. Dat ook de wetgever waarde hecht aan de beoordeling van informatietechnologie door accountants moge blijken uit de wetgeving in het kader van de Wet computercriminaliteit. Deze schrijft voor dat de accountant zijn bevindingen over de betrouwbaarheid en continuïteit rapporteert in zijn verslag aan bestuur en raad van commissarissen (BW boek 2 artikel 393 lid 4).

Accountants zullen zich meer moeten verdiepen in informatietechnologie en de invloed ervan op de accountantsfunctie. De redactie verwacht dat deze Compact hieraan een goede bijdrage zal leveren en wenst u veel wijsheid bij de komende interimcontroles.

Prof. A.W. Neisingh RE RA

Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering

Mw. W.A. de Munck RA

In het kader van de controle van de jaarrekening is beoordeling van de wijze waarop het management van een onderneming de risico's met betrekking tot informatietechnologie beheerst, van toenemend belang. Door die beoordeling kan de accountant zich een indruk vormen over de kwaliteit van de informatievoorziening en op grond daarvan een betere invulling geven aan de controle van de jaarrekening en de klankbordfunctie voor het management.

INLEIDING

De ontwikkelingen in de controlefilosofie hebben de afgelopen jaren een grote vlucht genomen. De controle-aanpak was vaak in sterke mate gegevensgericht en de accountant beperkte zich bij de controle van de jaarrekening tot een beoordeling van de interne-controleprocedures, die de getrouwheid van de financiële verantwoording moesten waarborgen; de interne controles in engere zin. Op deze wijze kon de accountant de controle vaak zodanig inrichten dat hij geen specifieke aandacht hoefde te schenken aan de automatisering van de te controleren onderneming.
Tegenwoordig is bij de controle van de jaarrekening het streven van de accountant erop gericht zich een beeld te vormen van de bedrijfsrisico's die de onderneming loopt en de interne controles waarmee de ondernemingsleiding deze risico's tracht te beheersen; de interne controles in bredere zin of management control genoemd.
Informatietechnologie (IT) speelt bij het besturen van ondernemingen en bij het beheersen van bedrijfsrisico's steeds meer een belangrijke rol en moet om die reden zelf ook in voldoende mate worden beheerst. De wijze waarop inhoud wordt gegeven aan de beheersing van informatietechnologie binnen ondernemingen loopt sterk uiteen en wordt onder meer beïnvloed door de omvang van de automatiseringsorganisatie, de technologie waarmee wordt gewerkt en de vraag of er met standaard- of zelf ontwikkelde software wordt gewerkt.
Het is derhalve van groot belang dat binnen het controleteam voldoende IT-kennis beschikbaar is, niet alleen voor de realisatie van de meest effectieve en efficiënte controle-aanpak, maar ook om als kritisch klankbord van de ondernemingsleiding te kunnen fungeren.
Eind 1993 stelde Fijneman [Fijn93] dat informatietechnologie door certificerende accountants nog steeds te defensief werd benaderd. Hij gaf daarmee aan dat de accountant informatietechnologie nog slechts fragmentarisch beoordeelde en geen duidelijke en gestructureerde plaats gaf in zijn controlebenadering.
De inschakeling van een EDP-auditor is zeker niet vanzelfsprekend of wordt veelal slechts overwogen ten behoeve van een oordeel in het kader van de Wet computercriminaliteit. De werkzaamheden van EDP-auditors blijven dan veelal beperkt tot een beoordeling van de algemene computercontroles (general IT controls). De rapportering naar aanleiding van deze werkzaamheden geeft de accountant niet altijd het inzicht en begrip dat noodzakelijk is voor het verbeteren van de dienstverlening aan de cliënt en wellicht ook van de controle-aanpak.
Dit artikel beoogt te benadrukken dat door een goede inzet van IT-kennis in het controleproces, de accountant zich een gedegen oordeel kan vormen over de kwaliteit van de informatietechnologie bij de cliënt. Een goede samenwerking met EDP-auditors is hierbij van groot belang. Een controlefilosofie die zich richt op de bedrijfsrisico's en het beheersingssysteem van deze risico's dwingt meer dan ooit tot een tijdige en doelgerichte inschakeling van specialisten, zoals EDP-auditors.

DE FASERING VAN HET CONTROLEPROCES

In dit artikel zal per fase van het controleproces worden aangegeven op welke wijze aandacht moet worden geschonken aan informatietechnologie en wat het belang daarvan is. Daarbij worden niet noodzakelijkerwijs alle stappen per fase besproken. Slechts die stappen waarbij de aandacht voor informatietechnologie van groot belang is of nader invulling behoeft, zullen worden toegelicht. Voor een volledig beeld van de stappen per fase zijn in de figuren wél alle stappen opgenomen, en zijn de stappen die nader worden toegelicht daarin vet gedrukt.

De rol van de EDP-auditor moet tijdens het controleproces naadloos aansluiten op de behoefte van de accountant. Uitsluitend een goede vorm van samenwerking kan leiden tot analyses en conclusies die waardevol zijn voor de accountant én de onderneming.
De volgende fasen worden onderscheiden:

Vaststelling controlestrategie
Planning controle
Verkrijgen effectief controlebewijs
Afsluitende beoordeling en evaluatie van controle bevindingen
Rapportering
Slotevaluatie

Figuur 1. Controleproces.

VASTSTELLING VAN DE CONTROLESTRATEGIE

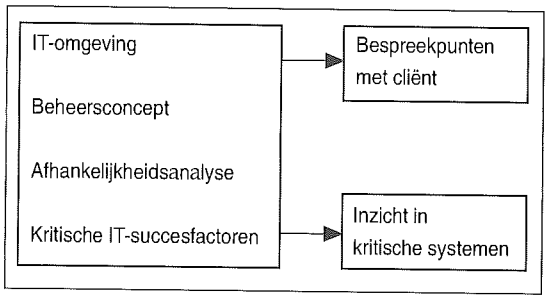
Tijdens de strategiefase verwerft de accountant inzicht in de aard en de omgeving van de onderneming. In deze fase richt de accountant zich op het bedrijfsgebeuren van de onderneming. Hij verwerft inzicht in de wijze waarop de leiding van de onderneming bedrijfsrisico's onderkent en deze tracht te beheersen.

Inzicht in het bedrijf van de cliënt
Inzicht in de wijze waarop de cliënt de ondernemingsrisico's tracht te beheersen
Vaststellen van de implicaties voor de controle

Figuur 2. Vaststellen van de controlestrategie.

Als de onderneming onderkent dat zij bepaalde risico's onvoldoende beheerst of als de accountant op grond van kennis en ervaring deze conclusie zelf trekt, is er sprake van risicovolle controlegebieden. Wat wel of niet risicovol is, wordt niet alleen bepaald door de kennis van de accountant over zijn eigen vakgebied, maar ook nadrukkelijk door de feitelijke situatie bij de onderneming.
Wat traditioneel door accountants als risicovol zou worden getypeerd, behoeft door goede interne beheersing bij de onderneming geen risicogebied meer te zijn. Een dergelijke situatie doet zich bijvoorbeeld voor als de kans op het ontstaan van fouten door complexe berekeningen groot is, maar door effectieve interne-controleprocedures in voldoende mate is gewaarborgd dat de fout tijdig wordt ontdekt. Het is in dergelijke situaties uiteraard wel van belang dat de accountant zich zekerheid verschaft over de effectiviteit van de interne beheersing van de risico's.

Voor de risico's en beheersingsmaatregelen ten aanzien van informatietechnologie bij een onderneming is het evenzeer van groot belang dat de accountant zich richt op de feitelijke situatie bij een onderneming. Figuur 3 geeft inzicht in de relevante IT-aspecten in de strategiefase.



Figuur 3. IT-aspecten in de strategiefase.

IT-omgeving

Inzicht in de IT-omgeving van de onderneming is onontbeerlijk voor de beoordeling door de accountant van het belang van automatisering voor de onderneming en het gekozen beheersconcept. Kennis over de IT-omgeving vormt daarbij de basis. De volgende aspecten zijn belangrijk voor een goed inzicht in de IT-omgeving:

- Inzicht in de informatiesystemen, bijvoorbeeld:
  - met welke systemen wordt gewerkt;
  - in welke mate zijn systemen gekoppeld en geïntegreerd;
  - in hoeverre vindt integratie plaats met externe systemen.

- Inzicht in de gebruikte technologie, bijvoorbeeld:
  - met welke besturingssoftware wordt gewerkt;
  - is sprake van een netwerkomgeving;
  - wat is de verwerkingstypologie (batch, online) van de verschillende systemen.

- Het profiel van de IT-organisatie, bijvoorbeeld:
  - wat is de omvang van de IT-organisatie;
  - is de IT-organisatie gecentraliseerd of gedecentraliseerd;
  - wat is het profiel van de IT-medewerkers (functies, opleiding e.d.).
- In welke mate zijn gebruikers betrokken bij IT-ontwikkelingen (variërend van vrijwel geen enkele betrokkenheid tot de situatie waarin de gebruikers budgettair en inhoudelijk volledig verantwoordelijk zijn gesteld voor informatietechnologie).

Het beheersconcept

In hun boek *Informatietechnologie; Management control van de geautomatiseerde informatievoorziening* geven Donkers, Groesz en Verstelle [Donk95] met behulp van een matrix, ontwikkeld door Nolan Norton, inzicht in een sturings- en beheersinstrumentarium, dat past bij de verschillende componenten van informatietechnologie.

De matrix geeft inzicht in de kenmerken van de componenten van informatietechnologie in de verschillende stadia van ontwikkeling, aangevuld met de daarbij behorende stadia van management control. Met behulp van deze matrix kan een indicatie worden gegeven of naar verwachting informatietechnologie op effectieve en efficiënte wijze wordt ingezet in de onderneming. Onevenwichtigheid in de stadia van ontwikkeling waarin de onderneming zich bevindt voor wat betreft de verschillende componenten in de matrix, zou kunnen duiden op een bewuste strategie van het management op dit gebied, maar ook op ineffectief gebruik van informatietechnologie. Immers, zo geven de schrijvers als voorbeeld van ineffectiviteit, het rendement van zeer geavanceerde IT-systemen en de meest vernuftige technologie zal doorgaans beperkt zijn, als de vaardigheden van de gebruikers in de omgang met informatietechnologie tekort schieten.

Met behulp van deze matrix kan een indicatie worden verkregen over de mogelijke effectiviteit van het gekozen management control-concept voor informatietechnologie. Deze indicatie kan belangrijk zijn voor de accountant voor het bepalen van zijn controlebenadering en kan aanleiding zijn om met het management van gedachten te wisselen.

Figuur 4. Kenmerken van de componenten in de verschillende stadia van ontwikkeling van informatietechnologie.

	Stadium van ontwikkeling					
Informatiesystemen	beperkt aantal niet-gekoppelde systemen gericht op efficiëntie-verbeteringen (de financiële en de salarisadministratie)	uitbreiding van systemen waarbij tevens koppeling binnen een afdeling plaatsvindt (de financiële administratie gekoppeld aan het budgetteringssysteem)	voltooiing van de taak-automatisering en bouw van de tweede generatie systemen	herbouwen van systemen gericht op organisatiebrede integratie over afdelingen heen	bouw van systemen die externe ondersteuning bieden aan bijv. afnemers en leveranciers	volledige integratie van externe en interne systemen per werkmaatschappij (business unit)
Technologie	mainframe/batch	combinatie van batch en online	hoofdzakelijk online	intelligente werkstations	invoering van nieuwe technologieën	down-sizing rekencentra
IT-personeel	computerspecialist	oriëntatie richting gebruikers	informatiemanager	facilitaire organisatie voor techniek	kennis vergaren van nieuwe technologie	IT-personeel naar de werkmaatschappij
IT-organisatie	centraal	centraal	centraal	decentraal	hercentralisatie	centraal en decentraal
Gebruikers	gebruikers nauwelijks betrokken; automatiseringsorganisatie bepaalt functionaliteit	enthousiasme van de gebruiker en enige betrokkenheid bij de ontwikkeling van systemen	gebruikersparticipatie tijdens de systeem-ontwikkeling	gebruikersorganisatie krijgt IT-budget	gebruikers bouwen systemen met enige ondersteuning van IT-deskundigen	gebruikersorganisatie (BU) is totaal verantwoordelijk voor de toepassing van informatietechnologie
Sturing m.b.t. de geautomatiseerde informatievoorziening	automatiseringsorganisatie beslist	automatiseringsorganisatie beslist samen met afdelingsmanagement	stuurgroep beslist	topmanagement besteedt aandacht; stuurgroep beslist	topmanagement beslist	topmanagement schept condities; BU-management beslist
Beheers-instrumentarium	geen planvorming; aandacht gericht op mogelijkheden	geen planvorming; introductie van SO-technieken	informatieplanning	gegevensgerichtheid	gedifferentieerde beheersmethoden	strategische besluitvorming

Leg voor de belangrijkste bedrijfsprocessen de mate van afhankelijkheid van de geautomatiseerde gegevensverwerking vast. De aldus ingeschatte afhankelijkheden kunnen in een later stadium van invloed blijken te zijn op de controle-aanpak.				
		Taxatie afhankelijkheidsgraad (L/G/H) met betrekking tot:		
Bedrijfs-proces	**Informatie-systeem**	**Betrouwbaar-heid**	**Beschikbaar-heid**	**Effectiviteit**

Figuur 5. Afhankelijkheidsanalyse.

De afhankelijkheidsanalyse

Met behulp van een afhankelijkheidsanalyse onderzoekt de accountant in samenspraak met het management van de onderneming in hoeverre de onderneming afhankelijk is van bepaalde systemen voor de sturing en beheersing van de bedrijfsuitoefening. In het kader van de controle van de jaarrekening manifesteert deze afhankelijkheid zich in een drietal aspecten:
- betrouwbaarheid;
- beschikbaarheid;
- effectiviteit.

Een voorbeeld:
Een informatiesysteem kan zeer betrouwbare informatie opleveren, maar als net die informatie ontbreekt die nodig is voor het nemen van beslissingen, is het systeem toch niet effectief. In die gevallen worden vaak allerlei persoonlijke toepassingen in een organisatie ontwikkeld, die wel de gevraagde informatie opleveren. Dit kan indicatief zijn voor een situatie waarin juist kritieke informatie wordt gegenereerd in een omgeving die niet of nauwelijks wordt beheerst door management control.

De afhankelijkheidsanalyse helpt de accountant inzicht te krijgen in de informatiesystemen die kritiek zijn voor de onderneming en voor zijn controlebenadering.

Kritieke IT-succesfactoren

De beoordeling van de kritieke IT-succesfactoren is een verdere verdieping van de beoordeling van informatiesystemen in de afhankelijkheidsanalyse. Het bepalen van de kritieke IT-succesfactoren sluit aan op de risico-analyse van de onderneming in algemene zin en behoort dus object van onderzoek te zijn van de accountant. Daarbij is de inspanning van de accountant erop gericht om, op basis van de ondernemingsdoelstellingen en de risico's (bedreigingen) dat die doelstellingen niet worden bereikt, de relevante IT-succesfactoren en stuurvariabelen te onderkennen.

Een eenvoudig voorbeeld:
Stel, een handelsbedrijf met veel leveranciers heeft als doelstelling het optimaal profiteren van betalingskortingen ('just-in-time'-betalingsstrategie).

Bij deze doelstelling zijn door de onderneming onder meer de volgende twee risico's onderkend:
- Bij de controle van de inkoopfacturen treedt te veel vertraging op.
- In het betalingsproces treedt te veel vertraging op.

Bij deze risico's zijn de volgende IT-stuurvariabelen te onderkennen:
- Het matchingsysteem van factuur met order en ontvangstbevestiging moet zodanig worden ondersteund door informatietechnologie, dat posten waarbij afwijkingen zijn gesignaleerd snel kunnen worden afgewerkt. Dit kan bijvoorbeeld door posten met geringe afwijkingen wel voor betaling te accepteren en achteraf verder te onderzoeken wat de oorzaak van de afwijking is geweest.
- In het geautomatiseerd betalingstraject moet zoveel mogelijk gebruik worden gemaakt van preventieve controles op belangrijke gegevens (rekeningnummer, betaaldatum), teneinde tijdrovende controles tussen moment van aanmaak van de betalingen en de uiteindelijke betaling zelf te beperken.

Het is dus van belang om voor bedrijfsdoelstellingen de kritieke IT-succesfactoren te onderkennen en voor de te onderkennen risico's de relevante IT-stuurvariabelen te definiëren. Deze analyse geeft de accountant niet alleen veel inzicht in de effectiviteit van informatietechnologie bij de ondersteuning van het bedrijfsproces, maar geeft hem ook een duidelijke indicatie over de mate waarin informatietechnologie binnen de onderneming is benut als instrument ter versterking van de interne controle op betrouwbare gegevensverwerking.
De analyse helpt de accountant zijn controle-inspanning te concentreren op de risicovolle processen en procedures.

PLANNING VAN DE CONTROLE

De planning van de controle is erop gericht vast te stellen hoe en door wie de controle verder zal worden uitgevoerd. Op grond van de werkzaamheden verricht in de strategiefase en initiële cijferanalyses komt de accountant tot een voorlopige vaststelling van de belangrijkste controledoelstellingen in het kader van de controle van de jaarrekening.

Figuur 6. Planning van de controle.

Uitvoeren cijferanalyses
Vaststellen belangrijke controledoelstellingen
Inzicht in interne controle
Vaststellen aanpak kritieke controledoelstellingen
Vaststellen controlemaatregelen
Samenwerking met andere externe accountants en specialisten
Vaststellen behoefte aan dienstverlening
Vaststellen vorm en tijdstip van rapporteren

In het kader van dit artikel wordt een belangrijke controledoelstelling gedefinieerd als een controledoelstelling waarbij het risico dat (cumulatief) een belangrijke fout onontdekt blijft, groot is. Dit risico wordt beïnvloed door een tweetal elementen.

Allereerst kan de omvang van een bepaalde transactiestroom of post in de jaarrekening zodanig zijn, dat deze door de onderneming geheel wordt beheerst met behulp van informatietechnologie. Zonder voldoende kennis en inzicht in het IT-systeem kan niet worden geconcludeerd dat de kans op een belangrijke fout in voldoende mate is beperkt. In dat kader merkte Boer [Boer94] reeds op dat door geïntegreerde informatietechnologie in toenemende mate kan worden volstaan met een gemeenschappelijke registratie die door verschillende bedrijfsfuncties wordt gebruikt. Het voeren van dubbele administraties is steeds minder noodzakelijk, omdat verschillende functies dezelfde gegevens beschikbaar hebben voor hun informatievoorziening. Hiermee verdwijnt in toenemende mate de basis voor controle door vergelijking van twee onafhankelijk van elkaar tot stand gekomen registraties. De oplossing is volgens Boer gelegen in het ontwerp van een doordacht stelsel van geprogrammeerde maatregelen in samenhang met de door verantwoordelijke functionarissen uit te voeren autorisatie-, controle- en correctietaken.

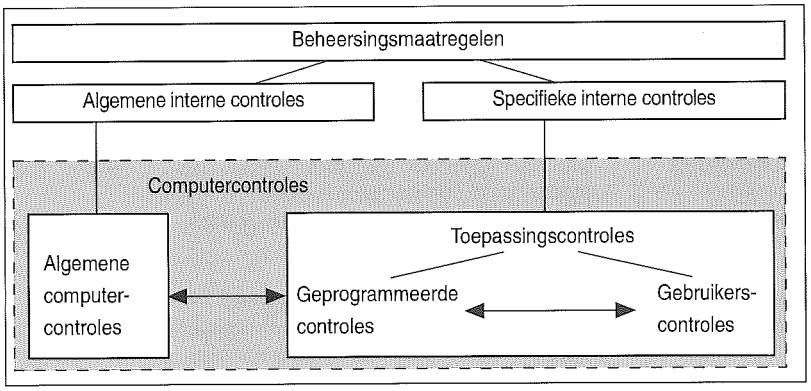
Daarnaast zijn er controledoelstellingen die als kritiek moeten worden aangemerkt, omdat
- voor de controle een belangrijke mate van vakkundig oordeel nodig is; of
- het verkrijgen van controlebewijs of het uitvoeren van controlemaatregelen moeilijk is.

In deze situaties is het risico op een belangrijke fout ook vergroot. Met name ingeval het verkrijgen van controlebewijs of het uitvoeren van controlemaatregelen moeilijk is, kan informatietechnologie daarbij een belangrijke rol spelen. Bijvoorbeeld wanneer het informatiesysteem zodanig complex is dat de uitkomsten niet meer kunnen worden vergeleken met de invoer en dus een samenstel van andere (computer)controles de betrouwbaarheid van de verwerking moet waarborgen.

Op grond van deze planningswerkzaamheden en de uitkomsten uit de strategiefase zal de accountant bepalen wat de kritieke IT-systemen zijn bij de onderneming en op welke wijze zekerheid kan worden verkregen omtrent de betrouwbaarheid van deze systemen.

De betrouwbaarheid van een IT-systeem wordt beheerst door computercontroles met een algemeen karakter (de general IT controls of algemene computercontroles; zie figuur 7) en computercontroles die zich richten op de betrouwbare werking van een specifieke applicatie (de application controls of toepassingscontroles).

De beoordeling van de opzet van de algemene computercontroles vindt veelal plaats met behulp van specifiek daartoe ontwikkelde vragenlijsten. De praktijk heeft uitgewezen dat als een accountant dergelijke beoordelingen een aantal malen samen met een EDP-auditor heeft verricht, hij in niet-



Figuur 7. IT-aspecten in de planningsfase.

complexe situaties die beoordeling zelf kan uitvoeren (zie figuur 8).

Beleid en management
Functiescheidingen
Logische toegangsbeveiliging
Fysieke toegangsbeveiliging
Systeemontwikkeling en onderhoudsprocedures
Continuïteit
Systeembeheer- en rekencentrumprocedures
Gebruikerssatisfactie

Figuur 8. Algemene computercontroles.

Ten behoeve van een goed inzicht in de meest effectieve toepassingscontroles is het noodzakelijk systemen nader te onderzoeken. Een dergelijk onderzoek moet aansluiten op de controlefilosofie en gericht zijn op de kwaliteit van de beheersing van risico's. Dit impliceert dat de methodiek inzicht moet geven in de mate waarin controles de onderkende risico's in de bedrijfsprocessen beheersen.
Bij de beoordeling van de effectiviteit van de beheersing van het bedrijfsproces wordt een matching gemaakt tussen de aangetroffen beheersingsmaatregelen en de risico's die de belangrijke bedrijfsdoelstellingen bedreigen. Deze matching beperkt zich niet tot de aangetroffen toepassingscontroles, maar is gericht op de selectie van de beheersingsmaatregelen die het meest effectief zijn in het beperken van de bedrijfsrisico's. De matching kan in de vorm van een matrix worden gepresenteerd (zie figuur 9).

De accountant zal door middel van systeemtests de goede werking van deze beheersingsmaatregelen moeten vaststellen ten behoeve van het verkrijgen van effectief controlebewijs.

Een systeembeoordelingsmethodiek die is gebaseerd op een risico-analyse biedt de mogelijkheid het onderzoek te beperken tot slechts die systeemfuncties die relevant zijn voor de beheersing van de risico's die de belangrijke controledoelstellingen in het kader van de controle van de jaarrekening bedreigen.

Bedrijfsdoelstelling	Verkoopleveringen uit voorraad binnen beperkte tijd.	
Risico's	**Beheersingsmaatregelen**	**Sterk/Zwak**
Inkooporder niet op tijd gecreëerd; fouten in voorraadniveau	Voorraadinventarisaties worden tweemaal per jaar uitgevoerd; verschillen worden aangepast in de voorraadadministratie. Partieel roulerende inventarisaties zouden beter zijn.	S/Z
Inkooporder niet geprint/verwerkt	Orders worden automatisch geprint en gecontroleerd door de Operations manager met het orderschema. Controle wordt niet uitgevoerd door onafhankelijke staffunctionaris.	S/Z
Inkooporder niet door leverancier ontvangen	Wekelijkse controle op openstaande orders. Leveranciers moeten order confirmeren.	S

Figuur 9. Matching van de risico's met de beheersingsmaatregelen.

VERKRIJGEN EFFECTIEF CONTROLEBEWIJS

Als het gaat om het verkrijgen van effectief controlebewijs ten aanzien van de werking van algemene computercontroles en toepassingscontroles zal de accountant de beschikking moeten hebben over voldoende kennis en ervaring.

Uitvoeren geplande controlemaatregelen (systeemtests, cijferanalyses en detailcontroles)

Vaststellen en analyseren controleverschillen
Uitvoeren controlemaatregelen m.b.t. voorwaardelijke verplichtingen, eventuele onwettige handelingen en transacties met verbonden partijen
Beoordelen gebeurtenissen na balansdatum
Bevestigingen van de ondernemingsleiding

Figuur 10. Verkrijgen effectief controlebewijs.

In mijn artikel in *Update on EDP & Accountancy* [Munc93] wordt, evenals in het artikel van Fijneman [Fijn93], nader ingegaan op de noodzakelijke controlewerkzaamheden in het geval dat aan algemene computercontroles, zoals toegangsbeveiliging, systeemontwikkelings-, test- en overdrachtsprocedures, controlezekerheid wordt ontleend.
Het testen van de toepassingscontroles wijkt in beginsel niet af van het testen van interne controles in het algemeen. Ten behoeve van bepaalde toepassingscontroles kan echter verregaande kennis van het systeem onontbeerlijk zijn en is inschakeling van een EDP-auditor een noodzaak.
In het kader van dit artikel wordt verder geen aandacht besteed aan het testen van computercontroles.

AFSLUITENDE BEOORDELING, EVALUATIE VAN CONTROLEBEVINDINGEN EN RAPPORTERING

De evaluatie van de bevindingen is erop gericht na te gaan of de computercontroles hebben gewerkt zoals bij de opzet van het controleprogramma in de planningsfase werd verondersteld. Indien afwijkingen zijn geconstateerd, moet worden nagegaan wat de reden is dat de computercontroles niet naar verwachting hebben gewerkt en afhankelijk van de verklaring moet worden vastgesteld welke compenserende controlewerkzaamheden noodzakelijk zijn.
Ofschoon de evaluatie van de controlebevindingen ten aanzien van de werking van de computercontroles niet wezenlijk afwijkt van de gewone systeemtests is het belangrijk dat de accountant en de EDP-auditor op dit punt nauw samenwerken. Juist door inbreng van beide vakgebieden is het mogelijk de consequenties van geconstateerde tekortkomingen goed te kunnen inschatten en gezamenlijk al dan niet aanvullende acties te definiëren.
Ook de concept-richtlijn, welke is opgesteld in overleg met de platformcommissie NIVRA-NOREA [NIVR95] en handelt over de samenwerking tussen accountant en EDP-auditor ter zake van de controle van een verantwoording, geeft hier expliciet aandacht aan.

Beoordelen controledossiers
Evalueren controleverschillen
Cijferbeoordeling jaarstukken en beoordeling op presentatie en continuïteit
Beoordelen of deugdelijke grondslag aanwezig is
Formuleren accountantsoordeel
Rapportering

Figuur 11. Afsluitende beoordeling, evaluatie controlebevindingen en rapportering.

In deze concept-richtlijn wordt eveneens aangegeven dat het bij samenwerking van groot belang is dat vooraf expliciete afspraken worden gemaakt over de documentatie en overige informatie die na afloop van het onderzoek voor de accountant beschikbaar moeten zijn, alsmede over de wijze waarop rapportering door de EDP-auditor aan de accountant of rechtstreeks aan de cliënt moet plaatsvinden. Het verdient aanbeveling de afspraken inzake rapportering ook met de cliënt af te stemmen, teneinde misverstanden of valse verwachtingen te voorkomen.

SLOTEVALUATIE

Tijdens de slotevaluatie worden de controle-aanpak en de dienstverlening aan de cliënt geëvalueerd, met het doel te komen tot verbetering.

Vaststellen van de aanpak om onze dienstverlening te verbeteren
In acht te nemen punten bij controle volgend jaar

Figuur 12. Slotevaluatie.

Met betrekking tot de integratie van informatietechnologie in de controle-aanpak richt de evaluatie zich op de volgende aspecten:

- Planning:
  - waren de gemaakte afspraken helder en adequaat;
  - moeten planningsafspraken worden bijgesteld?
- Kwaliteit van het afgeleverde werk:
  - heeft het team bereikt wat het zichzelf in de strategiefase tot doel heeft gesteld;
  - welke goede aspecten van het werk moeten volgend jaar worden herhaald of uitgebreid;
  - welke minder goede aspecten moeten volgend jaar worden verbeterd;
  - werden teamleden voldoende getraind en gecoached bij het uitvoeren van de IT-werkzaamheden?
- Tijd en geld:
  - was het werk op tijd gereed;
  - zijn de werkzaamheden verricht binnen het daarvoor gestelde budget of heeft tijdig budgetbijstelling plaatsgevonden?
- Toekomstige ontwikkelingen:
  - zijn toekomstige ontwikkelingen en IT-opportunities in voldoende mate onderkend en gecommuniceerd naar de cliënt?
- Actieplan:
  - ligt er een nieuw actieplan voor volgend jaar;
  - is het voldoende duidelijk wie verantwoordelijk is voor de te nemen acties en wanneer die acties staan gepland?

Wanneer er een EDP-auditor ingeschakeld is geweest, is het uiteraard van belang deze punten gezamenlijk te evalueren in het licht van de samenwerking tussen de accountant en de EDP-auditor. Daarbij moet specifiek aandacht worden geschonken aan de kwaliteit van de communicatie tussen accountant en EDP-auditor.

CONCLUSIE

Zoals aan het begin van dit artikel is gesteld, speelt informatietechnologie bij het besturen van ondernemingen en bij beheersen van risico's in de bedrijfsuitoefening steeds meer een belangrijke rol. In het kader van de controle van de jaarrekening is beoordeling van de wijze waarop het management van een onderneming de risico's met betrekking tot informatietechnologie beheerst dan ook van groot belang.
De onderneming maakt in toenemende mate gebruik van informatietechnologie om het bedrijfsproces te sturen of zelfs te innoveren en risico's te beheersen. De verwachting is derhalve dat de accountant bij zijn controle in belangrijke mate aandacht schenkt aan de IT-systemen. Alleen door aan die verwachting tegemoet te komen zal de accountant in staat zijn om als kritisch klankbord voor de ondernemingsleiding te functioneren.

Ofschoon vanuit de opdracht tot controle van de jaarrekening de aandacht primair zal zijn gericht op de betrouwbaarheid en beschikbaarheid (continuïteit) van informatietechnologie, verdient het aanbeveling ook aandacht te schenken aan de effectiviteit van IT-systemen. Zoals Moonen [Moon95] heeft gesteld in zijn lezing in het kader van het jubileumsymposium van de Vereniging van EDP Auditing van de Katholieke Universiteit Brabant, heeft het management te maken met in de ogen van zijn leden veel belangrijker problemen en beslissingsvraagstukken op het gebied van informatietechnologie dan de betrouwbaarheids- en continuïteitsproblematiek. De samenwerking tussen de accountant en de EDP-auditor moet erop zijn gericht beter aansluiting te vinden op de wensen van de cliënt. Eerst dan zal de serviceverlening daadwerkelijk verbeteren en zullen nieuwe mogelijkheden voor dienstverlening worden onderkend.
Samenwerking tussen accountant en EDP-auditor wordt dan ook aanbevolen en bij complexe informatietechnologie veelal noodzakelijk geacht. In het kader van de controle van de jaarrekening is het niet meer rationeel de inzet van een EDP-auditor als (budgettair) additioneel te beschouwen. De EDP-auditor moet opereren als gewoon lid van het controleteam en de werkzaamheden die hij moet verrichten in het kader van de controle van de jaarrekening moeten binnen het controlebudget vallen. Alleen dan zal een optimale bezetting van het team kunnen worden gerealiseerd.

Er kan nog zoveel worden geschreven en geregeld over de samenwerking tussen beide beroepsgroepen, het kan pas echt gaan werken als beide groepen tot een dialoog komen. Het doel van een dialoog is volgens Bohm [Bohm65] om verder te komen en meer te begrijpen dan een persoon alleen kan. 'In een dialoog proberen we niet te winnen. We winnen daar allemaal als het goed is. Dialoog brengt het gebrek aan samenhang in ons denken aan het licht. In een dialoog verkrijgen mensen inzichten waartoe ze alleen eenvoudig niet hadden kunnen komen.'

Mw. W.A. de Munck RA
Is werkzaam als senior manager bij KPMG EDP Auditors en richt haar aandacht voornamelijk op EDP-auditwerkzaamheden in het kader van de controle van de jaarrekening. Zij is mede verantwoordelijk voor het ontwikkelen van methoden, produkten en trainingen die bijdragen tot het verbeteren van de samenwerking tussen accountants en EDP-auditors ten behoeve van de jaarrekeningcontrole.

LITERATUUR

[Fijn93] R.G.A. Fijneman RE RA, *Ontwikkelingen in accountantscontrole in een geautomatiseerde omgeving*, Compact 1993/4.

[Donk95] Ir. J.A.M. Donkers, M. Groesz RE en ir. J.A. Verstelle RE, *Informatietechnologie; Management control van de geautomatiseerde informatievoorziening*, Kluwer-serie Controlling in de praktijk, 1995.

[Boer94] J.C. Boer RE RA, *De invloed van informatietechnologie op de interne-controleprincipes*, Compact 1994/4.

[Munc93] W.A. de Munck RA, *De invloed van automatisering op de accountantscontrole*, in: Update on EDP & Accountancy, VERA studiereeks nr. 3, 1993.

[NIVR95] NIVRA, *Samenwerking tussen accountant en EDP-auditor ter zake van de controle van een verantwoording*, concept-richtlijn 622, 1995.

[Moon95] Prof. H.B. Moonen RE RA, *Veranderingen in de praktijk van EDP Auditing vanuit het perspectief van de EDP-auditor*, lezing in het kader van het jubileumsymposium van de Vereniging van EDP Auditing van de Katholieke Universiteit Brabant, 1995.

[Bohm65] Uitspraken van D. Bohm door P.M. Senge geciteerd in zijn boek *The Fifth Discipline*, 1990.

Plaats en taken van de EDP-auditfunctie bij de KLM

J.G. de Vries RE RA

Door de toepassing van nieuwe automatiseringstechnieken nemen de mogelijkheden van controle in de gebruikersorganisatie af. De controlebenadering van de financial audit zal hieraan moeten worden aangepast.
Voor de EDP-auditfunctie betekent dit dat naast beoordeling van opzet en bestaan, ook de werking van maatregelen en procedures moet worden getoetst.

INLEIDING

Binnen veel ondernemingen heeft een herbezinning op de interne accountantsfunctie plaatsgevonden. Voor veel interne accountantsdiensten heeft dit geleid tot een gewijzigd takenpakket. De operational auditfunctie heeft bij een groot aantal ondernemingen vorm gekregen, meestal gepaard gaande met een andere invulling van de financial auditfunctie. Ook binnen de KLM heeft een dergelijk proces plaatsgevonden, waarbij, mede als gevolg van wijzigingen in toepassing van informatietechnologie (down-sizing, client/server-modellen, EDI), ook de plaats en taken van de EDP-auditfunctie zijn betrokken.

In dit artikel wordt een schets gegeven van hoe EDP-audit is gepositioneerd na de introductie van de operational auditfunctie binnen de KLM.
Hiertoe zal eerst worden beschreven wat onder operational, financial en EDP-audit wordt verstaan, waarna wordt ingegaan op waarom en voor wie EDP-audit in een organisatie wordt uitgevoerd en wat er met betrekking tot beheer wordt verwacht van de IT-organisatie. Verder wordt aangegeven wie wat zal gaan doen ten aanzien van EDP-audit en welke deskundigheden en vaardigheden daarvoor nodig zijn.

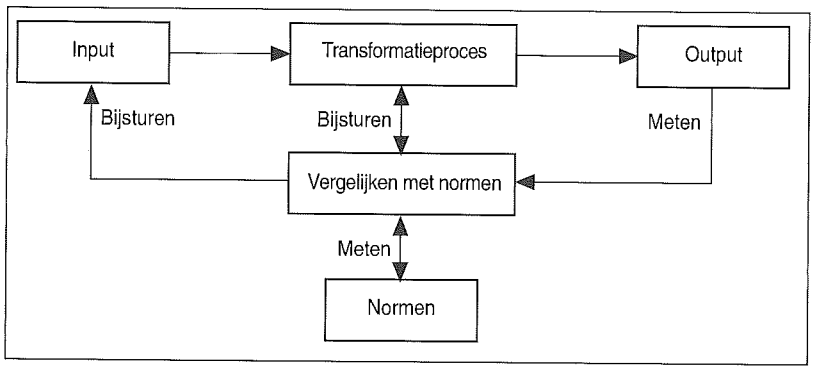
BEGRIPSBEPALINGEN

Operational audit

Operational audit wordt binnen de KLM omschreven als een onafhankelijk onderzoek van een deel van de organisatie, gericht op de beoordeling van de kwaliteit van de informatieverzorging ten behoeve van de besturing en beheersing van de processen van de KLM.

Onder kwaliteit wordt in dit verband verstaan:
- de effectiviteit en betrouwbaarheid van de informatie;
- de efficiëntie van de informatieverzorgende processen;
- de maatregelen ter beveiliging van activa, informatie, informatiesystemen en dergelijke;
- de naleving van in het kader van eenheid van beleid gedefinieerde regels;
- de doelmatigheid van de aanwending van middelen.

Onder kwaliteit wordt in dit verband dus niet alleen betrouwbaarheid verstaan, maar ook zeer nadrukkelijk de efficiency en effectiviteit.
Bij de uitvoering van de onderzoeken probeert operational audit vast te stellen of er sprake is van een regelkring, waarbij de continu goede werking van processen voortdurend wordt vastgesteld door uitkomsten te meten en te vergelijken met vooraf vastgestelde normen (zie figuur 1).



Figuur 1. Regelkring.

Financial audit

Financial audit wordt omschreven als het geheel aan controletaken dat dient ter verkrijging van een deugdelijke grondslag voor het afgeven van een verklaring bij de jaarrekening van de KLM.

Tot de herbezinning werd door de interne accountant nog een volledige controle van de interne jaarrekening uitgevoerd, leidende tot een verklaring bij die interne jaarrekening. De nieuwe taakopvatting betekende het einde van deze vorm van interne accountancy. Thans wordt nog slechts een deel van de financiële verantwoording door de interne accountant gecontroleerd. Aangezien het de wettelijk bepaalde taak van de externe accountant is om de te publiceren (geconsolideerde) jaarrekening van de KLM te certificeren, geschieden de door de interne accountant uit te voeren werkzaamheden op het gebied van financial audit dan ook onder de uiteindelijke verantwoordelijkheid van de externe accountant.

EDP-audit

EDP-audit wordt omschreven als het vakgebied dat zich bezighoudt met het beoordelen van en het adviseren over één of meer kwaliteitsaspecten van (onderdelen van) de informatievoorziening in een omgeving waar gebruik wordt gemaakt van informatietechnologie.

Momenteel wordt intern bestudeerd op welke wijze door de interne-auditfunctie invulling kan worden gegeven aan het 'Internal Control - Integrated Framework' van het 'Committee of Sponsoring Organizations of the Treadway Commission' (het COSO-rapport), waarin een ruime inhoud aan het begrip internal control wordt gegeven.
In de Verenigde Staten is het beursgenoteerde financiële instellingen (vooralsnog alleen binnenlandse) reeds verplicht gesteld om te voldoen aan de richtlijnen van het COSO-rapport. Hiertoe moet in het jaarverslag een management report worden opgenomen over opzet, bestaan en werking van de internal control zoals die in de onderneming functioneert.

WAAROM EN VOOR WIE EDP-AUDIT

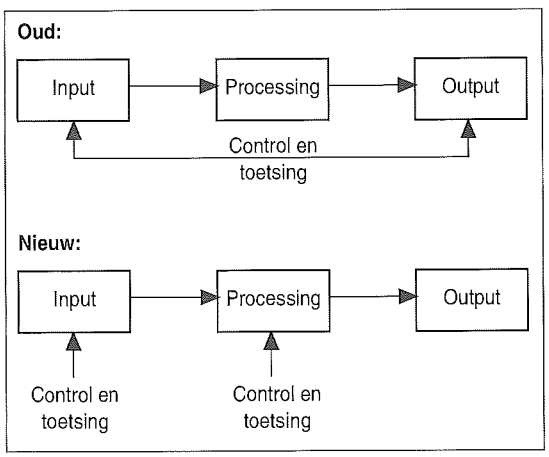
De toepassing van informatietechnologie binnen de KLM is wijdverspreid. De beheersing van nagenoeg alle binnen de KLM te onderkennen processen wordt geheel of gedeeltelijk ondersteund met geautomatiseerde systemen. Onder de te onderkennen processen worden in dit verband ook de verzorging van in- en extern gerichte financiële rapportages begrepen.

Binnen de KLM worden taken en verantwoordelijkheden steeds meer gedecentraliseerd. Bovendien wordt, ten behoeve van de vergroting van de flexibiliteit, op grote schaal gebruik gemaakt van de mogelijkheden tot down-sizing. Er is sprake van complexe vormen van automatisering, waarbij de relatie tussen ingevoerde gegevens en de door de systemen opgeleverde informatie niet langer zonder meer zichtbaar is. De verwerking van gegevens vindt plaats op diverse aaneengeschakelde platformen, waarbij steeds meer controletaken van de gebruikersorganisatie verschuiven naar applicatie- en systeemsoftware. De introductie van EDI maakt bovendien dat brondocumenten nog slechts in elektronische vorm beschikbaar zijn. Hierdoor wordt zowel het lijnmanagement (ten behoeve van de procesbeheersing) als het financiële management (voor managementinformatie en de financiële verslaglegging) afhankelijk van de maatregelen en procedures (de general controls) in de

automatiseringsorganisaties die de diverse platformen en systemen beheren. Deze general controls dienen bij wijze van spreken als paraplu voor de beheermaatregelen in de gebruikersorganisatie en in de applicaties (de application controls).

De reeds genoemde down-sizing betekent daarbij dat in plaats van met één paraplu, rekening moet worden gehouden met een samenstel van een aantal paraplu's en hun onderlinge samenhang. Bovendien neemt de complexiteit van de communicatie- en verwerkingsstructuren verder toe, waarbij ook controletaken worden geëffectueerd in de toegepaste netwerken en het netwerkbeheer.

Voor de KLM betekent dit dat geleidelijk wordt overgegaan op een hieraan aangepast beheerconcept. In het 'oude' beheerconcept ligt de nadruk traditioneel op controlemaatregelen achteraf in de gebruikersorganisatie. Gezien de gesignaleerde verschuiving van controlemaatregelen en de toenemende decentralisatie van de automatisering is een dergelijk beheerconcept niet langer effectief en efficiënt. De beheersing wordt meer en meer gezocht in het beheersen van de automatisering, waarbij de in de automatiseringsorganisatie getroffen paraplumaatregelen een betrouwbare verwerking van gecontroleerde input moeten waarborgen (zie figuur 2). De continue en juiste werking van deze paraplumaatregelen is dus voorwaarde om tot een effectiever en efficiënter beheerconcept te komen, waarbij zoveel mogelijk gebruik wordt gemaakt van geautomatiseerde controles.



Figuur 2. Oud en nieuw beheerconcept.

EDP-audit geeft ten behoeve van zowel het lijnmanagement als het financieel/economisch management (controllers en administratie) zekerheid omtrent de kwaliteit van deze paraplu. Op die wijze draagt EDP-audit bij aan het benodigde comfort level ten aanzien van de betrouwbaarheid van de geautomatiseerde gegevensverwerking dat een gewijzigd beheerconcept vereist.

Waar de procesbeheersing en de financiële administratie in toenemende mate afhankelijk zijn van de kwaliteit van de automatisering, is dit uiteraard ook het geval bij operational audit en financial audit, die de procesbeheersing en financiële verantwoordingen dienen te toetsen. Voor de financial audit betekent dit dat als gevolg van het wegvallen van controles in de gebruikersorganisatie, moet worden overgegaan op een systeemgerichte controlebenadering *met automatisering*. Dat wil zeggen dat voor de oordeelsvorming gebruik moet worden gemaakt van maatregelen en procedures in de automatiseringsorganisatie.

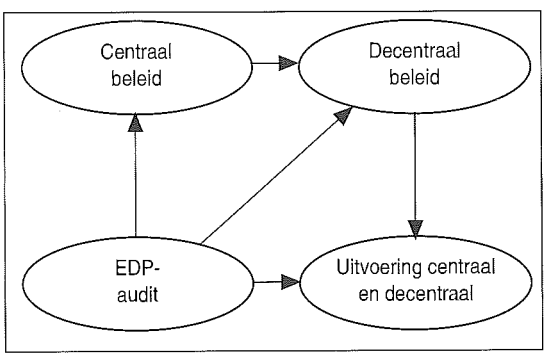
Dit maakt EDP-audit ten behoeve van de oordeelsvorming van financial en operational audit noodzakelijk.

Bovendien geldt een aantal wettelijke bepalingen zoals de Wet persoonsregistraties en de Wet computercriminaliteit, die een EDP-auditfunctie wenselijk maken.

WERKWIJZE EDP-AUDIT

EDP-audits richten zich in eerste aanleg op de opzet en het bestaan van maatregelen en procedures. Uitgegaan wordt van een Management Control Oriented Audit Approach, zoals die in de postdoctorale EDP-auditopleiding aan de Erasmus Universiteit wordt gedoceerd. Voor de gevolgde werkwijze betekent dit dat audits top-down worden gestructureerd, gericht op beleid en beheersing door het verantwoordelijk management. De uitvoering (werking) wordt slechts steekproefsgewijs in de audit betrokken teneinde het bestaan van maatregelen te verifiëren.

Gelijk operational audit doet, probeert ook EDP-audit te zoeken naar een regelkring. Ten behoeve van een doeltreffende, doelmatige en betrouwbare inzet van informatietechnologie, zowel centraal als decentraal, is een beheerstructuur noodzakelijk. Hierbinnen worden de normen gevonden die een effectieve en efficiënte EDP-audit mogelijk maken. Een dergelijke beheerstructuur dient in eerste aanleg te worden gevonden in de eenheid van beleid op het gebied van informatietechnologie zoals dat door het centrale en decentrale informatiemanagement moet worden vormgegeven(zie figuur 3).



Figuur 3. EDP-audit en eenheid van beleid.

De beheerstructuur dient daartoe minimaal te omvatten:
- IT-beleid;
- verantwoordelijkheidsstructuur;
- rapportage- en controlestructuur;
- richtlijnen ten aanzien van hardware;
- richtlijnen ten aanzien van systeemontwikkeling;
- richtlijnen ten aanzien van beveiliging;
- richtlijnen ten aanzien van communicatie.

Het object van onderzoek van EDP-audit wordt in drie functionele gebieden verdeeld:
- gebruikersorganisatie (GO), waarbij naar maatregelen en procedures in de gebruikersorganisatie wordt gekeken;
- systeemontwikkelingsorganisatie (SO), gericht op de beheersing van het systeemontwikkelingstraject;
- verwerkings- en transportorganisatie (VTO), waarbij de aandacht is gericht op maatregelen en procedures in het rekencentrum.

Met betrekking tot de te toetsen kwaliteitscriteria (betrouwbaarheid, effectiviteit en efficiency) wordt een viertal kwaliteitsdragers onderscheiden, namelijk:
- een proces, waarbij de wijze waarop ergens uitvoering aan wordt gegeven (bijvoorbeeld de wijze waarop een systeem wordt ontwikkeld), wordt getoetst;
- de structuur, waarbij de organisatiestructuur die een proces ondersteunt, wordt beoordeeld;
- de middelen, waarbij de in een proces gebruikte gereedschappen (bijvoorbeeld een bij de ontwikkeling gebruikt CASE-tool) worden beoordeeld;
- het produkt, waarbij het eindprodukt van een proces (bijvoorbeeld een ontwikkelde applicatie) wordt beoordeeld.

Er worden twee niveaus van EDP-audit onderscheiden:

Algemeen
Hieronder vallen systeembeoordelingen in de GO in het kader van een operational of financial audit met betrekking tot geautomatiseerde ondersteuning van het te onderzoeken proces. De onderzoeken beperken zich veelal tot de kwaliteitsaspecten exclusiviteit, integriteit en controleerbaarheid en kennen geen technische diepgang. Algemene EDP-audits worden uitgevoerd indien dat in het kader van een operational of financial audit noodzakelijk is, of op verzoek. Het betreft voornamelijk beoordelingen van operationele systemen. Audits op verzoek kunnen ook (en wel bij voorkeur) betrekking hebben op systemen in ontwikkeling.

Specifiek
Hieronder vallen meer complexe systeembeoordelingen in de GO en alle onderzoeken naar SO en VTO. De beoordelingen kennen meer technische diepgang en betreffen alle kwaliteitsaspecten. De auditobjecten omvatten alle objecten die de 'paraplu van beheermaatregelen' beïnvloeden. Hieronder vallen de overall beheerstructuur en de structuur en het proces binnen de SO en de VTO voor alle voorkomende automatiseringsorganisaties. De toegepaste produkten en middelen (hardware, systeemsoftware, datacommunicatiemiddelen, netwerkvoorzieningen) en de technische implementatie daarvan worden slechts in de audit betrokken indien noodzakelijk in het kader van een onderzoek.

Zoals de definitie aangeeft betreft EDP-audit zowel toetsing als advisering. De hoofdtaak is de toetsende rol. Advisering vindt plaats ten behoeve van het opheffen van geconstateerde tekortkomingen die bij de toetsing aan het licht zijn gekomen.

WIE DOET WAT

Grenzen tussen OA/FA en EDP-audit

Gezien de in gang gezette wijziging van het beheerconcept en de noodzaak om de audit daaraan aan te passen, dient de verantwoordelijke financial of operational auditor zich een beeld te vormen omtrent de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking. Hiertoe dienen onder meer de volgende punten in kaart te worden gebracht:
- beleid inzake de automatisering van de processen of de aansturing van de processen;
- afhankelijkheid van de automatisering;
- soorten en omvang van risico's voortvloeiend uit de geautomatiseerde component van het proces;
- betrokken functies en noodzakelijke functiescheidingen;
- automatiseringsomgeving:
  - centraal;
  - decentraal (mini, PC-netwerk, stand-alone PC);
- ondersteunende organisatie;
- aansturing van buiten het systeem, zoals:
  - interfaces;
  - datacommunicatie;
  - EDI.

De inventarisatie wordt in eerste instantie door een auditor uit de algemene praktijk (financial of operational audit) uitgevoerd. Bevindingen op bovenstaande aandachtspunten worden met een EDP-auditor doorgenomen. In samenspraak met de EDP-auditor wordt vervolgens bezien welke interne-controlemaatregelen moeten zijn genomen om mogelijke risico's af te dekken.

Aangezien de werkwijze van operational audit nauw aansluit bij de werkwijze van EDP-audit, is de EDP-auditfunctie binnen operational audit gepositioneerd.
Omdat financial audit de garantie moet hebben dat de voor haar noodzakelijke onderzoeken in voldoende mate worden uitgevoerd, worden onderling heldere afspraken ten aanzien van de uit te voeren werkzaamheden gemaakt.

Intern versus extern

Gezien het belang van de onder de paraplu vallende objecten, dient de algemene EDP-audit volledig intern te kunnen worden afgedekt. De onderzoeken worden zoveel mogelijk door de financial en operational auditor meegenomen bij de uitvoering van zijn/haar onderzoeken. Specifieke EDP-audits, veelal in de SO- en VTO-omgeving, behoeven een specialist EDP-auditor. Deze biedt ook ondersteuning aan de financial en operational auditor bij hun onderzoeken.

Het opbouwen en onderhouden van vooral technische kennis ten behoeve van beoordeling van produkten en middelen in de SO- en VTO-omgeving is slechts met grote moeite en tegen hoge kosten te doen, terwijl het aantal uit te voeren onderzoeken relatief gering is. Indien noodzakelijk worden hiervoor externen ingeschakeld. Een uitzondering vormen de gebruikte access control software en bij de systeemontwikkeling toegepaste hulpmiddelen, aangezien deze een belangrijk onderdeel uitmaken van de 'paraplu'.

Onderzoeken gericht op de beoordeling van de effectiviteit en/of efficiëntie dienen zoveel mogelijk door de interne functie te worden uitgevoerd, met dien verstande dat geen diepgaande *technische* onderzoeken zullen worden uitgevoerd. Dit betekent dat met name het onderzoek naar de efficiency van de VTO alleen met inschakeling van externe deskundigen kan worden gedaan.

BENODIGDE KENNIS EN VAARDIGHEDEN

Kennisniveau

De gekozen uitgangspunten stellen eisen aan het kennisniveau van zowel de EDP-auditor als de financial en operational auditor.

Financial en operational auditor
Zowel binnen financial audit als operational audit moet brede algemene kennis (HBO+-niveau) aanwezig zijn op het gebied van:
- auditing;
- administratieve organisatie;
- procesbeheersing;
- algemene kennis met betrekking tot automatisering en interne controle (ruime zin);
- specifieke kennis betreffende de auditspecialiteit (administratie, logistiek, quality management, etc.).

EDP-auditor
Binnen EDP-audit moet brede algemene kennis (HBO+-niveau) aanwezig zijn op de voornoemde algemene-auditgebieden, aangevuld met specifieke kennis van informatietechnologie, te weten:
- organisatie van de automatisering;
- systeemprogrammatuur;
- applicatieprogrammatuur;
- database-management;
- datacommunicatie;
- beveiliging van programmatuur en data, zowel fysiek als logisch;
- ontwikkelingsorganisatie.

Bovengenoemde kennisgebieden dienen voor alle binnen de KLM van toepassing zijnde hardwareplatformen en automatiseringsorganisaties te zijn afgedekt.
De hierbij aansluitende opleidingseis voor EDP-auditmedewerkers ligt op het niveau van AMBI (inclusief EDP-auditingmodule) of post-doctoraal EDP-auditing.

CONCLUSIE

De toepassing van nieuwe automatiseringstechnieken leidt ertoe dat de mogelijkheden tot controle in de gebruikersorganisatie afnemen. Dit maakt aanpassing van traditionele beheerconcepten noodzakelijk. Moderne beheerconcepten steunen meer op de beheermaatregelen in de automatiseringsorganisatie dan traditioneel het geval is.

De controlebenadering van met name de financial audit zal hieraan moeten worden aangepast. Traditionele gegevensgerichte en systeemgerichte controlebenaderingen zijn niet meer toereikend. Er zal moeten worden uitgegaan van een systeemgerichte controlebenadering met automatisering, waarbij ten behoeve van de oordeelsvorming wordt gesteund op de goede werking van maatregelen en procedures in de automatiseringsorganisatie.

Hoewel de EDP-audits zich nu nog beperken tot opzet en bestaan, is het ten behoeve van de oordeelsvorming dus noodzakelijk te komen tot beoordeling van de juiste werking van de beoordeelde maatregelen en procedures. In overleg met de externe EDP-auditor wordt thans gezocht naar de beste manier om dit binnen de huidige uitgangspunten in de werkmethoden te incorporeren.

J.G. de Vries RE RA
Is als EDP-auditor werkzaam binnen de operational audit afdeling van het Bureau Interne Accountant van de Koninklijke Luchtvaart Maatschappij NV en is als universitair docent betrokken bij de post-doctorale EDP-auditingopleiding van de Erasmus Universiteit Rotterdam.
Hij is lid (geweest) van diverse commissies en werkgroepen in NIVRA-verband en heeft een ruime ervaring op het vakgebied.

Wet op het consumentenkrediet: systeemgericht onderzoek vereist

R. van den Hoorn RA

Het jaarlijks onderzoek van de huisaccountant dat in het kader van de WCK plaatsvindt bij instellingen die consumentenkrediet verstrekken, dient erop gericht te zijn te controleren dat het administratieve systeem erin voorziet dat de relevante bepalingen uit de wet worden nageleefd. Dit houdt in een geautomatiseerde omgeving in dat een onderzoek moet plaatsvinden naar de algemene computercontroles en de specifieke toepassingscontroles. Deze onderzoeken hebben voor het eerst plaatsgevonden over 1993. Vanuit zijn ervaringen geeft Van den Hoorn aan hoe een dergelijk onderzoek het best kan worden aangepakt.

INLEIDING

(Financiële) instellingen die consumptieve kredieten verstrekken vallen onder de bepalingen van de Wet op het consumentenkrediet. In deze wet is een jaarlijks onderzoek door de accountant naar de toepassing van de wet voorgeschreven.

Dit artikel beschrijft het onderzoek door de accountant in het kader van de Wet op het consumentenkrediet. Bij dit onderzoek wordt door de wetgever impliciet een systeemgerichte aanpak voorgeschreven naar de opzet en het bestaan van de relevante bepalingen uit deze wet. Omdat bij deze ondernemingen veelal gebruik wordt gemaakt van geautomatiseerde informatiesystemen spitst dit artikel zich toe op de aanpak in een geautomatiseerde omgeving.

Achtereenvolgens wordt in dit artikel ingegaan op de inhoud van de wet, het onderzoek door de accountant en de aanpak van het onderzoek in het kader van de Wet op het consumentenkrediet.

WET OP HET CONSUMENTENKREDIET (WCK)

Met ingang van 1 januari 1992 is de Wet op het consumentenkrediet (WCK) (Stb. 1990, 395) in werking getreden. Deze wet is van toepassing voor kredietttransacties (geldkrediet en goederenkrediet) waaraan de kredietgever en, in voorkomend geval, de leverancier deelnemen in de uitoefening van een bedrijf of beroep en waarbij de kredietnemer een *natuurlijk persoon* is. Niet onder deze wet vallen kredietttransacties waarbij de kredietsom meer dan vijftigduizend gulden bedraagt.

Het toezicht op de naleving van de wet wordt in opdracht van Economische Zaken uitgevoerd door een externe accountant, in het vervolg de EZ-accountant genoemd. Deze is belast met het toezicht of de vergunninghouders als een goed kredietgever opereren.

Daarnaast geeft ingevolge artikel 25 van de WCK iedere vergunninghouder jaarlijks opdracht aan een onafhankelijke accountant (de zogeheten *'huisaccountant'*) tot het verrichten van onderzoek ten behoeve van het toezicht op de naleving van de relevante bepalingen van de wet. Hierbij gaat het om de toetsing van die delen van de wet die betrekking hebben op het kredietvergoedingspercentage, de looptijd, de provisie en de kredietvergoeding. Bij dit onderzoek wordt aangesloten bij het boekjaar van de vergunninghouder.
Dit onderzoek heeft voor het eerst over 1993 plaatsgevonden en dient jaarlijks plaats te vinden.

Onderzoek uit te voeren door de huisaccountant

Als hulpmiddel voor de uitvoering van het onderzoek beschikt de accountant over het 'Handboek onderzoek huisaccountant'. Dit handboek is als bijlage opgenomen bij de Regeling toezicht WCK en aan de vergunninghouders ter beschikking gesteld. Dit handboek bestaat uit zes hoofdstukken en een toelichting. In hoofdstuk 2 'Algemene bepalingen' valt te lezen dat het onderzoek van de huisaccountant uit twee delen bestaat.

'Het onderzoek van de huisaccountant omvat de volgende twee onderdelen.

a. Verzamelen van algemene gegevens (hoofdstuk 4 van dit handboek)

Bij de aanvang van zijn werkzaamheden verzamelt de huisaccountant gegevens, zowel ten behoeve van zijn onderzoek als ten behoeve van het onderzoek van de EZ-accountants.

b. Verzameling van gegevens inzake naleving voorschriften (hoofdstuk 5 van dit handboek)

Dit deel heeft betrekking op de bedrijfsvoering van de vergunninghouder, bezien in het licht van de voor het onderzoek van de huisaccountant relevante onderdelen van de wet en de daarop gebaseerde uitvoeringswetgeving. In concreto gaat het om de regels inzake de berekening van het effectief kredietvergoedingspercentage op jaarbasis en van de theoretische looptijd, alsmede de voorschriften inzake de provisie en de kredietvergoeding.'

Onderdeel a kan grotendeels door de vergunninghouder worden voorbereid. In dit artikel wordt nader ingegaan op onderdeel b.

In hoofdstuk 5 is een vragenlijst opgenomen welke zodanig is opgesteld dat op systematische wijze de relevante bepalingen van de wet worden nagelopen.

In hoofdstuk 6 ten slotte wordt de wijze van rapporteren behandeld.

Vragenlijst

Het vaktechnisch belangrijkste deel van het onderzoek bestaat uit de werkzaamheden ten behoeve van de invulling van de vragenlijst. Deze vragenlijst kent drie onderwerpen, te weten vragen over het effectief kredietvergoedingspercentage en de theoretische looptijd, vragen over de provisie die betaald wordt aan tussenpersonen en vragen over de berekende kredietvergoeding.

Het doel van het onderzoek is na te gaan of de vergunninghouder (bepaalde delen van) de wet naleeft. Bij het toetsen van de naleving van de wet komt al gauw de vraag op of de (accountantsbegrippen) opzet, bestaan en/of werking van de administratieve organisatie en procedures moeten worden beoordeeld. De toelichting verwoordt het onderzoek als volgt: 'Aanknopingspunt bij deze vragen is de wijze waarop de regeling (...) in de administratieve systemen van de vergunninghouder is verwerkt. Met andere woorden: of de programmatuur zodanig is dat deze ten gevolge heeft dat op een juiste wijze de theoretische looptijd en het effectief kredietvergoedingspercentage worden berekend'. Bij de toelichting op het onderdeel kredietvergoeding staat uitdrukkelijk vermeld dat de vragen uit de vragenlijst *niet* dienen te worden beantwoord aan de hand van individuele kredietdossiers. Tevens beginnen alle vragen in dit gedeelte van de vragenlijst met 'Is er in voorzien dat ...'.

Uit deze toelichting en deze wijze van formuleren kan worden afgeleid dat het niet om de doorlopende toetsing van de naleving van de wet gaat (de 'werking'), maar dat de accountant zijn onderzoek richt op de *opzet* en het *bestaan* van dat gedeelte van de administratieve organisatie dat ervoor moet zorgen dat de relevante delen van de wet worden nageleefd. Uit het feit dat het uitdrukkelijk niet de bedoeling is dat het onderzoek wordt uitgevoerd aan de hand van de individuele kredietdossiers, maar dat het onderzoek zich dient te richten op de wijze waarop de regeling in de systemen is verwerkt, kan worden afgeleid dat een *systeemgericht* onderzoek noodzakelijk is. Door slechts de uitkomsten te beoordelen kan de accountant niet de wijze waarop de regeling in de systemen is verwerkt, vaststellen.

Het onderzoek dient derhalve door middel van

een systeemgerichte aanpak vast te stellen dat de relevante bepalingen van de WCK in opzet in het systeem aanwezig zijn en bestaan.

SYSTEEMGERICHTE CONTROLE IN HET KADER VAN DE WCK

Aanpak van het onderzoek

Zoals hiervoor aangegeven is de doelstelling van het onderzoek vast te stellen dat de relevante bepalingen van de WCK op juiste en volledige wijze zijn opgenomen in het informatiesysteem van de vergunninghouder.

Bij de systeemgerichte controle van een informatiesysteem is de accountant voornamelijk geïnteresseerd in de controles die direct gericht zijn op de betrouwbaarheid van bestanden, gegevens en gegevensstromen. Deze controles kunnen door het informatiesysteem worden uitgevoerd of, in het voor- en natraject, door de gebruikers. Deze controles worden toepassingscontroles genoemd.

Het in het kader van het WCK-onderzoek belangrijkste gedeelte van het informatiesysteem van de cliënt is dat gedeelte dat de kredietvergoeding berekent. Om vast te stellen dat de berekeningen conform de WCK worden uitgevoerd, zal de accountant zijn onderzoek richten op de toepassingscontroles rond de berekening van de kredietvergoeding.

De werking van deze toepassingscontroles kan evenwel niet los worden gezien van de omgeving waarin deze functioneren, en de kwaliteit van de ontwikkelomgeving die deze controles hebben 'geproduceerd'.

Zo mogen geprogrammeerde toepassingscontroles niet uitgeschakeld kunnen worden door gebruikers en wordt de effectiviteit van handmatige toepassingscontroles bepaald door de controlebewustheid. Denk in dit verband bijvoorbeeld aan de password-discipline.

In de toepassingscontroles dient de juiste werking van de renteberekening conform de bepalingen van de WCK te zijn opgenomen.

Voordat dus gebruik kan worden gemaakt van de toepassingscontroles zal er een stelsel van organisatorische maatregelen en procedures moeten bestaan dat ervoor zorgt dat applicaties en toepassingscontroles adequaat worden ontworpen, geïmplementeerd en onderhouden, en niet kunnen worden aangetast. Dit stelsel van organisatorische maatregelen en procedures wordt algemene computercontroles genoemd. Deze bestaan uit de volgende onderdelen:

- algemene organisatie van de automatisering binnen de onderneming;
- systeemontwikkelings- en onderhoudsprocedures;
- test-, acceptatie- en overdrachtsprocedures;
- adequate functiescheidingen;
- logische en fysieke toegangsbeveiliging.

Hierna zal de controle-aanpak uiteengezet worden, gericht op de voor het WCK-onderzoek van belang zijnde toepassingscontroles, waarbij de algemene computercontroles als rode draad worden gehanteerd.

Algemene organisatie van de automatisering binnen de onderneming

Bij de algemene organisatie gaat het om de manier waarop het management met de automatisering omgaat. Nadere aandachtsgebieden zijn de plaats van de automatisering in de organisatie, de kwaliteit van de automatiseerders, en de mate waarin gebruikers tevreden zijn over de automatiseringsafdeling en haar produkten. Meer specifiek ten aanzien van de WCK is van belang om na te gaan welke afdelingen/functies binnen de organisatie zich bezighouden met de implementatie en het onderhoud van de WCK-procedures. Zijn deze functies onafhankelijk en deskundig genoeg en hebben deze voldoende gezag om een betrouwbare implementatie te waarborgen?

Systeemontwikkelings- en onderhoudsprocedures

Voorbeelden van methodieken die helpen om de kwaliteit van de opgeleverde produkten te waarborgen zijn het hanteren van een algemeen aanvaarde ontwikkelingsmethodiek en CASE-tools, peer review door collega-programmeurs, eigen testprocedures, adequate aandacht voor documentatie en voldoende gebruikersbetrokkenheid via voorlichtingsronden, prototyping en participatie in stuurgroepen.

Om vast te stellen dat voldoende aandacht aan de rekenregels volgens de WCK is geschonken, zal de accountant kennis nemen van het functioneel ontwerp, handleidingen, notulen van de stuurgroep/ontwikkelgroep en dergelijke. Hieruit dient te blijken dat bij de bouw dan wel het onderhoud van het systeem voldoende aandacht is besteed aan de relevante bepalingen van de WCK. Vervolgens dient de accountant aan de hand van het detailontwerp na te gaan dat op juiste en volledige wijze de diverse rekenregels zijn verwerkt, dan wel vast te stellen dat op dit onderdeel voldoende (interne) controle is uitgeoefend.

Ten slotte is het belangrijk dat bij onderhoud van de programmatuur de rekenregels niet worden aangetast. Hiertoe is het van belang dat als onderdeel van de onderhoudsprocedures is opgenomen

dat alle wijzigingsverzoeken (mede) worden geautoriseerd door een persoon/stuurgroep die vaststelt dat de integriteit van de relevante rekenregels niet wordt aangetast wanneer aan het verzoek wordt voldaan.

Test-, acceptatie- en overdrachtsprocedures

Nadat de accountant heeft vastgesteld dat in de ontwerp- en bouwfase rekening is gehouden met de bepalingen van de WCK, zal de accountant vaststellen dat adequate test-, acceptatie- en overdrachtsprocedures ervoor hebben gezorgd dat het ontworpen informatiesysteem ook als zodanig in produktie is genomen. Van belang is dat bij het testen specifiek de juistheid van de rekenregels conform de WCK is getest. De accountant stelt vast dat voldoende relevante testgevallen zijn ontworpen, verwerkt en dat de uitkomsten zijn getoetst aan de relevante bepalingen van de WCK. Bij de toetsing van de volledigheid van de testgevallen is het van belang dat ten minste de situaties zoals deze zijn opgenomen in de vragenlijst onderdeel hebben uitgemaakt van de testset. Bij twijfel over de volledigheid van de gehanteerde testset kan de accountant besluiten de tests, aan de hand van de situaties in de vragenlijst, over te doen. Daarbij dient de accountant te constateren dat de softwareversie waarin wordt getest gelijk is aan de versie die in het jaar van controle aanwezig was. Dit kan worden bewerkstelligd door gebruik te maken van reeds aanwezige output van verschillende contractsituaties, en aan de hand van deze output de tests over te doen.

Adequate functiescheidingen

Nadat in de ontwerp- en bouwfase voldoende aandacht aan de WCK is geschonken, en de test-, acceptatie- en overdrachtsprocedures ervoor hebben gezorgd dat op juiste wijze deze applicaties in produktie zijn genomen, dienen adequate functiescheidingen te garanderen dat

- deze in produktie genomen applicaties niet worden aangetast;
- de door deze applicaties gebruikte rente- en provisietabellen niet door ongeautoriseerden kunnen worden gewijzigd.

Bovenstaande moet worden afgedwongen door fysieke en logische toegangsbeveiliging.

Logische en fysieke toegangsbeveiliging

Om te voldoen aan de voorwaarden van de WCK met betrekking tot de berekende kredietvergoeding is het niet voldoende dat alleen de juiste werking van de renteberekening wordt geconstateerd. In het kader van de WCK is het tevens van belang dat door de vergunninghouder de juiste (door het Ministerie van Economische Zaken opgegeven) rentetarieven zijn gehanteerd. Hiertoe dient de accountant na te gaan of er adequate logische toegangsbeveiliging is tot de rentetabellen, en of er in is voorzien dat deze tijdig (omlaag) worden aangepast.

De nadere uitvoering van de controle op adequate logische toegangsbeveiliging is afhankelijk van de technische omgeving waarin het informatiesysteem draait. Specifieke aandacht richt de accountant op de bevoegdheid tot muteren van de rente- en provisietabel. Hij zal de procedure rond het onderhoud van deze tabellen beoordelen en nagaan dat de bevoegdheid tot muteren slechts beperkt binnen de onderneming is uitgedeeld.

SAMENVATTING

Het onderzoek door de huisaccountant in het kader van de WCK is een systeemgericht onderzoek. Volgens de toelichting bij het Handboek kan de accountant niet volstaan met de beoordeling van individuele kredietdossiers. Bij het onderzoek is het van belang na te gaan dat het administratieve systeem erin *voorziet* dat de relevante bepalingen uit de wet worden nageleefd.

In een geautomatiseerde omgeving zal een onderzoek moeten plaatsvinden naar de algemene computercontroles en de specifieke toepassingscontroles. De specifieke toepassingscontroles dienen te waarborgen dat de rekenregels in overeenstemming zijn met de relevante bepalingen van de WCK. De algemene computercontroles dienen te waarborgen dat deze toepassingscontroles inderdaad zijn opgenomen in de programmatuur en dat er adequate logische toegangsbeveiliging is rond de kritische (rente- en provisie)tabellen. Tot slot zullen adequate onderhoudsprocedures ervoor moeten zorgen dat de integriteit van de rekenregels niet wordt aangetast.

Door bovengenoemde werkzaamheden wordt de kennis van de accountant omtrent het geautomatiseerde informatiesysteem van de desbetreffende onderneming vergroot. Deze kennis en de uitkomsten van het onderzoek kunnen tevens worden gebruikt in het kader van de algemene jaarrekeningcontrole. Zo wordt een hoge mate van efficiency bereikt in de uitvoering van de werkzaamheden. In welke mate gebruik kan worden gemaakt van de uitkomsten is echter afhankelijk van de exacte omstandigheden bij de cliënt, en zal door de accountant ter plaatse moeten worden nagegaan.

LITERATUUR

[Fijn93] R.G.A. Fijneman, *Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving*, Compact 1993/4.

[Gast92] S.J. Gaston, *Managing and Controlling Small Computer Systems including Lan's*, The Canadian institute of chartered accountants, 1992.

R. van den Hoorn RA
Is sinds 1984 werkzaam bij KPMG. Eerst in de algemene controlepraktijk, sinds juli 1993 bij KPMG EDP Auditors. Hij is bezig met de post-doctorale EDP-Auditopleiding aan de Vrije Universiteit te Amsterdam. Zijn auditervaring ligt met name op het gebied van administratieve organisatie en informatiesystemen. Binnen KPMG is hij docent van de cursus interne controle en automatisering.

Third party review en -mededeling bij uitbesteding van IT-services

Drs. P. Veltman RE RA

Nu steeds meer organisaties ertoe overgaan delen van hun automatisering uit te besteden aan derden of hun IT-afdelingen te verzelfstandigen, en daarbij steeds afhankelijker worden van de beheersingsmaatregelen die de dienstverlenende organisatie heeft getroffen, neemt ook de belangstelling voor zogenaamde third party-mededelingen toe.
Beroepsvoorschriften op dit terrein zijn in het buitenland verder ontwikkeld dan in Nederland. Het artikel geeft een verkenning van het terrein.

INLEIDING

Regelgevende instanties in met name de Verenigde Staten en het Verenigd Koninkrijk zijn de laatste jaren opgeschrikt door de spectaculaire ondergang van vooraanstaand geachte ondernemingen. Bij deze deconfitures was bovendien vaak sprake van ernstige onregelmatigheden. Dit was reden voor het uitvaardigen van wet- en regelgeving om het management nadrukkelijker te confronteren met zijn verantwoordelijkheid voor interne controle, waarbij ook een rol werd toebedacht aan de externe accountant.
Een probleem doet zich voor als onderdelen van de bedrijfsprocessen zijn uitbesteed, zoals vaak het geval is bij automatisering. De uitbestedende organisatie wordt dan afhankelijk van de interne controle bij de service-organisatie, maar moet toch haar verantwoordelijkheid kunnen nakomen voor het stelsel van interne-controlemaatregelen als geheel. Een third party-mededeling kan dan uitkomst bieden.

In dit artikel wordt stilgestaan bij de uitvoering van en de rapportage over onderzoeken van de interne controle bij service-organisaties ten behoeve van derden, tegen de achtergrond van de geschetste ontwikkelingen. Na een korte achtergrondschets wordt ingegaan op enkele begrippen in relatie tot IT-uitbesteding en aandachtspunten bij uitbesteding. Vervolgens komen de third party review (TPR) en de third party-mededeling (TPM) aan de orde. Tot slot wordt kort aandacht besteed aan de betekenis van een TPR en TPM voor de uitbestedende organisatie en haar accountant.
Het artikel heeft het karakter van een terreinverkenning. Veel van dit terrein is nog niet in kaart gebracht, en het voert buiten het bestek van dit artikel om de vele witte plekken in te vullen.

ACHTERGROND

Zowel bij overheid en andere regelgevende instanties als bij het management van organisaties en haar accountants bestaat de laatste jaren onmiskenbaar een verhoogde aandacht voor de kwaliteit van interne controle. Aanleiding hiervoor was de ondergang van een groot aantal spaarbanken in de Verenigde Staten en van ondernemingen als BCCI en Maxwell in het Verenigd Koninkrijk. Gealarmeerd door de omvang van de financiële verliezen en de in veel gevallen vergaande onverantwoordelijkheid en immoraliteit van bestuur en management bij deze deconfitures, hebben toezichthoudende instanties in deze landen nieuwe regelgeving uitgevaardigd aangaande bestuur en interne controle bij ondernemingen.[1]
In de VS werd bij deze regelgeving aansluiting gezocht bij het bekende COSO-rapport ('Internal Control - Integrated Framework' ([COSO92])), dat uitgaat van een brede benadering van interne controle.

Elementen in de nieuwe regelgeving (zie bijvoorbeeld [Cadb92] en [FDIC93]) zijn het benadrukken van de verantwoordelijkheid van het management voor de kwaliteit van de interne controle, tot uitdrukking komend in een mededeling ('management representation') in het jaarverslag. Deze verantwoording moet door de externe accountant worden beoordeeld.

Voor de Nederlandse situatie kan als voorbeeld worden genoemd de Wet toezicht kredietwezen 1992, die in artikel 22 een bepaling bevat welke De Nederlandsche Bank (DNB) de bevoegdheid geeft aan onder toezicht staande instellingen aanbevelingen en algemene richtlijnen voor hun bedrijfsvoering te geven met betrekking tot de administratieve organisatie – met inbegrip van de financiële administratie en de interne controle.
De bepalingen in deze wet en de inmiddels op grond hiervan uitgevaardigde aanbevelingen en richtlijnen[2] gaan vooralsnog belangrijk minder ver dan die in de Angelsaksische landen.

Een bijzondere situatie in de interne controle ontstaat als onderdelen van kritieke bedrijfsprocessen zijn uitbesteed aan een service-organisatie. Dit kan het geval zijn bij uitbesteding van automatiseringsdiensten, maar doet zich bijvoorbeeld ook voor bij uitbesteding van effectenbewaring. In deze situatie is de uitbestedende organisatie voor wat betreft de beheersing van haar bedrijfsprocessen en in voorkomende gevallen haar voortbestaan, afhankelijk van de getroffen maatregelen van interne controle bij de service-organisatie. Ook de accountant die belast is met de controle van de jaarrekening van de uitbestedende organisatie, kan in een positie geraken dat hij moet steunen op de goede werking van de interne controle bij de service-organisatie om tot een goedkeurend oordeel te kunnen komen.

Vanzelfsprekend moet ook zonder de genoemde wet- en regelgeving het management zijn verantwoordelijkheid kunnen nakomen voor het totale systeem van interne controle, en moet de externe accountant van de uitbestedende organisatie hier zo nodig op kunnen steunen bij de controle van de jaarrekening. De geschetste ontwikkelingen hebben er echter toe bijgedragen dat de eisen die worden gesteld aan onderzoeken van en rapportages over de interne controle bij service-organisaties ten behoeve van derden, worden aangescherpt. Het meest duidelijke voorbeeld hiervan is het uitbrengen in 1992 door het Amerikaanse AICPA van SAS 70 ([AICP92]), ter vervanging van SAS 44, mede naar aanleiding van het COSO-rapport. De rapportages volgens de geactualiseerde richtlijnen bieden het management en de auditors van uitbestedende organisaties meer steun bij het beoordelen van de effectiviteit van de interne controle bij service-organisaties, en daardoor bij het inrichten en beoordelen van de interne controle bij de uitbestedende organisatie.

Een bijzondere situatie in de interne controle ontstaat als onderdelen van kritieke bedrijfsprocessen zijn uitbesteed aan een service-organisatie.

Ook in Nederland bestaat bij regelgevende instanties zorg over de gevolgen van het uitbesteden van automatiseringsdiensten, zoals blijkt uit het uitbrengen door DNB van een considerans inzake de uitbesteding van de geautomatiseerde gegevensverwerking door kredietinstellingen ([DNB94]). Daarnaast kan het Voorschrift Informatiebeveiliging Rijksdienst worden vermeld, waarin de volgende bepaling is opgenomen:
'Indien de systeemexploitatie geheel of gedeeltelijk is uitbesteed, dient volgens een vastgesteld schema een onafhankelijk oordeel over de kwaliteit van de bij de opdrachtnemer getroffen informatiebeveiligingsmaatregelen en over het handhaven en naleven daarvan te worden verlangd.' ([DIBI94]).

BEGRIPPEN

Vooral met betrekking tot uitbesteding van automatiseringsdiensten lijkt een Babylonische spraakverwarring te zijn ontstaan. In deze paragraaf wordt getracht hierin enige helderheid te brengen, maar eerst wordt ingegaan op enkele begrippen met betrekking tot third party reviews en -mededelingen.

TPR en TPM

In Nederland lijkt de term third party-mededeling (TPM) ingang te hebben gevonden, waar in de Angelsaksische landen wordt gesproken van een third party review (TPR). TPM heeft betrekking op

1 *Zoals bekend heeft de nieuwe regelgeving verdere debâcles, zoals Orange County in de VS en Barings in het VK, niet kunnen voorkomen.*

2 *Administratieve organisatie bij kredietinstellingen, Nederlandse Staatscourant van 28 mei 1993 - nr. 99.*

de uitkomsten van een onderzoek, terwijl TPR het onderzoek zelf betreft. In het Nederlands zou kunnen worden gesproken van een 'derdenmededeling' respectievelijk een 'derdenonderzoek'.[3]

In lijn met de Angelsaksische benamingen wordt in dit artikel uitgegaan van de volgende definities:

Service-organisatie: Organisatie die automatiseringsdiensten verleent.

Service-auditor: Auditor die ten behoeve van één of meer derden onderzoeken verricht naar opzet en werking van de interne controle bij een service-organisatie en hierover rapporteert.
De 'auditor' kan hierbij een accountant, EDP-auditor of anderszins gekwalificeerde zijn.

User-organisatie: Organisatie die automatiseringsdiensten afneemt.

User-auditor: Auditor van organisatie die automatiseringsdiensten afneemt. In het algemeen betreft dit de accountant die belast is met de controle van de jaarrekening, maar het kan ook gaan om een auditor die de opdracht heeft een onderzoek uit te voeren naar de interne controle bij de user-organisatie.

Third party-mededeling: Een schriftelijke mededeling van een service-auditor inhoudende de uitkomsten van een onderzoek naar de interne controle bij een service-organisatie, ten behoeve van één of meer derden.[4]

Third party review: Onderzoek van een service-auditor naar de interne controle bij een service-organisatie, ten behoeve van één of meer derden.

Uitbesteding

Uitbesteding van automatiseringsdiensten kan betrekking hebben op het gehele scala van IT-services, variërend van de ontwikkeling van informatiesystemen of het beschikbaar stellen van computer- of netwerkcapaciteit, tot en met de gehele automatiseringsfunctie of een belangrijk deel daarvan.

Traditionele, inmiddels minder gangbare begrippen om bepaalde vormen van IT-services aan te duiden zijn:

Time-sharing: Het beschikbaar stellen van computercapaciteit (tegenwoordig vooral netwerkcapaciteit).

Dataservice: De exploitatie (ontwikkeling, onderhoud en verwerking) van een informatiesysteem. Het bekendste voorbeeld hiervan is de salarisverwerking.

Tegenwoordig wordt vooral gesproken over 'facilities management' en 'outsourcing':

Facilities management: In [Zwar91] werd hiervoor de volgende definitie gehanteerd:
'Facilities Management is het op basis van een langlopend contract en tegen een vaste prijs overnemen van de exploitatie en het beheer van een combinatie van een aantal IT-facilities. Onder dergelijke IT-facilities wordt verstaan: hardware inclusief onderhoud, software inclusief ondersteuning, personeel, systeem- en netwerkbeheer, software-ontwikkeling, installatie van nieuwe applicaties en opleidingen.'

Deze definitie is tot stand gekomen in nauw overleg met de toenmalige vereniging Computer Service- en Softwarebureaus (COSSO), waarvan veel facilities management-aanbieders lid waren.
Facilities management wordt wel beschouwd als de meest vergaande vorm van uitbesteding, en is te vergelijken met het uitbesteden van (niet-kern-) activiteiten als catering, gebouwenbeheer en wagenparkbeheer.

Outsourcing: Zoals bekend is 'outsourcing' een neologisme, gevormd door de samentrekking van 'out' en 'resourcing'. Naar de indruk van de auteur wordt 'outsourcing' heden ten dage als synoniem van 'uitbesteding' beschouwd.

Volgens [Nola91] echter, is outsourcing de meest vergaande vorm van uitbesteding. Het verschil met facilities management is vooral dat outsourcing is gericht op het bereiken van strategische organisatiedoelstellingen in plaats van efficiëntievoordelen, waardoor de relatie met de outsourcing-partner het karakter krijgt van een strategische alliantie, verschillend van een leverancier/afnemer-verhouding.

In dit artikel zal verder worden uitgegaan van de neutrale term uitbesteding – tenzij anders aangegeven –, waarmee dan vooral het uitbesteden van de exploitatie van een informatiesysteem wordt bedoeld.

Interne controle

Het begrip interne controle wordt in dit artikel gehanteerd in de brede betekenis zoals aangegeven in het eerder genoemde COSO-rapport, waarop in een volgende paragraaf nader wordt ingegaan. Voor interne controle in deze betekenis wordt ook wel het begrip management control gehanteerd.

AANDACHTSPUNTEN BIJ UITBESTEDING VOOR DE USER-ORGANISATIE

Bij uitbesteding van automatiseringsdiensten wordt de user-organisatie voor wat betreft de kwaliteit van de informatievoorziening, zoals de betrouwbaarheid en continuïteit, afhankelijk van de maatregelen van interne controle die de service-organisatie heeft getroffen. Deze afhankelijkheid kan zover gaan dat het voortbestaan van de user-organisatie ermee in het geding is, zoals bij een luchtvaartmaatschappij die haar reserveringssysteem heeft uitbesteed.[5]

3 *Op de eventuele betekenisverschillen (met bijbehorende vaktechnische consequenties) tussen 'review', 'audit' en 'investigation' (of 'beoordeling', 'controle' en 'onderzoek') wordt in het kader van dit artikel niet ingegaan.*

4 *Overigens kan worden beargumenteerd dat in de zin van de GBR-1994 ([NIVR94]) sprake is van een verklaring, betrekking hebbend op een (niet-financiële) verantwoording van het management van de service-organisatie.*

5 *Dat hierbij niet alleen de continuïteit van het informatiesysteem van belang is maar ook de betrouwbaarheid, moge blijken uit het voorbeeld van Virgin Atlantic (VA), dat een deel van haar reserveringssysteem had uitbesteed aan British Airways (BA). Medewerkers van BA maakten misbruik van deze situatie onder meer door gefingeerde boodschappen over volgeboekte en gecancelde VA-vluchten over het netwerk te sturen, waardoor VA opbrengsten misliep.*

Bij schade die het gevolg is van tekort schietende interne controle bij de service-organisatie, kan de user-organisatie deze aansprakelijk stellen, waarbij met name de desbetreffende contractbepalingen van belang zijn. Service-organisaties weten echter meestal een vergaande aansprakelijkheidsuitsluiting in het contract te bewerkstelligen, niet alleen ten aanzien van de oorzaken van de schade waarvoor zij aansprakelijk kunnen worden gesteld, maar ook ten aanzien van de omvang.

Ook indien de service-organisatie voor de volle omvang van de schade kan worden aangesproken, biedt dit niet altijd soelaas. Als de service-organisatie over onvoldoende middelen beschikt is de gedupeerde user-organisatie niet geholpen. Weliswaar kan de service-organisatie een aansprakelijkheidsverzekering hebben afgesloten, maar dit is niet altijd mogelijk, en bovendien is ook hierbij sprake van allerlei uitsluitingsbepalingen en beperkingen van het verzekerd risico.

Zelfs indien de schade geheel kan worden verhaald op de service-organisatie en haar verzekeraar, is het de vraag of het belang van de gedupeerde user-organisatie en van de maatschappij in het algemeen hiermee altijd is gediend. Het primaire doel van de meeste organisaties is continuïteit; in geval van discontinuïteit is het moeilijk voorstelbaar dat de schadevergoeding in alle opzichten toereikend zal zijn.
Het is om deze redenen dat de user-organisatie in veel gevallen een legitieme behoefte heeft om te worden geïnformeerd over de opzet en de werking van de interne controle bij de service-organisatie. Hetzelfde geldt voor de user-auditor en eventueel voor regelgevende instanties.

Voor de service-organisatie is het vanzelfsprekend uitermate onpraktisch om alle user-organisaties afzonderlijk in de gelegenheid te stellen zich een oordeel te vormen over de getroffen maatregelen van interne controle. In deze situatie biedt een TPM uitkomst.
Voor de user-organisaties is het zaak in het contract met de service-organisatie regelingen op te nemen met betrekking tot wederzijdse verantwoordelijkheden en daaruit voortvloeiende aansprakelijkheden, aansprakelijkheidsverzekeringen en het verschaffen van informatie aan user-organisatie, user-auditor en toezichthoudende instanties.[6]
Een checklist van mogelijke contractvoorwaarden is opgenomen in tabel 1.

HET UITVOEREN VAN EEN THIRD PARTY REVIEW

Bij een third party review kunnen de onderstaande fasen worden onderkend:
1 opdrachtverstrekking;
2 vaststelling onderzoeksobject, doel en reikwijdte (scope);
3 planning en uitvoering;
4 oordeelvorming.

In dit rijtje is de fase van opdrachtaanvaarding buiten beschouwing gelaten. Deze problematiek leent zich voor behandeling in een afzonderlijk artikel.

Op het viertal genoemde fasen wordt in de volgen-

Tabel 1. Checklist contractvoorwaarden bij uitbesteding (ontleend aan [AICP87]).

- Beschrijving van aan te leveren invoer, uit te voeren bewerkingen en op te leveren uitvoer.
- Procedures voor het afhandelen van fouten.
- Procedures voor het beveiligen van gegevens.
- Afspraken over het uitvoeren van controles bij de service-organisatie.
- Bepalingen over de verantwoordelijkheid van de user-organisatie, in het bijzonder met betrekking tot invoergegevens, invoercontroles en wijzigingen van stamgegevens.
- De contactpersoon bij de service-organisatie en de persoon bij de user-organisatie die bevoegd is afspraken te maken met de service-organisatie.
- Een beschrijving van de verschillende tarieven voor bijvoorbeeld gegevensconversie, normale verwerking, programmering, materiaal, tariefdifferentiatie voor piek- en daluren, bezorging, opslag, speciale rapporten en herhaalde verwerking.
- Voorzieningen voor conversie en deconversie, waaronder de mogelijkheid van parallelle verwerking.
- Bepalingen over de aansprakelijkheid van de service-organisatie, inclusief aansprakelijkheidsverzekering, in geval van foutieve verwerking of verlies van gegevens.
- Bepalingen over het eigendom van gegevensbestanden, programma's en documentatie.
- Bepalingen over vorm en frequentie van de facturering.
- Bepalingen over de verantwoordelijkheid van de service-organisatie voor het onderhouden van een controlestructuur.
- De verantwoordelijkheid van de service-organisatie voor het informeren van de user-organisatie over veranderingen die van invloed zijn op de gegevensverwerking, uitvoer, of andere procedures.
- Het verwerkingsrooster, waaronder de aanlevertijden voor invoer en uitvoer.
- De verantwoordelijkheid van de service-organisatie voor het opleggen van bepaalde arbeidsvoorwaarden, zoals een geheimhoudingsplicht, aan haar personeel.
- De geldigheidsduur en verlengings- en opzeggingsvoorwaarden van het contract.
- Bepalingen over de verantwoordelijkheid van de service-organisatie om auditors van de user-organisatie rapportages te verschaffen van de auditor van de service-organisatie.
- Bepalingen over de verantwoordelijkheid van de service-organisatie om informatie te verschaffen en anderszins medewerking te verlenen aan auditors en toezichthoudende instanties.

6 Dat dit niet altijd eenvoudig zal zijn, moge blijken uit het aangehaalde art. 5 lid c van het Voorschrift Informatiebeveiliging Rijksdienst (zie paragraaf Achtergrond), waarin wordt voorgeschreven dat een onafhankelijk oordeel wordt 'verlangd' (in plaats van 'vereist' of 'verkregen' of iets dergelijks).

de paragrafen nader ingegaan. De rapportagefase wordt behandeld in de paragraaf TPM.

FASE 1, OPDRACHTVERSTREKKING

Bij de opdrachtverstrekking zijn onder meer van belang de opdrachtgever en de opdrachtnemer.

Opdrachtgever
De opdracht tot het uitvoeren van een TPR kan afkomstig zijn van de service-organisatie, een of meer user-organisaties (mogelijk op instigatie van de user-auditor) of een toezichthoudende instantie. Als de opdracht afkomstig is van een derde moet de medewerking van de service-organisatie worden verkregen, al dan niet op grond van contractuele of wettelijke bepalingen.

Bij traditionele IT-services, zoals de exploitatie van een salarissysteem ten behoeve van meerdere user-organisaties, en bij leveranciers van standaardpakketten, kan een 'user group' goed van pas komen, om de medewerking van de service-organisatie te verkrijgen en om concrete invulling te geven aan de opdracht.

Voor de feitelijke uitvoering van een TPR ligt inschakeling van een EDP-auditor voor de hand.

Ook bij andere vormen van IT-dienstverlening, bijvoorbeeld de verwerking op een gemeenschappelijke infrastructuur van informatiesystemen die niet gemeenschappelijk worden gebruikt, kan een user group haar diensten bewijzen, al zal de nadere invulling van de opdracht dan een algemener karakter hebben.

Opdrachtnemer
Gebruikelijk is dat de opdracht tot uitvoering van een TPR wordt verstrekt aan een openbaar accountantskantoor, hetgeen ook in lijn is met bestaande wet- en regelgeving (zoals de Wet computercriminaliteit en het DNB-memorandum ([DNB88])). Gezien de benodigde automatiseringskennis ligt het echter voor de hand dat voor de feitelijke uitvoering een beroep wordt gedaan op een EDP-auditor.

Andere instanties die in aanmerking kunnen komen zijn de volgende:
- openbaar EDP-auditorskantoor. Zelfstandig gevestigde EDP-auditors met een openbare functie zijn er echter nog niet veel; de meeste EDP-auditors zijn verbonden aan een openbaar accountantskantoor, interne accountantsdienst of overheidsdienst;
- interne auditorsdienst van de service-organisatie. Als bezwaar hiertegen geldt dat een dergelijke dienst een minder onafhankelijke positie ten opzichte van het management van de service-organisatie inneemt. Bovendien kan uitvoering van een TPR en verstrekking van een TPM door een interne auditorsdienst op gespannen voet staan met de desbetreffende beroepsvoorschriften (NIVRA/NOVAA, NOREA), vooral als sprake is van een openbaar te maken verklaring bij een verantwoording;
- interne auditorsdienst van een user-organisatie;
- overheidsdienst als de EDP Audit Pool;
- software- en adviesbureaus, keuringsinstanties en dergelijke.

Een onderzoek ten behoeve van derden van de interne controle bij organisaties die automatiseringsdiensten verlenen, vereist behalve deskundigheid op het gebied van administratieve organisatie en automatisering, een onafhankelijke positie en onpartijdigheid in het oordeel. In de meeste gevallen kwalificeert een EDP-auditor die verbonden is aan een openbaar kantoor zich hiervoor het best.
In het vervolg van dit artikel zal voor de degene die de TPR uitvoert en de TPM verstrekt, ongeacht wie dit is, de term service-auditor worden gebruikt, tenzij anders aangegeven.

Kosten
De kosten van een TPR kunnen ten laste worden gebracht van de service-organisatie (indirect ten laste van de user-organisaties), rechtstreeks ten laste van de user-organisaties, of ten laste van de toezichthoudende instantie.

FASE 2, VASTSTELLING ONDERZOEKSOBJECT, DOEL EN REIKWIJDTE (SCOPE)

De scope van een TPR wordt bepaald door het onderzoeksobject, de kwaliteitsaspecten c.q. kwaliteitseisen, en de mate van diepgang waarin de objecten worden onderzocht.

Onderzoeksobject

Het onderzoeksobject is uiteraard afhankelijk van de dienstverlening van de service-organisatie. Bij een softwarebureau of -leverancier zal de opdracht betrekking hebben op een informatiesysteem, en bij een computerservicebureau mede of met name op de verwerking van een informatiesysteem. In het algemeen gesteld heeft de opdracht betrekking op:
- het ontwerpen, ontwikkelen en onderhouden van informatiesystemen;
- het verwerken van informatiesystemen;
- een combinatie hiervan;
- specifieke onderdelen van de dienstverlening.

Meer concreet wordt het onderzoeksobject gevormd door de maatregelen van interne controle die moeten waarborgen dat de dienstverlening aan bepaalde eisen voldoet of bepaalde doelstellingen bereikt. 'Waarborgen' moet hierbij niet worden geïnterpreteerd als 'garanderen', maar als het verschaffen van redelijke, maar geen absolute zekerheid over het voldoen aan de eisen.

In navolging van het COSO-rapport kan interne controle worden gedefinieerd als een proces, gerealiseerd door de leiding en alle betrokkenen binnen de organisatie, opgezet om redelijke zekerheid te verschaffen over het bereiken van doelstellingen in de volgende categorieën:
- effectiviteit en efficiëntie van bedrijfsprocessen;
- betrouwbaarheid van financiële verslaggeving;
- naleving van wet- en regelgeving.

Deze categorieën zijn van belang voor de user-organisatie, maar laten zich niet eenvoudig vertalen naar onderzoeksobjecten bij een TPR. In de paragraaf Kwaliteitsaspecten en -eisen wordt hierop teruggekomen.

Met betrekking tot interne controle wordt in het COSO-rapport nader onderscheid gemaakt tussen algemene, voorwaardenscheppende componenten en de eigenlijke interne controles.

Algemene componenten van interne controle
De algemene componenten bestaan uit vier categorieën, die onderling nauw met elkaar samenhangen en elkaar deels overlappen:

Controle-omgeving
De controle-omgeving omvat het geheel van factoren die de werksfeer en cultuur binnen een organisatie bepalen en daardoor de controlebewustheid van de mensen binnen de organisatie. Tot deze factoren behoren:
- integriteit, ethische waarden en deskundigheid van de mensen binnen de organisatie;
- mentaliteit en wijze van optreden van de leiding;
- wijze van delegatie van bevoegdheden en verantwoordelijkheden;
- personeelsbeleid.

Het begrip controle-omgeving is ook bekend uit het 'SAC-rapport' ([IIA91]).

Risicobeheersing
Risicobeheersing betreft het identificeren en analyseren van de risico's die het behalen van de doelstellingen van de organisatie bedreigen, en het treffen van maatregelen om de risico's te bewaken en te verminderen.

Informatie en communicatie
Informatie omvat hetgeen wordt gesignaleerd, vastgelegd en gecommuniceerd in een vorm en op tijdstippen die de mensen binnen een organisatie in staat stellen hun verantwoordelijkheden na te komen.
Communicatie omvat het verstrekken van informatie zowel binnen de organisatie als daarbuiten. Effectieve communicatie vraagt een duidelijk signaal van de leiding dat verantwoordelijkheden voor interne controle ernstig worden genomen, alsmede informatie aan alle personeelsleden over hun rol in relatie tot interne controle.

Algemene interne-controlemaatregelen vormen een raamwerk om de effectieve uitvoering van specifieke interne controles te ondersteunen.

Het bewaken van het proces van interne controle
Het bewaken is gericht op de vaststelling van de goede werking van het interne-controlesysteem in de tijd. Dit kan geschieden in de vorm van permanente activiteiten, afzonderlijke evaluaties of een combinatie van beide.

Hoewel deze voorwaardenscheppende componenten ontegenzeggelijk van belang zijn voor de goede werking van de interne controle, zullen zij in de regel niet expliciet in een TPR c.q. TPM worden betrokken.
In de Canadese beroepsrichtlijnen (zie [Widd90]) wordt met betrekking tot de controle-omgeving echter gesteld dat zij weliswaar geen directe relatie heeft met specifieke interne-controlemaatregelen, maar dat de service-auditor niettemin de verantwoordelijkheid heeft de invloed van de controle-omgeving op de interne controle te beoordelen. Voor zover aspecten van de controle-omgeving deel uitmaken van de relevante interne-controlemaatregelen (bijvoorbeeld opleidingsplannen en -budgetten van personeel) moet hierover ook worden gerapporteerd.
In de geraadpleegde Nederlandse literatuur ([NIVR82] en [NIVR89]) zijn hieromtrent geen specifieke aanbevelingen of richtlijnen opgenomen. In de accountancy is het overigens gebruikelijk om in het kader van de jaarrekeningcontrole de controle-omgeving te beoordelen.

Eigenlijke interne controles
De eigenlijke interne controles omvatten, wederom met de woorden van het COSO-rapport, de uitvoering van de voorschriften en maatregelen die helpen om zekerheid te verschaffen dat de richtlijnen van de leiding worden opgevolgd en dat de nodige acties worden ondernomen ter beheersing van de risico's die het bereiken van de doelstellingen van de organisatie in gevaar brengen.
Interne controles omvatten een scala van activiteiten, zoals goedkeuringen, machtigingen, verificaties, aansluitingen, beoordelingen van de uitkomsten van bedrijfsactiviteiten, beveiliging van activa en functiescheiding.

De eigenlijke interne controles kunnen nader wor-

den ingedeeld in algemene controles en specifieke controles.

Algemene interne-controlemaatregelen zijn geen controles als zodanig, maar vormen een raamwerk om de effectieve uitvoering van specifieke interne controles te ondersteunen. Zij omvatten:
- systemen voor budgettering en het sturen op performance-indicatoren;
- algemene aspecten van een eventuele interne auditfunctie: plaats in de organisatie, rapportagelijnen, taakopdracht, deskundigheid, etc.;
- algemene computercontroles (general IT controls). Deze hebben betrekking op aspecten als automatiserings- en beveiligingsbeleid, functiescheiding, systeemontwikkeling, logische en fysieke toegangsbeveiliging, backup en uitwijk, change management van hard- en software, en operating.

De algemene controles worden ook wel gezien als een onderdeel van het bewaken van het proces van interne controle.

Specifieke interne controles zijn de daadwerkelijke controle-activiteiten. In relatie tot geautomatiseerde gegevensverwerking zijn vooral de toepassingscontroles (application controls) van belang, die samen met de algemene computercontroles de computercontroles vormen. De toepassingscontroles bestaan uit geprogrammeerde controles in applicaties en daarmee verbonden handmatige procedures.

Vanzelfsprekend is een TPR primair gericht op de computercontroles (algemeen en/of specifiek). Welke computercontroles van belang zijn hangt af van de dienstverlening van de service-organisatie en uiteraard van de opdracht. Bij een onderzoek naar een informatiesysteem in ontwikkeling kunnen bijvoorbeeld de algemene computercontroles met betrekking tot systeemontwikkeling worden betrokken alsmede de (geprogrammeerde) toepassingscontroles. Bij pakketbeoordeling is het gebruikelijk om uitsluitend deze laatste te onderzoeken.[7] Bij een onderzoek naar de verwerking van informatiesystemen zullen de relevante algemene computercontroles object van onderzoek zijn, in het bijzonder de beveiliging, backup en uitwijk, change management en de operating-functie.

Kwaliteitsaspecten en -eisen

Het kwaliteitsaspect is de eigenschap van de dienstverlening waarop de TPR zich richt, bijvoorbeeld de betrouwbaarheid of de continuïteit. Kwaliteitseisen kunnen worden beschouwd als een nadere concretisering van het overkoepelende kwaliteitsaspect, bijvoorbeeld de eis dat maximaal één op de duizend transacties foutief mag worden verwerkt.

Kwaliteitsaspecten
In relatie tot geautomatiseerde gegevensverwerking worden vaak de volgende kwaliteitsaspecten onderkend:
- betrouwbaarheid: de redelijke zekerheid dat de verwerking van gegevens juist, volledig, tijdig en geoorloofd geschiedt;
- continuïteit: de redelijke zekerheid dat de gegevensverwerking ongestoord voortgang zal kunnen vinden, dat wil zeggen ook na ernstige storingen binnen redelijke termijnen kan worden hervat.
  Onder continuïteit is bij informatiesystemen en programmapakketten tevens te verstaan dat aan de voorwaarden is voldaan om deze systemen te kunnen onderhouden. (Beide definities zijn ontleend aan [NIVR82].);
- vertrouwelijkheid: de redelijke zekerheid dat kennisneming van gegevens beperkt blijft tot daartoe gerechtigden;
- doelmatigheid of efficiëntie: de redelijke zekerheid dat de gegevensverwerking geschiedt tegen aanvaardbare kosten;
- doeltreffendheid of effectiviteit: de redelijke zekerheid dat de gegevensverwerking en informatievoorziening aansluit op de informatiebehoeften en doelstellingen van de user-organisatie;
- bescherming van (materiële) waarden: de redelijke zekerheid dat materiële waarden niet verloren gaan of worden ontvreemd. De bescherming van niet-materiële waarden (concurrentiegevoelige gegevens, waardevolle programma's) valt onder het aspect vertrouwelijkheid.

Hieraan kan nog worden toegevoegd:
- controleerbaarheid: de mate waarin kan worden vastgesteld dat de vereiste kwaliteit wordt gerealiseerd. Dit kwaliteitsaspect heeft betrekking op alle hiervoor genoemde aspecten, en is vooral ook van belang voor de service-auditor bij het uitvoeren van zijn onderzoek.

In [NIVR89] worden enigszins afwijkende kwaliteitsaspecten geïntroduceerd, zoals integriteit en exclusiviteit. Exclusiviteit heeft betrekking op het geoorloofd gebruik van informatie en omvat vertrouwelijkheid (het kennis nemen van informatie) en een deel van betrouwbaarheid (het wijzigen van informatie). Integriteit omvat het resterende deel van betrouwbaarheid (de overeenstemming met het afgebeelde deel van de werkelijkheid).
Hoewel deze begrippen inmiddels hun weg hebben gevonden naar de Nederlandse vakliteratuur van accountancy en EDP-auditing, sluit met name exclusiviteit minder goed aan op de internationaal gebruikelijke terminologie.

De onderscheiden kwaliteitsaspecten kunnen worden beschouwd als een verdere uitwerking van de doelstellingen van interne controle die in het COSO-rapport worden onderkend. Het voldoen aan wet- en regelgeving komt echter niet expliciet tot uitdrukking, maar zit verscholen in de andere aspecten.
Voor een user-organisatie kan een TPR inzake vrijwel al de genoemde kwaliteitsaspecten van belang zijn. Gebruikelijk is echter dat een TPR betrekking heeft op de betrouwbaarheid (bijvoorbeeld in relatie tot de jaarrekeningcontrole bij de user-organisatie) en de continuïteit (inclusief de controleerbaarheid). Onderstaand wordt ingegaan op mogelijke TPR's inzake andere kwaliteitsaspecten.

7 *Bij certificering van computersystemen op beveiligingsaspecten, zoals volgens de Europese Information Technology Security Evaluation Criteria (ITSEC), wordt er overigens naar gestreefd het certificaat zoveel mogelijk te baseren op 'development assurance' (in plaats van 'evaluation assurance'), in verband met de steeds korter wordende 'time to market' van dergelijke produkten.*

Vertrouwelijkheid
User-organisaties die concurrentie- of privacygevoelige gegevens of waardevolle programmatuur laten verwerken door de service-organisatie, zullen belangstelling hebben voor een TPR inzake het vertrouwelijkheidsaspect. In NIVRA 58 ([NIVR91]) wordt met betrekking tot een dergelijk onderzoek als vaktechnische beperking aangegeven dat de auditor geen oordeel kan geven over de wijze waarop de functionarissen die met vertrouwelijke gegevens werken, met deze gegevens omgaan. De laatste schakel in de keten is de mens, en als deze de gegevens niet geheim houdt, bijvoorbeeld door ze in zijn privé-omgeving te verspreiden, dan kan de auditor dit niet vaststellen.

De vraag is echter in hoeverre dit vaktechnische probleem zich ook voordoet bij service-organisaties: voor personeelsleden van de service-organisatie zal het in het algemeen niet nodig zijn dat zij uit hoofde van hun functie inhoudelijke kennis hebben van de gegevens en programma's van user-organisaties. Door technische maatregelen (met name encryptie en een adequaat sleutelbeheer) kan worden verhinderd dat zij deze kennis toch opdoen.
Afgezien daarvan speelt het probleem van misbruik van bevoegdheden niet alleen bij het vertrouwelijkheidsaspect, maar ook bij andere kwaliteitsaspecten. Een overigens bevoegde functionaris van de service-organisatie kan misbruik maken van de technische mogelijkheden waarover hij uit hoofde van zijn functie beschikt en bijvoorbeeld gegevens manipuleren of een 'Trojan horse'[8] implementeren, met (eventueel op termijn) consequenties voor de betrouwbaarheid of continuïteit van de gegevensverwerking.
In ieder geval dienen inherente vaktechnische beperkingen, welke dan ook, toereikend in de TPM te worden toegelicht.[9]

Doelmatigheid
Een TPR inzake de doelmatigheid is iets waarin user-organisaties waarschijnlijk het meest zijn geïnteresseerd, vooral als zij op grond hiervan een besparing kunnen realiseren. De doelmatigheid van een service-organisatie komt tot uitdrukking in het kostprijsdeel van het tarief, dat daarnaast bestaat uit een winstopslag.
In dit verband is het nuttig naar de aard van de dienstverlening onderscheid te maken tussen twee typen service-organisaties.

Ten eerste zijn er *zelfstandige organisaties* die aan een groot aantal heterogene user-organisaties zonder onderlinge binding, min of meer uiteenlopende automatiseringsdiensten verlenen. Voorbeelden zijn IBM, EDS en Geisco.
Bij deze vorm van dienstverlening is sprake van, nog toenemende, concurrentie, zodat mag worden aangenomen dat het tarief (kostprijs en winstopslag) bedrijfseconomisch aanvaardbaar is.
Een TPR van de doelmatigheid is bij dergelijke service-organisaties bedrijfseconomisch waarschijnlijk niet rationeel.

Ten tweede zijn er *branche-organisaties*, waaronder tevens begrepen rekencentra binnen een groepsstructuur, die ten behoeve van een homogene groep user-organisaties, die veelal aandelen houden in de service-organisatie, min of meer uniforme diensten verlenen. Voorbeelden zijn de eerder genoemde service-organisaties die specifieke bancaire diensten verzorgen, zoals betalingsverkeer.
Hierbij is de facto sprake van een monopolie, hetgeen voor wat de winstopslag betreft geen probleem inhoudt voor de user-organisaties, mits zij op de een of andere manier kunnen participeren in de winst.

Een TPR heeft gewoonlijk betrekking op de betrouwbaarheid en de continuïteit (inclusief controleerbaarheid).

Gezien de monopoliepositie bestaat er voor deze service-organisaties geen druk vanuit de markt om de kostprijs zo laag mogelijk te houden. Bij dit type service-organisatie kan een TPR van de doelmatigheid waardevol inzicht opleveren.

Vanzelfsprekend zijn bij deze twee typen tussenvormen denkbaar.

Een TPR van de doelmatigheid kan het best worden uitgevoerd aan de hand van referentiegegevens van vergelijkbare service-organisaties (bijvoorbeeld elders in de wereld), een techniek die 'benchmarking' wordt genoemd. Als geen referentiegegevens beschikbaar zijn is een dergelijk onderzoek een moeizame en kostbare aangelegenheid, gezien de benodigde (technische) deskundigheid.

Doeltreffendheid
Het ligt niet voor de hand dat de service-auditor een onderzoek uitvoert naar de effectiviteit van de dienstverlening (in relatie tot de informatiebehoeften en organisatiedoelstellingen van de user-organisaties). Niet alleen kunnen de doelstellingen zeer divers zijn, hetgeen overigens ook bij andere kwaliteitsaspecten een probleem kan vormen, maar vooral zijn de user-organisaties en user-auditors het best in staat deze te beoordelen, aangezien hiervoor inzicht in de doelstellingen van de user-organisatie noodzakelijk is.

Bescherming van waarden
Bij bepaalde vormen van uitbesteding (meestal facilities management genoemd), waarbij de hardware eigendom is van de user-organisatie maar de operations en het management worden verzorgd door de service-organisatie, kan de user-organisatie geïnteresseerd zijn in een TPR inzake de bescherming van waarden. (Een dergelijke TPR is daarnaast vooral van belang bij bepaalde service-organisaties die andere dan automatiseringsdiensten verlenen, zoals bewaring van effecten of kostbare metalen.)

8 Een 'Trojan horse' kan in dit verband worden gedefinieerd als een programma met een schijnbaar of werkelijk nuttige functie, waarin een component is verborgen met een kwaadaardige functie.

9 De accountancy kent in dit verband nog het leerstuk van het axiomatisch voorbehoud: een vaktechnische beperking die zelfs voor een leek zo vanzelfsprekend is of althans wordt geacht, dat zij niet expliciet behoeft te worden vermeld. In het vakgebied EDP-auditing wordt dit begrip niet gehanteerd, waarschijnlijk omdat er zo weinig vanzelfsprekendheden zijn. Niettemin ziet men in EDP-auditrapporten de 'uncertainty paragraph', met vermelding van inherente onderzoeksbeperkingen, steeds korter worden of zelfs geheel verdwijnen. (Vergelijk bijvoorbeeld de aanbevolen teksten voor mededelingen in NIVRA 26 en NIVRA 53 of 58.) Overigens is het axiomatisch voorbehoud binnen de accountancy regelmatig onderwerp van discussie.

Kwaliteitseisen
Het kwaliteitsaspect (of de kwaliteitsaspecten) waarop de TPR betrekking heeft, is de overkoepelende kwaliteitseis waaraan de maatregelen van interne controle worden getoetst. Aangezien de afstand tussen de overkoepelende kwaliteitseis (zoals de betrouwbaarheid van de informatieverwerking) en de interne-controlemaatregelen (zoals invoerscreening) betrekkelijk groot is, bestaat er behoefte aan meer concrete eisen[10] om deze afstand te overbruggen.

Idealiter is voor de dienstverlening waarop de TPR van toepassing is, een service level agreement afgesloten waarin de kwaliteitseisen concreet zijn uitgewerkt. In de praktijk blijkt echter dat voor zover dit het geval is, er nog altijd een grote vertaalslag nodig is om te komen tot concrete toetsingscriteria. Een oplossing kan zijn om aansluiting te zoeken bij baseline-criteria, zoals de Code voor informatiebeveiliging ([NNI94]).

Ten aanzien van de scope-afbakening in relatie tot de kwaliteitseisen doet zich een accentverschil voor tussen de situatie in Nederland en die in de VS en Canada (literatuur met betrekking tot de situatie in andere landen is in het kader van dit artikel niet geraadpleegd).
Waar in Nederland uiteindelijk wordt getoetst aan een overkoepelende eis, die geldt voor het onderzoeksobject als geheel, wordt in deze landen voornamelijk getoetst aan min of meer concreet uitgewerkte eisen. Dit verschil komt niet alleen tot uitdrukking in de bijlagen bij de mededeling (en mogelijk in de uitvoering van het onderzoek), maar ook in de scope-afbakening en in de mededeling.

Ter illustratie zijn in de voorbeelden 1 en 2 enige (sterk vereenvoudigde en gestileerde) gedeelten van de bijlagen bij een Canadese TPM opgenomen, betrekking hebbend op algemene computercontroles (ontleend aan [Widd90]).

In de VS en Canada wordt de scope vooral bepaald door de concrete controledoelstellingen en bijbehorende controlemaatregelen die in het onderzoek worden betrokken.
In Nederland staan bij de afbakening van het onderzoek de kwaliteitsdrager en het kwaliteitsaspect centraal. Hierbij heeft zich een zekere theorievorming ontwikkeld, waarbij de onderzoeksobjecten bijvoorbeeld worden ingedeeld in statische

Voorbeeld 1. Samenvattende bijlage bij TPM.

XYZ Service Organization (XYZ) operates a data centre which provides its customers on-line computer based systems. Batch generation of reports extracted from on-line data is also available on request.

The data centre houses computer hardware and system software and accomodates operators responsible for day-to-day operations of the network, computer systems and production scheduling, the hardware support function responsible for installation and maintenance of hardware, and an operations support function responsible for disk and tape support, maintenance and back-up of data and software.

The stated internal control objective and control procedures included in this report apply to XYZ operations as they relate only to timesharing services. Specifically excluded from this report are controls within individual systems, controls executed at customer premises and other services provided by XYZ, including data conversion services, custom application development and facilities management.

The effectiviness of control procedures performed by customers of XYZ should also be considered as part of the overall system of internal control relating to processing performed at the XYZ data centre.

Stated Internal Control Objective
The data processing environment at the XYZ data centre is secure and the integrity of processing is maintained.

Control Procedures

1 Segregation of functions exists for computer operations, systems support, hardware support, applications development and administrative functions.

2 Physical access to computer facilities, software and documentation is restricted and monitored.

3 Logical access security to prevent inadvertent or unauthorized access to systems software, application programs and data exists and is monitored.

4 System software changes and enhancements are subject to authorization and testing prior to implementation.

5 An environmentally controlled facility exists for the operation of data processing equipment.

6 Off-site hardware exists and file back-ups are maintained to enable execution of the disaster recovery plan.

7 Data centre operations, including the communications network, are monitored and problems identified are resolved on a timely basis.

10 Ook wel normen genoemd. Een eis kan worden beschouwd als iets waaraan moet zijn voldaan, en een norm als iets waaraan kan worden getoetst. In de regel vallen eisen en normen samen.
Een eis wordt ook wel een criterium of doelstelling genoemd. In dit artikel worden eis, norm, criterium en doelstelling als synoniem beschouwd.

Stated Internal Control Objective
Logical access is restricted to prevent inadvertent or unauthorized access to systems software, application programs and data.

Control Procedures

3.1 Procedures exist to ensure all accesses are authorized.

3.2 All authorized personel are issued unique user identification codes and are responsible for maintaining the corresponding passwords.

3.3 Access control software is implemented to restrict access and report violations of logical security.

3.4 Access violation reports are reviewed on a timely basis and followed-up.

3.5 Network transmissions originate from pre-determined terminal locations. Dial-up access is restricted.

3.6 Utilities identified as having special capabilities are restricted in their use and usage is monitored and justified.

Voorbeeld 2. Deel van detailbijlage bij TPM.

componenten, zoals organisatie, database en computersysteem, en dynamische activiteiten, zoals systeemontwikkeling, databasebeheer en functiebeheer ([NIVR89]), of in structuur, proces, produkt en middel (zie bijvoorbeeld [Kock92]).

Een sterk punt van vooral de Amerikaanse benadering is het maken van onderscheid tussen de verantwoordelijkheid van de service-organisatie en van de user-organisatie. Goed beschouwd is de service-auditor niet in staat een uitspraak te doen over bijvoorbeeld de betrouwbaarheid van de verwerking van een informatiesysteem bij een service-organisatie zonder hierbij tevens de handmatige toepassingscontroles bij de user-organisatie te betrekken. Volgens de Amerikaanse voorschriften moeten de controledoelstellingen ofwel zodanig worden geformuleerd dat de service-organisatie deze zelfstandig kan bereiken, of moet worden aangegeven welke controles additioneel door de user-organisatie moeten worden uitgevoerd opdat de doelstellingen worden gehaald.
[AICP87][11] geeft als voorbeeld de volgende controledoelstelling:
'Er moet redelijke zekerheid bestaan dat cliëntgegevens na invoer beschermd zijn tegen ongeautoriseerde of onopzettelijke wijziging.'

De service-organisatie zal beschikken over een systeem voor logische toegangsbeveiliging waarmee deze bescherming kan worden ondersteund. Maar de service-organisatie is hierbij afhankelijk van maatregelen die de user-organisatie moet treffen, zoals met betrekking tot het toekennen, wijzigen en intrekken van bevoegdheden.

Nauwkeuriger geformuleerd resulteert een controledoelstelling die wel door de service-organisatie kan worden bereikt:
'Er moet redelijke zekerheid bestaan dat cliëntgegevens na invoer beschermd zijn tegen ongeautoriseerde of onopzettelijke wijziging door:
- personeel van de service-organisatie;
- andere cliënten van de service-organisatie;
- ander personeel van de user-organisatie dan dat de cliënt heeft geautoriseerd.'

Indien de controledoelstellingen zodanig zijn geformuleerd dat zij uitsluitend (mede) kunnen worden bereikt door controlemaatregelen die de user-organisatie moet treffen, moet dit volgens SAS 70 in de 'scope paragraph' en 'opinion paragraph' van de TPM worden vermeld (zie voorbeeld 3 in de paragraaf TPM).

Het opstellen van (algemene) kwaliteitseisen en het (laten) vastleggen in de service level agreement is de uiteindelijke verantwoordelijkheid van de user-organisatie, terwijl het treffen van maatregelen om hieraan te voldoen tot de verantwoordelijkheid van de service-organisatie behoort.
In zijn algemeenheid kan niet worden aangegeven wie, door het formuleren van concrete normen, de vertaalslag zou moeten maken van algemene kwaliteitseisen naar maatregelen. De normen kunnen afkomstig zijn van een user-organisatie of user group, de service-organisatie, een toezichthoudende instantie of een andere bron. Bij het opstellen van de normen kan de service-auditor een ondersteunende rol vervullen. SAS 70 schrijft voor dat in de scope-paragraaf van de TPM wordt vermeld door wie de normen zijn gespecificeerd (zie voorbeeld 3).

Diepgang

Met diepgang wordt in dit verband gedoeld op de vraag of de interne-controlemaatregelen in opzet, opzet en bestaan, dan wel opzet en werking worden onderzocht. De opzet heeft betrekking op het ontwerp van de maatregelen, het bestaan betreft de daadwerkelijke uitvoering van de maatregelen op een bepaald moment, en de werking is het bestaan gedurende een zekere periode.

In NIVRA 53 is getracht deze begrippen, die tot het auditorsjargon behoren en door de lezer van een

11 *[AICP87] is overigens nog gebaseerd op SAS 44, dat inmiddels is vervangen door SAS 70. In verband hiermee wordt [AICP87] momenteel herzien.*

auditorsrapport niet altijd worden doorgrond, te vervangen door het begrippenpaar statisch en dynamisch. Onderzoek van een statisch object, zoals een informatiesysteem, houdt een opzetbeoordeling in, en onderzoek van een dynamisch object, zoals het onderhouden van een informatiesysteem, impliceert een beoordeling van de werking.
Deze poging lijkt in de praktijk niet te zijn geslaagd, hetgeen met het oog op de internationaal gebruikelijke terminologie wel zo goed is.

Internationaal (bijvoorbeeld [AICP87], [AICP92], [Widd90], [IAPC92]) wordt gewoonlijk onderscheid gemaakt tussen de volgende typen onderzoeken:
- onderzoeken naar opzet en bestaan (aangeduid als 'type 1' of 'type A');
- onderzoeken naar opzet en werking ('type 2' of 'type B');
- overige, waaronder onderzoeken naar de opzet van een informatiesysteem.

Type 2-onderzoeken volgens de richtlijnen van SAS 44, die nu door SAS 70 is vervangen, hadden gewoonlijk betrekking op een tamelijk korte periode, in de orde van enkele weken. In Nederland zou dan waarschijnlijk van een onderzoek naar opzet en bestaan (type 1) zijn gesproken. De verwachting bestaat dat de opvolger van [AICP87], die wordt vervangen naar aanleiding van het uitbrengen van SAS 70, een langere periode zal voorschrijven, bijvoorbeeld minimaal een kwartaal of een halfjaar.

Beperking van de diepgang van de TPR op grond van subjectieve verhinderingen is onder voorwaarden geen bezwaar.

NIVRA 53 noemt nog enkele andere factoren die van invloed zijn op de diepgang van het onderzoek:
- de oogmerken van de opdrachtgever;
- het type oordeel;
- het beschikbare budget;
- de lengte van de onderzoeksperiode;
- de deskundigheid van degene die het onderzoek uitvoert;
- de arbeid benodigd voor het formuleren van normen.

De meeste hiervan behoren tot wat in de accountancy wordt genoemd de subjectieve verhinderingen. Beperking van de diepgang van de TPR op grond van subjectieve verhinderingen (geen budget, geen deskundigheid) is op zichzelf geen bezwaar, mits uiteraard de opdrachtgever hiermee akkoord gaat, er geen wettelijke bepalingen of andere richtlijnen zijn die zich hiertegen verzetten, en mits de consequenties hiervan toereikend worden omschreven in de scope- en oordeelparagraaf van de TPM.
Bij diepgang kan ook worden gedacht aan de mate waarin details of uitzonderingssituaties in de TPR worden betrokken. Bijvoorbeeld: van een factureringssysteem wordt wel de verwerking van routinematige transacties onderzocht, maar blijft de verwerking van bijzondere transacties, zoals creditnota's, pro forma nota's voor monster- en zichtzendingen en doorbelastingen van personeelsverkopen, buiten beschouwing. In de praktijk worden voor onderzoeken met een beperkte diepgang volgens deze interpretatie termen gebruikt als:
- 'globaal' of 'beknopt' onderzoek, onderzoek 'in hoofdlijnen';
- tegenwoordig vooral: 'quick scan', 'quick review', 'quick assessment'.

Bij een onderzoek van de toepassingscontroles van een (financieel) informatiesysteem (operationeel of in ontwikkeling) kan de beperking relatief eenvoudig worden geconcretiseerd in termen van financieel belang. Bij een onderzoek van de algemene computercontroles is dit moeilijk.
Voor quick scan-achtige onderzoeken bestaan (internationaal en nationaal) nauwelijks of geen beroepsvoorschriften of -richtlijnen. Dit hangt samen met het feit dat voor onderzoeken van interne controle geen concreet uitgewerkt materialiteitsconcept beschikbaar is (zie ook de paragraaf over oordeelvorming).

FASE 3, PLANNING EN UITVOERING

De planningsfase omvat de gebruikelijke activiteiten bij het uitvoeren van een audit. Controletechnieken die bij het uitvoeren van een TPR worden toegepast, zijn inlichtingen van de gecontroleerde, bijvoorbeeld door middel van interviews en enquêtes, kennisneming van documentatie, zoals beschrijvingen en output, en directe waarnemingen.

Vooral bij een onderzoek naar de werking doet de vraag zich voor hoeveel en welke controles moeten worden uitgevoerd om redelijke zekerheid[12] te verkrijgen dat de interne-controlemaatregelen werken conform de opzet.
Uit de accountancy is het risicomodel bekend, waarin een relatie wordt gelegd tussen auditrisico (AR), inherent risico (IR), interne-controlerisico (ICR) en ontdekkingsrisico (OR). Dit model geeft een indicatie voor aard en omvang van de uit te voeren controlewerkzaamheden, maar is niet zonder meer toepasbaar op onderzoeken van de interne controle. Het model gaat uit van de controle van gegevens (als controle-object), waarbij de interne controle (als controlemiddel) zekerheid kan toevoegen over de betrouwbaarheid hiervan. Bij een TPR is (uitsluitend) de interne controle object van onderzoek, waardoor met name AR en OR een andere inhoud krijgen. Theorievorming op dit punt verkeert nog in een pril stadium.

De TPR moet erop zijn gericht vast te stellen dat er geen tekortkomingen bestaan in de interne controle van een zodanige ernst dat zij een bepaalde kri-

12 *De 'redelijke zekerheid' heeft hierbij geen betrekking op het bereiken van interne-controledoelstellingen, maar op het vaststellen dat er geen tekortkomingen bestaan.*

tieke grens overschrijden. In de accountancy is voor dit criterium het materialiteitsconcept ontwikkeld, dat echter evenmin direct toepasbaar is op onderzoeken van de interne controle. Weliswaar zou aansluiting kunnen worden gezocht bij dit concept als de TPR is gericht op het aspect betrouwbaarheid, maar voor andere kwaliteitsaspecten, zoals continuïteit, is dit niet zo eenvoudig. Bovendien zullen de klanten van de service-organisatie verschillende materialiteitscriteria hanteren.

In [Widd90] wordt daarom voorgesteld aansluiting te zoeken bij het vermogen van de service-organisatie om uit de financiële reserves of via een aansprakelijkheidsverzekering schade op te vangen die het gevolg is van falen van de interne controle waarop de TPR betrekking heeft. Deze benadering biedt zeker perspectief, maar behoeft verdere uitwerking.

FASE 4, OORDEELVORMING

Bij een type 1-onderzoek heeft het oordeel van de service-auditor betrekking op de vraag of de opzet van de maatregelen van interne controle voldoende zekerheid geeft (internationaal: 'redelijke zekerheid', of 'redelijke, maar geen absolute zekerheid') dat aan de gestelde kwaliteitseisen kan worden voldaan (mits de maatregelen worden uitgevoerd), en of de maatregelen daadwerkelijk worden uitgevoerd. Bij een type 2-onderzoek moet bovendien een oordeel worden gegeven over de voortdurend goede werking.
In deze paragraaf wordt ingegaan op mogelijke oordelen, waarbij, vooruitlopend op de paragraaf TPM, in enkele gevallen wordt aangegeven hoe hierover kan worden gerapporteerd.

Goedkeurend oordeel
Indien geen materiële tekortkomingen zijn geconstateerd of materiële onderzoeksonzekerheden (hoe dan ook gedefinieerd) zijn blijven bestaan, heeft het oordeel een goedkeurende strekking. De Amerikaanse en Canadese beroepsrichtlijnen schrijven voor dat het oordeel positief wordt verwoord, dus geen 'negative assurance'.

Bij een goedkeurend oordeel kan sprake zijn van niet-materiële tekortkomingen, dat wil zeggen tekortkomingen die niet van zodanige ernst zijn dat zij de strekking van het oordeel beïnvloeden.
Het vermelden van niet-materiële tekortkomingen, evenals aanbevelingen om tekortkomingen op te heffen, wordt in [Widd90] afgeraden. Het verdient de voorkeur deze in een separate brief op te nemen. Wel kunnen aanbevelingen worden opgenomen met betrekking tot de interne-controlemaatregelen die door de user-organisaties moeten worden uitgevoerd.

Goedkeurend oordeel met beperking
Een goedkeurend oordeel met beperking (ook wel voorbehoud genoemd[13] moet worden gegeven als sprake is van een materiële tekortkoming en/of een materiële onderzoeksonzekerheid. Tekortkomingen kunnen betrekking hebben op:
- de opzet: maatregelen zijn afwezig of onvoldoende effectief;
- het bestaan: maatregelen zijn niet geïmplementeerd;
- de werking: maatregelen worden niet bij voortduring effectief uitgevoerd.

Het wegen van tekortkomingen in de werking vereist vakkundig oordeel.

Vooral het wegen van tekortkomingen in de werking vereist vakkundig oordeel. De tests die de service-auditor heeft uitgevoerd, zullen betrekking hebben gehad op een (niet-mathematische) steekproef van interne-controlemaatregelen; voor het extrapoleren van één of meer tekortkomingen hierin bestaan geen mathematische modellen. Bij de weging is bijvoorbeeld van belang of de maatregel van interne controle handmatig of geautomatiseerd is. Een fout in een geprogrammeerde controle is gezien het repeterend karakter ernstiger dan het enkele malen niet effectief uitvoeren van een handmatige controle.

Het is denkbaar dat een tekortkoming wordt gecompenseerd door een maatregel die buiten de scope van het onderzoek valt. Voor de service-organisatie en de service-auditor bestaan dan verschillende alternatieven:
- de compenserende maatregel onvermeld laten (met handhaving van de beperking);
- nader onderzoek uitvoeren naar de compenserende maatregel en de uitkomst hiervan in het oordeel betrekken (met handhaving van de oorspronkelijke beperking);
- scope van het onderzoek en beschrijving van het onderzoeksobject aanpassen. Oordeel opnieuw bezien na aanvullend onderzoek.

Vaak zal het voorkomen dat geconstateerde tekortkomingen al tijdens het onderzoek worden verholpen, of dat acties met dat doel in gang worden gezet. Dit kan worden vermeld in het oordeel, met handhaving van de oorspronkelijke beperking.

Een materiële onderzoeksonzekerheid kan zich voordoen als de service-organisatie een deel van de dienstverlening waarop het onderzoek betrekking heeft gehad, weer heeft uitbesteed aan een andere service-organisatie, en de service-auditor zich geen oordeel heeft kunnen vormen over de interne controle aldaar. Er is hierbij sprake van een objectieve verhindering.
Een alternatief voor een oordeel met beperking is in dit geval het aanpassen van de scope van het onderzoek.
In NIVRA 53 wordt de mogelijkheid van een voor-

13 *De GBR-1994 ([NIVR94]) schrijven voor dat de bewoordingen 'onder voorbehoud' worden gebruikt bij onderzoeksonzekerheden, en 'met uitzondering van' bij tekortkomingen ('bedenkingen' genoemd).*

behoud uitgesloten, met als belangrijk motief dat het wegen van een voorbehoud een uiterst moeilijke zaak is. Dit moge zo zijn, maar daarom hoeft de uitdaging nog niet uit de weg te worden gegaan.

Oordeelonthouding
Van een oordeelonthouding is sprake als de auditor niet tot een totaaloordeel kan komen met betrekking tot de gestelde criteria voor het onderzoeksobject ([NIVR89]). NIVRA 53 geeft als voorbeeld een kleinschalige omgeving waarin geen functiescheiding bestaat tussen systeemontwikkeling en operating. Op bedrijfseconomische gronden kan deze tekortkoming niet op korte termijn worden opgeheven.
Een nadere uitleg over de omstandigheden die de auditor kunnen verhinderen tot een totaaloordeel te komen, wordt in NIVRA 53 niet gegeven. Hierbij kan worden opgemerkt dat het gegeven voorbeeld in NIVRA 53 wat ongelukkig is gekozen. Het voorbeeld is rechtstreeks overgenomen uit de accountancy, waarbij de interne-controlemaatregel van functiescheiding voorwaarde is om te komen tot een goedkeurend oordeel over de jaarrekening, als onderzoeksobject. Bij een TPR is echter de interne controle onderzoeksobject, zodat in het voorbeeld niet zozeer sprake is van een onderzoeksonzekerheid, als wel van een tekortkoming in het onderzoeksobject.

Een oordeelonthouding impliceert een combinatie van onderzoeksonzekerheden van meer dan materiële betekenis. In de accountancy wordt dit 'wezenlijke' betekenis genoemd.

In [Widd90] wordt weliswaar melding gemaakt van de mogelijkheid van een oordeelonthouding, maar deze wordt niet verder uitgewerkt. In de Amerikaanse richtlijnen wordt de mogelijkheid niet genoemd.

Afkeurend oordeel
Bij een afkeurend oordeel is de service-auditor tot de slotsom gekomen dat het onderzoeksobject niet aan de gestelde criteria voldoet ([NIVR89]). Er is in termen van de accountancy sprake van een combinatie van tekortkomingen van wezenlijke betekenis.
Voor de Amerikaanse en Canadese richtlijnen geldt weer dat de mogelijkheid hooguit wordt genoemd, maar niet wordt uitgewerkt.

TPM

Door middel van de TPM brengt de service-auditor verslag uit van de uitkomsten van zijn onderzoek. De TPM zal minimaal de beschrijving van het oordeel inhouden. Omtrent de verdere inhoud van de TPM is in Nederland nog weinig geregeld.

In deze paragraaf zal worden ingegaan op enkele aandachtspunten bij een TPM, aan de hand van een tweetal voorbeelden.

TPM volgens SAS 70

De beroepsvoorschriften in de VS zijn beduidend verder ontwikkeld dan in Nederland. Een voorbeeld van een TPM volgens de huidige Amerikaanse voorschriften is weergegeven in voorbeeld 3, waarbij de eerste twee kolommen ter toelichting zijn toegevoegd door de auteur van dit artikel.

Oordeel
De strekking van het oordeel in het voorbeeld is goedkeurend met beperkingen (tussen vierkante haken). Deze beperkingen hebben betrekking op:
- een controlemaatregel waarvan de opzet niet goed is beschreven;
- een controlemaatregel die in opzet of bestaan niet effectief is;
- controlemaatregelen die door de user-organisaties moeten worden uitgevoerd.

Bijlagen
SAS 70 bevat geen concrete richtlijnen omtrent de bijlagen bij de TPM. Naar verwachting zal de opvolger van [AICP87] de volgende inhoud voorschrijven (in lijn met de bestaande voorschriften):
- een beschrijving van de dienstverlening en de interne-controlestructuur, opgesteld door of onder verantwoordelijkheid van de service-organisatie. Deze bijlage dient te bevatten:
  - algemene beschrijving van de service-organisatie en haar dienstverlening;
  - belangrijkste elementen van de controle-omgeving;
  - interne-controledoelstellingen en -maatregelen;
  - interne controles die door de user-organisaties moeten worden uitgevoerd;
- aanvullende informatie van de service-auditor over de uitgevoerde tests;
- eventuele aanvullende informatie van de service-organisatie.

Vermelding controledoelstellingen
In de bijlagen bij de Amerikaanse TPM worden de interne-controledoelstellingen (tevens toetsingsnormen) concreet weergegeven. Voor de Nederlandse situatie is dit niet zo vanzelfsprekend. In [NIVR82] werd geconstateerd dat er nog geen sprake is van vaste, uitgekristalliseerde normen, en in deze situatie is nog weinig verandering gekomen. NIVRA 26 vermeldt hierover verder het volgende:
'Het zou dan ook voor de hand liggen dat de accountant de door hem aangelegde normen expliciet vermeldt in of bij zijn mededeling. Een voor iedere lezer begrijpelijke beschrijving is echter praktisch zo moeilijk op te stellen dat in dit rapport wordt gepleit in plaats daarvan in een bijlage bij de mededeling het aangetroffen stelsel aan maatregelen en procedures te omschrijven. Uit de beschrijving kan de lezer dan afleiden welk concreet stelsel door de accountant is beoordeeld.'

In NIVRA 53 wordt op deze problematiek niet ingegaan.

Scope paragraph.	Applications, services or other aspects of the service organization covered.	We have examined the accompanying description of the Example application of XYZ Service Organization.
	Purpose of service auditor's engagement.	Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of XYZ Service Organization's policies and procedures that may be relevant to a user organization's internal control structure, (2) the control structure policies and procedures included in the description were suitably designed to achieve the control objectives specified in the description, if those policies and procedures were complied with satisfactorily [and user organizations applied the internal control structure policies and procedures contemplated in the design of XYZ Service Organization's policies and procedures], and (3) such policies and procedures had been placed in operation as of _____.
	Party specifying the control objectives.	The control objectives were specified by _____.
	Scope and nature of service auditor's procedures.	Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.
	Disclaimer of opinion on the operating effectiviness of the policies and procedures.	We did not perform procedures to determine the operating effectiviness of policies and procedures for any period. Accordingly, we express no opinion on the operating effectiviness of any aspects of XYZ Service Organization's policies and procedures, individually or in the aggregate.
	[If description is inaccurate or insufficient.]	[The accompanying description states that XYZ Service Organization uses operator identification numbers and passwords to prevent unauthorized access to the system. Based on inquiries of staff personel and inspections of activities, we determined that such procedures are employed in Applications A and B but are not required to access the system in applications C and D.]
	[If there are significant deficiences in the design or operation of the service organization's policies and procedures.]	[As discussed in the accompanying description, from time to time the Service Organization makes changes in application programs to correct deficiences or to enhance capabilities. The procedures followed in determining whether to make changes, in designing the changes, and in implementing them do not include review and approval by authorized individuals who are independent from those making the changes. There are also no specified requirements to test such changes or provide test results to an authorized reviewer prior to implementing the changes.]
Opinion paragraph.	The service auditor's opinion.	In our opinion, [except for the matter referred to in the first of the two preceding paragraphs,] the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's policies and procedures that had been placed in operation as of _____. Also in our opinion, [except for the deficiency referred to in the second of the two preceding paragraphs,] the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily [and user organizations applied the internal control structure policies and procedures contemplated in the design of XYZ Service Organization's policies and procedures].
Other separate paragraphs.	Inherent limitations ('uncertainty paragraph').	The description of policies and procedures at XYZ Service Organization is as of _____ and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiviness of specific policies and procedures at the Service Organization is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.
	Parties for whom the report is intended.	This report is intended solely for use by the management of XYZ Service Organization, its customers, and the independent auditors of its customers.

Voorbeeld 3. TPM volgens SAS 70 inzake opzet en bestaan ([AICP92]).

Anno 1995 bestaan er in Nederland nog geen voorschriften of richtlijnen aangaande het opnemen van concrete eisen bij een TPM. Wel kan worden geconstateerd dat in EDP-auditrapporten in toenemende mate de toetsingsnormen worden vermeld.

Uitgevoerde tests
In Nederland is het niet gebruikelijk dat een beschrijving wordt opgenomen van aard, omvang en tijdstip van de controlewerkzaamheden die de service-auditor heeft verricht. De Amerikaanse benadering, die voorschrijft dat de service-auditor informatie verschaft over de uitgevoerde tests, legt een grote verantwoordelijkheid bij de lezer van het rapport, die geacht wordt op grond van de verschafte detailinformatie zelfstandig tot een oordeel te kunnen komen.
In Canada was het eveneens gebruikelijk deze informatie op te nemen, maar gelet op de toenemende standaardisatie op het gebied van onderzoeksuitvoering en rapportage, wordt thans aanbevolen een beschrijving van de uitgevoerde tests achterwege te laten.

Verspreiding
De verspreiding van de TPM blijft in het Amerikaanse voorbeeld beperkt tot een kleine groep, maar vaak worden potentiële klanten (alsmede toezichthoudende instanties) aan deze groep toegevoegd, waardoor het rapport vrijwel openbaar wordt. Hierbij moet echter worden bedacht dat de service-organisatie weliswaar een commercieel belang heeft bij verspreiding op grote schaal - gesteld dat de strekking van het oordeel goedkeurend is - maar dat in de bijlagen van het rapport, die een onlosmakelijk geheel vormen met de TPM, detailinformatie is opgenomen over de te bereiken controledoelstellingen en de getroffen maatregelen, waaronder beveiligingsmaatregelen. Deze informatie is niet alleen concurrentiegevoelig, maar biedt ook misbruikmogelijkheden aan kwaadwillenden.

Openbaar gemaakte TPM (onderdeel van jaarverslag)

In voorbeeld 4 is een openbaar gemaakte TPM (met beperking) weergegeven. Een dergelijke mededeling zonder nadere beschrijving van het onderzoeksobject heeft als bezwaar dat het voor de user-organisatie moeilijk is de reikwijdte van de TPM en de eventuele consequenties voor haar interne-controlestructuur te beoordelen, temeer daar er sprake is van ruimte voor verbetering bij de service-organisatie.

Voorbeeld 4. Security audit statement S.W.I.F.T. 1992 Annual Report.

Scope paragraph.	Aspects covered.	We were retained to review the security controls set up by the Society for Worldwide Interbank Financial Telecommunications s.c. (S.W.I.F.T.) to assure the availability of the system and to maintain the integrity and confidentiality of sensitive information related to the S.W.I.F.T. network and of messages after submission to and before dispatch from S.W.I.F.T. Access Points.
	Scope and nature of auditor's procedures.	Migration to SWIFT II has been completed in August 1992. The security audit was carried out in October and November 1992, and was based predominantly on evaluation of information obtained by review of documented procedures and other relevant documentation, observation of procedures, and interviews with S.W.I.F.T. staff.
	Inherent limitations (explanation of the concept adequate).	The level of protection that is required must be in line with the legitimate expectations of S.W.I.F.T. users. A computer network of the size and complexity of SWIFT II cannot expected to be completely without risks and additionally, global system security relies on the implementation by S.W.I.F.T. users of the security procedures defined in the User Handbooks. The range and extent of security controls that we deem necessary takes into account the required system efficiency, the amplitude of risks, and the cost and difficulty to implement protective measures.
	Weaknesses.	Our detailed report to the management identifies some areas where there is still room for amelioration and we have made recommendations to this effect. Implementation of these recommendations is already in progress or will commence in 1993, according to well-defined plans.
Opinion paragraph.	Auditor's opinion.	With those observations in mind, in our opinion the security controls established by S.W.I.F.T. are adequate for the class of service provided by the S.W.I.F.T. network.

OVERIGE AANDACHTSPUNTEN

In deze paragraaf worden enkele bijzondere aandachtspunten bij een TPR en TPM behandeld.

Letter of representation
De Amerikaanse en Canadese richtlijnen schrijven voor dat van het management een representation letter wordt verkregen voordat de TPM wordt uitgebracht. In deze brief, met dezelfde datum als de TPM, moet het management zijn verantwoordelijkheid bevestigen voor het instellen en onderhouden van een adequate interne-controlestructuur, en voor het verschaffen van alle relevante informatie aan de service-auditor. Voorbeeld 5 bevat een representation letter volgens [AICP87].

Ketenuitbesteding
Het is denkbaar dat de service-organisatie een deel van de dienstverlening waarop de TPM betrekking heeft, weer heeft uitbesteed aan een andere service-organisatie. Zoals [DIBI94] ook al aangeeft doet deze situatie zich vooral voor bij netwerkservices, waarbij de service-organisatie in veel gevallen basisdiensten afneemt van PTT Telecom. De service-auditor van de uitbestedende service-organisatie kan in deze situatie eventueel gebruik maken van een TPM van de service-auditor van de onderaannemer (overigens niet van toepassing bij het genoemde voorbeeld). Vragen die hierbij opkomen zijn:

- Moet de service-auditor van de uitbestedende organisatie hiervan melding maken in zijn TPM en zo ja, op welke wijze?
- Welke aanvullende werkzaamheden moet de service-auditor van de uitbestedende service-organisatie eventueel verrichten, zoals overleg met de service-auditor van de onderaannemer, het opvragen van nadere informatie en/of dossier-review?

In de binnenlandse en buitenlandse beroepsrichtlijnen is hieromtrent nog weinig of niets geregeld.

HET GEBRUIK VAN EEN TPM

Directe belanghebbenden van een TPM zijn user-organisaties, user-auditors en toezichthoudende instanties. Een TPM kan aan user-organisaties en toezichthoudende instanties redelijke zekerheid verschaffen dat de uitbestede IT-services en daarmee de bedrijfsprocessen die hiervan afhankelijk zijn, aan de gestelde kwaliteitseisen voldoen.

De user-auditor kan een TPM gebruiken bij de controle van de jaarrekening, voor het verkrijgen van inzicht in het stelsel van interne-controlemaatregelen en van controlebewijs.

In deze paragraaf wordt kort ingegaan op enkele aandachtspunten bij het gebruik van een TPM. Voor een meer uitvoerige behandeling wordt verwezen naar de aangehaalde literatuur (met name [AICP87] en [Widd90]).

Service-auditor
Behalve in bijzondere situaties, bijvoorbeeld in het geval dat de Wet computercriminaliteit of het

Voorbeeld 5. Representation letter (ontleend aan [AICP87]).

We are writing at your request to confirm our understanding that your review of our description of the control structure policies and procedures of XYZ Service Organization data center and its Example application was made to enable you to evaluate whether the control structure policies and procedures were suitably designed to achieve the control objectives specified in the report. We further understand that your review included such procedures as you considered necessary to clarify your understanding of the control structure policies and procedures that we described.

In connection with your review, we confirm that we have supplied you with all significant, relevant information of which we are aware, and we confirm that we have fairly and accurately described the control structure policies and procedures of the XYZ Service Organization data center as well as its Example application. We understand that your review related only to information that we provided, and it may not have resulted in identification of all internal accounting controls. In addition, we acknowledge that we are responsible for the following:

- Establishing and maintaining an appropriate system of internal control relating to the information processing that is performed for users.
- Disclosing to you any significant system changes that have occurred since your last examination.
- Disclosing to you any irregularities by service-center management or employees who have significant roles in the system or internal controls over information processed for user organizations.

We further understand that your report is intended solely for use by the management of XYZ Service Organization, its customers, and the independent auditors of its customers.

We will not reproduce or incorporate your opinion or supplemental information without your specific written permission.

DNB-memorandum van toepassing is, bestaat er geen wet- en regelgeving aangaande de benodigde kwalificaties om een TPR uit te voeren. Bij het beoordelen van de waarde van een TPM zijn vooral van belang de deskundigheid, gewaarborgd door bijvoorbeeld opleidings- en permanente-educatievereisten van beroepsorganisaties, de kwaliteitsborgingsmaatregelen en de onafhankelijkheid ten opzichte van de auditee (service-organisatie).

Meest cruciaal voor het gebruik van de TPM is de strekking van het oordeel.

Onderzoeksobject
Het onderzoeksobject betreft de dienstverlening en het bijbehorende stelsel van interne-controlemaatregelen. Het is denkbaar dat de TPM niet de gehele dienstverlening bestrijkt, waardoor individuele user-organisaties met de TPM niet of nauwelijks zijn gebaat.

In het onderzochte stelsel van interne-controlemaatregelen kunnen talloze beperkingen zijn aangebracht, die eveneens het nut van de TPM voor een individuele user-organisatie en user-auditor kunnen beperken, bijvoorbeeld:
- de TPM heeft slechts betrekking op de algemene computercontroles en niet op de voor een individuele user-organisatie kritieke toepassingscontroles;
- van een service-organisatie met meerdere computercentra is slechts een enkel centrum in de TPR betrokken.

Kwaliteitsaspect en kwaliteitseisen
Het is denkbaar dat de TPM betrekking heeft op een kwaliteitsaspect dat voor een individuele user-organisatie minder relevant is, of dat de gestelde kwaliteitseisen zijn gebaseerd op de middelmaat, terwijl een individuele user-organisatie in hoge mate afhankelijk is van het kwaliteitsaspect.

Diepgang
TPM's inzake opzet of opzet en bestaan zijn vooral informatief, hetgeen voor user-organisaties voldoende kan zijn. Een periodieke doorlichting van de service-organisatie kan voldoende zekerheid geven dat de kwaliteit van de dienstverlening is gewaarborgd.

Ook voor de user-auditor die belast is met de jaarrekeningcontrole zijn dergelijke TPM's informatief. De TPM geeft hem inzicht in het totale stelsel van interne controle en ondersteunt hem bij het beoordelen van de interne-controlemaatregelen die de user-organisatie moet uitvoeren. Als de user-auditor echter wil of moet steunen op de interne controles die de service-organisatie verricht, is volgens de geldende beroepsvoorschriften in binnen- en buitenland een 'type 2'-mededeling (inzake opzet en werking) vereist. Ook dan kan de effectiviteit van het controlebewijs beperkt zijn, door een te kort tijdsinterval of doordat de TPM een verkeerde periode bestrijkt vanuit het oogpunt van de jaarrekeningcontrole bij de user-organisatie.

Oordeel
Meest cruciaal voor het gebruik van de TPM is natuurlijk de strekking van het oordeel. Het behoeft geen betoog dat een goedkeurend oordeel zonder beperkingen het meest waardevol is voor het gestelde doel: het verschaffen van (positieve) zekerheid. Is de strekking anders dan moeten de redenen hiervoor worden geanalyseerd om te bepalen wat de consequenties zijn voor bijvoorbeeld de uit te voeren interne controles door de user-organisatie, het uitbestedingscontract of de jaarrekeningcontrole bij de user-organisatie.

SAMENVATTING EN CONCLUSIE

De opzienbarende ondergang van een groot aantal ondernemingen in de afgelopen jaren heeft regelgevende instanties in binnen- en buitenland ertoe aangezet nadere voorschriften en richtlijnen uit te vaardigen aangaande het bestuur van en de interne controle bij organisaties. De verantwoordelijkheid van het management voor interne controle wordt benadrukt, en de opdracht aan de externe accountant wordt in sommige gevallen uitgebreid tot het attesteren van de beweringen van het management omtrent de kwaliteit en de werking van de interne controle. Interne controle is hierbij niet alleen gericht op de betrouwbaarheid van de financiële verslaggeving, maar ook op de effectiviteit en efficiëntie van de bedrijfsprocessen en de naleving van wet- en regelgeving.

Los hiervan gaat de ontwikkeling dat organisaties delen van de geautomatiseerde gegevensverwerking uitbesteden, nog steeds verder. De uitbestedende organisaties en de fungerende auditors hebben behoefte aan waarborgen dat de interne controle bij de service-organisatie van voldoende niveau is, een behoefte die wordt versterkt door bovengenoemde regelgeving.

Buitenlandse en internationale beroepsorganisaties van auditors hebben in het licht van deze ontwikkelingen hun voorschriften en richtlijnen inzake mededelingen ten behoeve van derden over onderzoeken van de interne controle bij service-organisaties eveneens aangescherpt.

In dit artikel is ingegaan op de scope-afbakening, onderzoeksuitvoering, oordeelvorming en rapportage bij een third party review, waarbij een vergelijking is gemaakt tussen de desbetreffende binnenlandse en buitenlandse beroepsvoorschriften en -richtlijnen. Tevens is kort stilgestaan bij de gebruiksmogelijkheden van een TPM. Het artikel had

het karakter van een terreinverkenning, waarbij vele witte plekken op de kaart werden gesignaleerd.

De conclusie mag luiden dat er internationaal nog veel research nodig is om de witte plekken op de kaart van het verkende terrein in te vullen, bijvoorbeeld op het gebied van het risicomodel en het materialiteitsconcept. Ook mag worden geconcludeerd dat in Nederland nog veel werk moet worden verzet om te komen tot beroepsvoorschriften die de vergelijking met de Amerikaanse en Canadese kunnen doorstaan.[14]

LITERATUUR

[AICP87] American Institute of Certified Public Accountants, *Audits of Service-Center-Produced Records*, Audit and Accounting Guide, 1987.

[AICP92] American Institute of Certified Public Accountants, *Reports on the Processing of Transactions by Service Organizations*, Statement on Auditing Standards No. 70, 1992.

[Cadb92] Report of the Committee on the Financial Aspects of Corporate Governance ('Cadbury-rapport'), *The Code of Best Practice*, Gee, 1992.

[COSO92] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control - Integrated Framework*, 1992.

[DIBI94] Directie Interbestuurlijke Betrekkingen en Informatievoorziening, Ministerie van Binnenlandse Zaken, *Voorschrift Informatiebeveiliging Rijksdienst*, Den Haag, september 1994.

[DIBI95] Directie Interbestuurlijke Betrekkingen en Informatievoorziening, Ministerie van Binnenlandse Zaken, *Handboek Informatiebeveiliging Rijksdienst*, Den Haag, februari 1995.

[DNB88] De Nederlandsche Bank, *Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen*, 1988.

[DNB94] De Nederlandsche Bank, *Uitbesteding van de geautomatiseerde gegevensverwerking*, Considerans bij de uitbesteding van de geautomatiseerde gegevensverwerking door kredietinstellingen, 1994.

[FDIC93] Federal Deposit Insurance Corporation, *Management Responsibility for Financial Statements and Internal Control*, Section 112 of the FDIC Improvement Act (FDICIA, 1991), 1993.

[IAPC92] International Auditing Practices Committee of the International Federation of Accountants, *Audit Considerations Relating to Entities Using Service Organizations*, International Standard on Auditing 6, 1992.

[IIA91] The Institute of Internal Auditors Research Foundation, *Systems Auditability and Control Report, Module 2, Audit and Control Environment*, The Institute of Internal Auditors, 1991.

[Kock92] H.C. Kocks en J.A. Verstelle, *Kwaliteitsbeheersing bij systeemontwikkeling, De mogelijke rol van een EDP-auditor*, Informatie, jaargang 34, nr. 3, 1992.

[KPMG94] KPMG, *Handboek KPMG Audit Service*, 1994.

[NIVR82] Nederlands Instituut van Registeraccountants, *Automatisering en controle Deel IV. Mededelingen door de accountant met betrekking tot de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking*, NIVRA-geschrift nummer 26, Kluwer, 1982.

[NIVR89] Nederlands Instituut van Registeraccountants, *Automatisering en controle Deel VII. Kwaliteitsoordelen over informatievoorziening*, NIVRA-geschrift nummer 53, Kluwer, 1989.

[NIVR91] Nederlands Instituut van Registeraccountants, *Automatisering en controle Deel VIII. Privacy-bescherming; de gevolgen voor organisaties en de rol van de accountant*, NIVRA-geschrift nummer 58, Kluwer, 1991.

[NIVR94] NIVRA, *Verordening Gedrags- en Beroepsregels Registeraccountants 1994*, Nederlandse Staatscourant van 8 maart 1995 - nr. 48, in werking getreden op 10 maart 1995, vastgesteld in de bijeenkomst van de ledenvergadering op 30 november 1994.

[NNI94] Nederlands Normalisatie Instituut, *Code voor informatiebeveiliging. Een leidraad voor beleid en implementatie*, 1994.

[Nola91] R.L. Nolan, *Outsourcing, harbinger of I/S's Transformation*, Stage bij Stage, Vol.9, nr.5, 1991.

[Stee93] D. Steeman et al. (red.), *EDP-auditing en accountantscontrole*, themanummer, Compact 1993/4.

[Widd90] R.J. Widdowson, *Auditor Reports on Control Procedures at Service Organizations (Third Party Reports)*, An Audit Technique Study, The Canadian Institute of Chartered Accountants, 1990.

[Zwar91] C. de Zwart, *Nooit chaos uitbesteden: Facilities Management deel 2*, Rendement, maart 1991.

[Zwar94] H. de Zwart et al. (red.), *Handboek EDP-auditing*, Kluwer, 1994.

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.

14 Recent heeft de Commissie voor de Organisatie van de Informatievoorziening (COIV) van het NIVRA een werkgroep TPM opgestart, waaraan ook leden van de NOREA deelnemen. De Commissie Richtlijnen Accountantscontrole (CORA) zal in het najaar van 1995 richtlijn 402, Overwegingen bij controles van huishoudingen die gebruik maken van servicebureaus, uitbrengen. Deze richtlijn is een vertaling (en bewerking) van IAS 6 ([IAPC92]).

Maatwerk past informatiebeveiliging

Drs. E. Roos Lindgreen
Mw.drs. C. Schönfeld RI

De recent in Nederland geïntroduceerde Code voor Informatiebeveiliging heeft de discussie over het nut van checklists bij informatiebeveiliging weer doen oplaaien.
Het gebruik van checklists werkt kostenbesparend maar voldoet lang niet altijd. Het alternatief van de maatwerkbenadering is om op basis van classificatie en analyse een toegesneden pakket van normen en maatregelen op te stellen.
De auteurs, die zowel theoretisch als praktisch nauw betrokken zijn bij informatiebeveiliging, betogen dat de Code in essentie geen checklist is maar een leidraad om te komen tot een maatwerkoplossing, en spreken hun voorkeur uit voor deze benadering van informatiebeveiliging.

INLEIDING

Informatiebeveiliging blijft de gemoederen bezighouden. Gelukkig maar, want beveiliging is geen eenmalig vraagstuk. Technologische en organisatorische ontwikkelingen maken een voortdurende herbezinning noodzakelijk. Vanaf het begin is Compact een forum geweest voor de discussie over informatiebeveiliging en vele auteurs hebben er in de loop der jaren hun visie op uiteenlopende aspecten van dit onderwerp in gegeven.
Over het doel van beveiliging zijn de meeste auteurs het eens: informatiebeveiliging moet de organisatie behoeden voor financiële en niet-financiële risico's die samenhangen met de informatievoorziening. Maar over de wijze waarop zij in de praktijk gestalte moet krijgen, verschilt men van mening. Er lijkt zich een soort schisma in de beveiligingswereld af te tekenen. Aan de ene kant vinden we voorstanders van een zogenaamde 'maatwerk'-benadering, die ervoor pleiten om het toepassen van beveiligingsmaatregelen altijd vooraf te laten gaan door een grondig onderzoek naar de mate waarin een organisatie afhankelijk is van haar informatiesystemen en naar de bedreigingen waaraan deze systemen blootstaan. Aan de andere kant staan voorstanders van een zogenaamde 'confectie'-benadering, die het gebruik van tijdbesparende checklists en standaarden propageren. In dit artikel wordt deze vermeende controverse tussen maatwerk en confectie nader beschouwd.
De opbouw van het artikel is als volgt: aan de hand van drie stellingen beschrijven we informatiebeveiliging als een stelsel van cyclische activiteiten op zowel strategisch, tactisch als operationeel niveau. In aansluiting op eerdere artikelen in Compact ([Fijn91], [Gils94], [Giel89], [Heij91], [Kuip89], [Wely92]) zal de aandacht uitgaan naar de strategische cyclus. Deze bestaat uit drie opeenvolgende fasen, te weten:

1. analyseren en normstelling;
2. selecteren en invoeren van maatregelen;
3. controleren en evalueren.

In dit artikel krijgt de eerste fase – analyse en normstelling – de meeste aandacht, omdat de invulling van deze fase bepalend is voor het onderscheid tussen een maatwerk- of een confectiebenadering.

STELLINGEN

De behandeling van informatiebeveiliging geschiedt in dit artikel aan de hand van een raamwerk. De bouwstenen van dit raamwerk bestaan uit een drietal stellingen.

Stelling 1: Informatiebeveiliging schept keuzeproblemen.

De problematiek van informatiebeveiliging roept vragen op, die door het management moeten worden beantwoord. Tegen welke risico's treft men beveiligingsmaatregelen? Welke risico's worden willens en wetens geaccepteerd? Welke beveiligingsmaatregelen worden er ingevoerd? Welke maatregelen worden direct gerealiseerd, en welke maatregelen pas na enige tijd? Het zal duidelijk zijn dat men bij het beveiligen van informatiesystemen keuzes moet maken ([Kuip89]). Soms wordt wel eens de suggestie gewekt dat die keuzes uitsluitend zijn gebaseerd op een rationele afweging van de risico's tegen de kosten van de beveiligingsmaatregelen. In de praktijk worden ze daarnaast ook sterk beïnvloed door commerciële overwegingen, politieke motieven en menselijke emoties. Deze en andere irrationele factoren blijven in dit artikel echter buiten beschouwing.

Stelling 2: Informatiebeveiliging is cyclisch.

De onder stelling 1 genoemde keuzeproblemen keren, weliswaar in gewijzigde vorm, steeds terug en maken zo deel uit van een cyclus, die we in dit artikel 'beveiligingscyclus' zullen noemen. Deze cyclus is noodzakelijk door het feit dat de organisatie, de informatiesystemen en de technische infrastructuur voortdurend veranderen. Bovendien ontdekken zowel gebruikers als hackers regelmatig nieuwe kwetsbaarheden, die steeds sneller wereldkundig worden gemaakt. De informatiebeveiliging moet daarom steeds worden herzien ([Rain93]). Gebeurt dat niet, dan zullen de getroffen maatregelen door veroudering aan effectiviteit inboeten. Daarom kunnen we de verschillende activiteiten in het kader van informatiebeveiliging beschouwen als evenzovele cybernetische regelkringen - dat wil zeggen oneindige cycli van informeren, bijsturen en evalueren ([Wien61]).

Stelling 3: Beveiligingscycli komen voor op alle bestuurlijke niveaus in de organisatie.

De onder stelling 2 genoemde cycli treffen we op zowel strategisch, als tactisch en operationeel niveau aan. Voorbeelden daarvan zijn:

- Op strategisch niveau vindt de formulering en regelmatige bijstelling van het beveiligingsbeleid plaats ([Heij91]).

- Op tactisch niveau moeten waarborgen worden geschapen voor de scheiding tussen ontwikkel- en produktie-omgeving en moeten procedures voor bijvoorbeeld change- en problem-management worden opgesteld en geïmplementeerd.

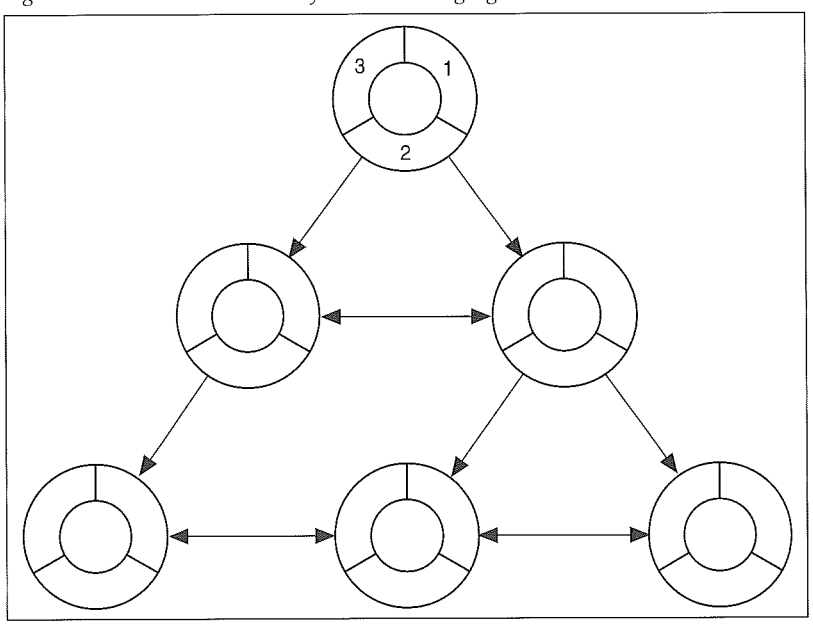
- Op operationeel niveau moeten wachtwoordprocedures worden opgesteld en toegangspermissies worden onderhouden.

Uit deze voorbeelden blijkt tevens dat informatiebeveiliging op alle niveaus verschillende eenheden en functionarissen tegelijk bezighoudt. Een goede afstemming tussen al deze partijen is essentieel. Als de verticale afstemming – het vertalen van beleid naar uitvoering – onvoldoende is, dreigt het gevaar dat de operationele beveiliging onvoldoende strookt met de strategische doelstellingen van de organisatie. Als de horizontale afstemming – regulier en incidenteel overleg tussen afdelingen – onvoldoende is, kunnen kwetsbaarheden ontstaan doordat twee verantwoordelijke eenheden een bepaalde cruciale beveiligingscyclus niet tot hun taakveld rekenen, maar er stilzwijgend van uitgaan dat de ander de verantwoordelijkheid daarvoor op zich heeft opgenomen.

Het bestuurlijk niveau waarop een beveiligingscyclus zich afspeelt, blijkt mede bepalend te zijn voor de maximale doorloopsnelheid ervan. Voor de formulering en bijstelling van beveiligingsbeleid geldt een cyclus van ongeveer drie tot vijf jaar, voor het definiëren van organisatie en procedures op tactisch niveau geldt een kortere cyclus van ongeveer één tot drie jaar. Activiteiten op operationeel niveau, zoals het opzetten en controleren van een stelsel van toegangspermissies, ten slotte kennen nog kortere cycli.

Tot zover ons raamwerk: beveiliging schept cyclische keuzeproblemen, die in verschillende verschijningsvormen op alle niveaus van de organisatie voorkomen. Dit raamwerk is schematisch weergegeven in figuur 1.

Figuur 1. Een raamwerk voor informatiebeveiliging.



ACTIVITEITEN OP STRATEGISCH NIVEAU

Op strategisch niveau kunnen we de activiteiten informeren, bijsturen en evalueren meer specifiek aanduiden als:

1. analyse en normstelling;
2. selecteren en invoeren van maatregelen;
3. controleren en evalueren aan de hand van de normen.

In dit artikel krijgen analyse en normstelling verreweg de meeste aandacht, omdat de wijze waarop deze stap wordt ingevuld karakteristiek is voor het verschil tussen maatwerk- en confectiebenadering.

Een betaalmodule is fraudegevoeliger dan een applicatie die slechts financiële overzichten bijhoudt.

Analyse en normstelling

In de eerste stap moet worden vastgesteld welke onderdelen van de informatiebeveiliging in welke mate waartegen moeten worden beveiligd. De beslisser moet hiervoor weten (a) in welke mate de organisatie *afhankelijk* is van de juiste en ongestoorde werking van de verschillende onderdelen van de informatievoorziening, en (b) in welke mate elk onderdeel onbeschermd is tegen de verstorende invloed van *bedreigingen*. Hieronder wordt ingegaan op de manier waarop deze informatie kan worden verkregen.

Afhankelijkheidsanalyse

Het bepalen van de mate waarin een organisatie afhankelijk is van de juiste en voortdurende werking van de informatiesystemen wordt hier in navolging van [Gils94] en [Rijk94] afhankelijkheidsanalyse genoemd (men gebruikt ook wel de term gevoeligheidsanalyse). De wijze waarop deze afhankelijkheid wordt bepaald, wordt in navolging van [Adam94] aangeduid met de term 'classificatie van gegevens en applicaties'. Onder classificatie wordt verstaan: de indeling van gegevens en applicaties in het licht van de verschillende relevante kwaliteitsaspecten. De in [NIVR89] opgesomde kwaliteitsaspecten worden in het kader van informatiebeveiliging veelal gecomprimeerd tot betrouwbaarheid, beschikbaarheid en vertrouwelijkheid; ook integriteit, continuïteit en exclusiviteit worden gebruikt. In de Angelsaksische literatuur spreekt men meestal van de zogenaamde CIA-aspecten: Confidentiality (vertrouwelijkheid), Integrity (betrouwbaarheid) en Availability (beschikbaarheid). Vaak zal er echter behoefte bestaan om de kwaliteitsaspecten verder uit te splitsen; vertrouwelijkheid kan men zo bijvoorbeeld toespitsen op persoonsvertrouwelijkheid en bedrijfsvertrouwelijkheid.

Het belang van de verschillende kwaliteitsaspecten verschilt per omgeving. In een militaire omgeving is 'vertrouwelijkheid' veel belangrijker dan in een commerciële omgeving, waar 'fraudebestendigheid' wellicht het meest relevant is. [Velt91] geeft aan dat deze verschillen ook een groot probleem vormen bij het gebruik van de evaluatiecriteria TCSEC en ITSEC, die in respectievelijk Amerika en Europa zijn opgesteld.

[Wely92] maakt een onderscheid tussen 'aspecten' (de hierboven genoemde CIA-aspecten) en 'beveiligingsbelangen', maar deze beveiligingsbelangen, bijvoorbeeld wettelijke eisen op het gebied van de vertrouwelijkheid, kunnen naar onze mening zonder bezwaar beschouwd worden als differentiaties van de drie genoemde hoofdaspecten.

Soms gebruikt men voor de classificatie de term 'gegevensclassificatie', hetgeen suggereert dat uitsluitend de aard van de gegevens bepalend is voor de waarde die men aan het gebruik ervan door een applicatie moet toekennen in het licht van één van de bovengenoemde beveiligingsdoelstellingen. De aard van de applicatie is echter minstens zo belangrijk. Een betaalmodule is immers fraudegevoeliger dan een applicatie die slechts financiële overzichten bijhoudt en waarmee geen betalingen worden verricht, terwijl het in beide gevallen om financiële gegevens gaat.

Aan de andere kant is het voorstelbaar dat men binnen een applicatie weer zal willen differentiëren tussen verschillende gegevens, met name om zo aan te geven dat de rechten tot bepaalde gegevens (bijvoorbeeld tot gegevens als bankrekeningnummers en inkoopfactuurbedragen) beperkt moeten worden tot bepaalde functionarissen. In dat geval zal - binnen een classificatie van toepassingen - een gegevensclassificatie moeten worden uitgevoerd.

Het classificeren kan geschieden door rangschikking van gegevens en applicaties ten aanzien van de kwaliteitsaspecten als hoog, gemiddeld en laag, of met behulp van een puntensysteem. In die zin zal een applicatie met gegevens over de cliënten van een lommerd op de beveiligingsdoelstelling 'persoonsvertrouwelijkheid' de score 'hoog' krijgen. Het voordeel van zo'n rangschikking zal duidelijk zijn: op grond hiervan kan worden bepaald welke prioriteiten moeten worden gesteld bij het nemen van maatregelen ten aanzien van geautomatiseerde systemen in een en dezelfde organisatie ([Fijn91]). Daarbij moet erop worden gewezen dat een lage score niet betekent dat een toepassing niet beveiligd hoeft te worden! Het kan zijn dat men op grond van zo'n lage score kiest voor een zogenaamde confectiebenadering; hierop komen wij hieronder terug.

Het is zinvol om het management intensief bij de classificatie te betrekken omdat dit zal leiden tot meer toewijding aan de te nemen beslissingen ten aanzien van het beveiligingsbeleid.

Bedreigingenanalyse
Om de informatiesystemen daadwerkelijk te beveiligen is verder informatie nodig over de bedreigingen waaraan zij bloot staan, de kans dat de bedreigingen werkelijkheid worden en over de impact die dit kan hebben. Ook ten aanzien van het inwinnen van deze informatie worden weer verschillende termen gebruikt, zoals risico-analyse ([Adam 94]) en bedreigingenanalyse ([Gils94], [Rijk94]); in een terechte oproep tot discussie over de vele onduidelijkheden op dit gebied gebruikt [Baut94] de prettig compacte termen 'A-analyse' (afhankelijkheidsanalyse) en 'B-analyse' (bedreigingenanalyse).

Wij spreken hier verder van bedreigingenanalyse, waarmee dan gedoeld wordt op het zo goed en zo kwaad mogelijk vaststellen van de kans dat een bedreiging werkelijkheid wordt, gecombineerd met de impact hiervan. Voor beide geldt, dat ze zelden zinvol in harde cijfers uitgedrukt kunnen worden. In de praktijk bestaat echter toch vaak de wens om het resultaat van de bedreigingenanalyse in kosten te kunnen kwantificeren, omdat het management een al dan niet rationele kosten/baten-afweging wil kunnen maken ten aanzien van de voorgestelde beveiligingsmaatregelen. In dat geval zal men dus toch vaak proberen om de schade zo goed mogelijk in geld uit te drukken!

[Gils94] wijst, naast bovengenoemde bezwaren, ook op de lange doorlooptijd die de officiële methoden voor risico-analyse die op de markt voorhanden zijn, vereisen, en meent – naar onze mening terecht – dat goede resultaten kunnen worden bereikt door de bij de informatiesystemen betrokken medewerkers de relevante bedreigingen te laten aangeven.

A en B: apart of samen?
Er bestaan verschillende inzichten ten aanzien van de operationalisering van het bovenstaande. Sommige auteurs vinden dat men eerst de afhankelijkheidsanalyse met behulp van een classificatie en dan pas een bedreigingenanalyse moet uitvoeren, waarna op basis van een combinatie van beide de zogenaamde beveiligingsnormen en, op basis daarvan, de noodzakelijke maatregelen bepaald kunnen worden ([Adam94], [Gils94]). Anderen, bijvoorbeeld [Heij91], stellen impliciet of expliciet dat beide analyses kunnen worden samengevoegd, waarbij de beveiligingsnormen en van daaruit de maatregelen worden bepaald zonder dat de afhankelijkheden en de bedreigingen apart worden benoemd. Het voordeel van deze aanpak is natuurlijk een besparing van tijd en inspanning, maar het samenvoegen heeft als gevaar dat niet alle bedreigingen in kaart worden gebracht en dat geen uitspraak wordt gedaan over de kans dat de bedreigingen werkelijkheid worden.
De term 'beveiligingsnormen' wordt overigens geïntroduceerd door [Gils94]; naar onze mening een zeer bruikbaar begrip voor het resultaat van de confrontatie van de uitkomsten van classificatie en bedreigingenanalyse.

Hulpmiddelen
De laatste jaren zijn er in snel tempo produkten op de markt verschenen die het uitvoeren van classificatie en bedreigingenanalyse ondersteunen. Zo zijn er boeken met methoden voor het classificeren van informatiesystemen en het vaststellen van bedreigingen en daarmee gepaard gaande schades, alsmede decision support systems waarin men gegevens over de organisatie kan laten verwerken om tot een beoordeling van de getroffen beveiligingsmaatregelen te komen.
Wat deze produkten gemeen hebben is dat men, om ze te kunnen aanwenden, een goede kennis van de bedrijfsprocessen, van de gebruikte informatiesystemen en van informatiebeveiliging moet hebben. Het gevaar van de hulpmiddelen is dan ook, dat ze kunnen suggereren ook zonder dit inzicht succesvol te kunnen worden aangewend ([Park91]). Een waarschuwing op de verpakking van deze produkten – 'alleen onder deskundig toezicht gebruiken' – zou naar onze mening dan ook wettelijk verplicht moeten worden gesteld.

Het management wil een kosten/baten-afweging kunnen maken ten aanzien van voorgestelde beveiligingsmaatregelen.

Selecteren en invoeren van maatregelen

Nu de afhankelijkheden en de bedreigingen in kaart zijn gebracht, kunnen de beveiligingsnormen worden bepaald. Vervolgens moet aan de hand van deze normen worden bepaald welke beveiligingsmaatregelen voor toepassing in aanmerking komen. Doelmatigheid en doeltreffendheid van de maatregelen alsmede hun onderlinge samenhang zullen daarbij voor de beslisser van belang zijn.
Het selecteren en invoeren van maatregelen is een activiteit die op tactisch en/of operationeel niveau plaatsvindt. Ook deze activiteit kunnen we weer beschouwen als een cybernetische regelkring, dat wil zeggen als een opeenvolging van de fasen informeren, bijsturen en evalueren.

Bij het inwinnen van informatie over beveiligingsmaatregelen stuit men in het algemeen op twee problemen.
In de eerste plaats is de vraag welke maatregelen er mogelijk zijn vaak moeilijk volledig te beantwoorden. Veel beveiligingsmaatregelen zijn zelfs voor ingewijden verre van doorzichtig; niet alleen het specialistische karakter van informatiebeveiliging, maar ook het gebrek aan eenduidige terminologie is hieraan debet. De praktijk leert dat technische maatregelen – door een klaarblijkelijk effectieve marketing van beveiligingsleveranciers – vaak wel in voldoende mate vertegenwoordigd zijn, maar dat niet-technische maatregelen – bijvoorbeeld organisatorische, procedurele, psycho-

logische, ergonomische en educatieve maatregelen – veel minder aandacht krijgen dan ze op grond van hun bewezen effectiviteit verdienen.
In de tweede plaats is het vaak moeilijk te voorspellen welke implicaties het treffen van een beveiligingsmaatregel zal hebben. In de vorige paragraaf is al aangevoerd dat het niet meevalt de verwachte kosten in geval van schade vast te stellen. Hetzelfde geldt voor de kosten van beveiligingsmaatregelen – verborgen kosten spelen bij informatiebeveiliging een grote rol. Neem de aanschafprijs van een beveiligingspakket: deze beslaat slechts een fractie van de integrale kosten; bijkomende kosten vloeien voort uit installatie, onderhoud, configuratie, monitoring en upgrading. Wie de kosten in kaart probeert te brengen zal merken dat sommige kostensoorten zeer moeilijk of zelfs helemaal niet in geld uit te drukken zijn. Als voorbeeld noemen we de negatieve invloed die een beveiligingsmaatregel op andere kwaliteitsaspecten van de informatievoorziening kan hebben, zoals de ergonomie van een systeem. Deze kostenpost is nauwelijks in geld uit te drukken, maar zal in sommige gevallen wel degelijk doorslaggevend zijn voor het verwerpen of accepteren van een beveiligingsmaatregel.

Met een algemene checklist kan men snel een zeker niveau van beveiliging bereiken.

Het invoeren van beveiligingsmaatregelen wordt door menigeen gezien als een belemmering van de persoonlijke vrijheid en als het maken van onproduktieve kosten. Een en ander kan weerstand veroorzaken die zich in een veelheid aan vormen kan uiten, variërend van het aanleggen van privésluiproutes tot een collectieve weigering om de voorgeschreven maatregelen uit te voeren. Sancties blijken lang niet altijd effectief. Veel auteurs halen het belang van een bedrijfsbreed positief beveiligingsbewustzijn aan, maar zijn helaas minder specifiek over hoe men zo'n bewustzijn zou kunnen realiseren. Het tonen van kwetsbaarheden schudt alle betrokkenen weliswaar even wakker, maar deze bewustzijnsverhoging is slechts tijdelijk van aard. De praktijk leert dat een voor alle betrokkenen duidelijk zichtbare externe controle het beveiligingsbewustzijn wél op positieve wijze kan beïnvloeden, evenals het opnemen van een aandachtspunt 'beveiligingsbewustzijn' in de beoordelingscriteria van de betrokken medewerkers.

Controleren en evalueren

In de laatste fase van de beveiligingscyclus moet regelmatig worden gecontroleerd of de organisatie het door haar gewenste niveau van beveiliging nog handhaaft.

Een discussie over controlemethoden en -technieken zou hier te ver voeren. Wel willen we, in lijn met het voorafgaande, ook pleiten voor een 'maatwerk'-benadering van de controle. Dat houdt onder meer in, dat bij het opstellen van een controleplan uitgegaan moet worden van een afweging van zowel de risico's die inherent zijn aan de geautomatiseerde bedrijfsprocessen als het risico dat men bij het uitvoeren van het onderzoek loopt, oneffenheden niet aan het licht te kunnen brengen. Naarmate deze risico's groter zijn, zal het onderzoek intensiever moeten zijn.
Ook moeten doeltreffendheid en doelmatigheid van de getroffen beveiligingsmaatregelen regelmatig geëvalueerd worden in het licht van de eerder door de organisatie bepaalde beveiligingsnormen. Controle en evaluatie zullen in de praktijk vaak hand in hand gaan. Voorwaarde voor beide is onafhankelijkheid, beveiligingstechnische deskundigheid, nauwkeurigheid en zorgvuldigheid van de uitvoerder. In de praktijk kan aan deze combinatie van eisen worden voldaan door het inschakelen van gekwalificeerde onafhankelijke deskundigen zoals EDP-auditors.

MAATWERK EN CONFECTIE

Bij het doorlopen van beveiligingscycli leggen de betrokkenen hun bevindingen met betrekking tot afhankelijkheden, bedreigingen en maatregelen vast om de opgedane kennis niet verloren te laten gaan. Deze vastlegging neemt vaak de vorm aan van een overzichtelijke checklist, die echter specifiek is voor de onderzochte informatiesystemen en kwaliteitsaspecten.

Men kan echter ook – en in sommige gevallen met recht – kiezen voor een algemene of confectiebenadering, waarbij men uitgaat van de veronderstelling dat een zelfde beveiligingsvraagstuk voor vergelijkbare informatiesystemen door verschillende organisaties op identieke wijze kan worden opgelost. Bij een confectiebenadering worden de beveiligingsmaatregelen geselecteerd op basis van een bestaande receptuur of checklist. Algemene checklists zijn er in vele soorten en maten. Drie voorbeelden zijn de bekende Checklist Informatiebeveiliging van het NGI ([NGI91]), de Normbladen voor Informatiebeveiliging, een gedetailleerde vragenlijst waarmee de aanwezigheid van strategische, tactische en operationele maatregelen wordt getoetst ([Aald85]), en het document [Curr91] dat operationele richtlijnen geeft voor het beveiligen van Unix-systemen. Deze checklists verschillen onderling sterk, maar hebben ten minste één overeenkomst, namelijk dat ze uitgaan van het beginsel van universele toepasbaarheid.

De belangrijkste reden voor het hanteren van een algemene checklist is doelmatigheid. Men kan het tijdrovende 'informeren' in de verschillende besturingscycli overslaan: voor het strategisch niveau betekent dat de analyse en normstelling, waar hierboven zoveel aandacht aan is gegeven, en de selectie van de maatregelen. In feite laat men deze activiteiten nu over aan de opsteller van de checklist.

Met een algemene checklist kan men dus snel een zeker niveau van beveiliging bereiken, zonder dat men hiervoor opnieuw het wiel hoeft uit te vinden – gemak dient de mens.

Checklists worden niet alleen om efficiency-redenen gehanteerd, maar ook om tot standaardisatie te komen, bijvoorbeeld tussen handelspartners. Het feit dat men de informatiebeveiliging op een uniforme wijze heeft geregeld, kan het vertrouwen in elkaar vergroten. Mede om deze reden vinden wij het gebruik van dergelijke checklists dan ook heel nuttig, maar de vraag is: is het gebruik van een checklist ook voldoende voor een goede beveiliging? Wij denken van niet. De organisatie, de informatietechnologie en het probleemgebied informatiebeveiliging zijn te divers, te complex en te veranderlijk om met een boodschappenlijstje afgehandeld te kunnen worden. Hiervoor zijn ten minste drie oorzaken aan te voeren:

1. 'One size does not fit all'
De beveiligingsbehoeften van verschillende organisaties vertonen onderling vaak veel minder gelijkenis dan men op grond van andere overeenkomsten zou verwachten. Zelfs binnen één branche lopen de produkten en bedrijfsprocessen van verschillende organisaties onderling sterk uiteen. Hetzelfde geldt voor de met de automatisering van deze processen samenhangende risico's en relevante beveiligingsmaatregelen. Daarnaast realiseren organisaties hun informatievoorziening op zeer uiteenlopende manieren. Bestaande verschillen worden vergroot door decentralisatie, waardoor de gebruikte automatiseringsmiddelen zelfs per werknemer kunnen verschillen. Voor wat betreft de beveiliging op het operationele vlak hebben standaardisatie en logische recentralisatie – het gebruik van speciale programmatuur om een gedecentraliseerde omgeving te benaderen als een centraal systeem – vooralsnog niet geleid tot de uniformiteit waarbij een checklist-benadering zou volstaan. Ten slotte zijn sommige maatregelen door verschillen in de omvang, de externe omgeving en de bedrijfscultuur voor de ene organisatie wel toepasbaar, maar voor de andere niet. Zo kunnen maatregelen die zijn gebaseerd op een vergaande controletechnische functiescheiding, niet worden gerealiseerd in kleine of onderbemande organisaties, of is het uitlenen van wachtwoorden door systeemprogrammeurs in een informele organisatie niet of nauwelijks te voorkomen.
Als de beveiligingsbehoefte van een organisatie al te zeer verschilt van de beveiligingsbehoefte waarvoor de checklist ontwikkeld is, resulteert het blindelings toepassen van de checklist in misbeveiliging.

2. Checklists zijn statisch
Door de dynamiek van informatiebeveiliging is een met veel moeite samengestelde checklist vaak binnen afzienbare tijd verouderd. Beveiliging op basis van een frequent bijgewerkte checklist is ook mogelijk. In sommige methoden ([Jaar91]) definieert men een minimumpakket aan beveiligingsmaatregelen, dat is gebaseerd op de beveiliging van bedrijven die als goed beveiligd te boek staan. Deze baseline wordt frequent aangepast. Dat hieraan kosten verbonden zijn spreekt voor zich.

3. Inbrekers houden van checklists
Een derde nadeel van de checklist-benadering is het gegeven dat een standaard-checklist in handen van een tegenstander een gevaarlijk wapen is. Wie over een geldige checklist beschikt weet immers automatisch welke beveiligingsmaatregelen omzeild moeten worden.

Samenvattend: het gebruik van een checklist brengt weliswaar een grote besparing van tijd en energie met zich mee, maar voldoet in lang niet alle gevallen. Met [Gils94] vinden we checklists wel geschikt in de beginfase van een beveiligingstraject, bijvoorbeeld om een bepaald onderdeel van de informatievoorziening snel naar een minimumniveau te tillen. Ook voor risico-arme of uniforme en stabiele omgevingen zou men het hanteren van een checklist kunnen overwegen. In andere gevallen is een maatwerkbenadering noodzakelijk – waarop het toepassen van bestaande checklists een zinvolle aanvulling kan vormen.

Het gebruik van een checklist brengt weliswaar een grote besparing van tijd en energie met zich mee, maar voldoet in lang niet alle gevallen.

TEN SLOTTE: DE CODE VOOR INFORMATIEBEVEILIGING

Ten slotte nog een woord over de recent geïntroduceerde 'Code voor Informatiebeveiliging' ([NNI94]), die – naar Engels voorbeeld – onder auspiciën van het Ministerie van Economische Zaken door het Nederlands Normalisatie Instituut is uitgegeven en wordt ondersteund door een groot aantal bedrijven en organisaties. De doelstelling van deze Code is: het verschaffen van een gemeenschappelijke basis ten aanzien van de informatiebeveiliging voor bedrijven en het (daardoor) bevorderen van het vertrouwen in het handelsverkeer tussen bedrijven.
Hoewel één van de medewerkers bij de introductie stelde, dat bij gebruik van de Code een gedetailleerde risico-analyse of kosten/baten-analyse niet nodig zou zijn ([Comp94]), volgt de Code naar onze mening wel degelijk de maatwerkbenadering. De Code is geen operationele checklist maar heeft de vorm van een leidraad waarin het belang van het vastleggen van beveiligingseisen in een beveiligingsdocument wordt benadrukt en waarbij

Drs. E. Roos Lindgreen Is AIO bij de Technische Universiteit Delft en doet promotie-onderzoek op het gebied van informatie- en netwerkbeveiliging.

Mw.drs. C. Schönfeld RI Is Hoofd EDP-audit van de Gemeentelijke Accountantsdienst (GAD) van Amsterdam. Zij is als zodanig nauw betrokken bij het toezicht op het informatiebeveiligingsbeleid van de gemeente Amsterdam. Daarvoor was zij als adviseur informatiebeveiliging werkzaam bij het Directoraat Generaal van de Volkshuisvesting (DGVH) bij het Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu (VROM).

wordt uitgegaan van het feit dat de kosten van de beveiligingsmaatregelen voor IT-voorzieningen afgewogen dienen te worden tegen de waarde voor het bedrijf van de informatie en de schade die kan ontstaan wanneer niet voldoende maatregelen worden getroffen. Het blijft dus noodzakelijk om zelf activiteiten in de sfeer van risico-afweging uit te voeren. Het is dus zeker niet zo dat de Code in schril contrast staat – zoals in [Comp94] wordt gesteld – met het nieuwe 'Besluit voorschrift Informatiebeveiliging rijksdienst' ([Rijk94]), dat de in dit artikel geschetste maatwerkmethode met afhankelijkheidsanalyse en bedreigingenanalyse volgt. Van een contrast is geen sprake! Hetzelfde geldt voor twee andere documenten die onlangs het licht zagen, de brochure 'Beveiliging van persoonsregistraties' van de Registratiekamer ([Regi94]) en het Handboek Informatiebeveiliging van de gemeente Amsterdam ([Adam94]), die ook een maatwerkbenadering propageren.

CONCLUSIES

Informatiebeveiliging schept cyclisch terugkerende keuzeproblemen op alle niveaus van de organisatie. Het informatie- en besluitvormingsproces op strategisch niveau wordt gevormd door een afhankelijkheidsanalyse (A-analyse), bedreigingenanalyse (B-analyse) en de selectie van maatregelen. De wijze waarop dit proces wordt uitgevoerd, is bepalend voor het onderscheid tussen maatwerk en confectie; het eerste heeft onze voorkeur.

LITERATUUR

[Adam94] *Handboek Informatiebeveiliging Gemeente Amsterdam*, Stadsdrukkerij Amsterdam, 1994.

[Aald85] J.C.H. Aalders, I.S. Herschberg en A. van Zanten, *Handbook for Information Security*, North-Holland Publishing, 1985.

[Baut94] J. Bautz, *A-, B-, K-analyses mode of iets blijvends?*, NGI Nieuwsbrief Afdeling Beveiliging, november 1994.

[Blum69] S.C. Blumenthal, *Management Information Systems, a framework for planning and development*, Prentice Hall, 1969.

[Comp94] *Landelijk veilige code noodzakelijk*, Computable 1994 week 49.

[Curr90] D.A. Curry, *Improving the Security of your Unix System*, SRI International, April 1990.

[Fijn91] R.G.A. Fijneman et al., *Betrouwbaarheid geautomatiseerde informatiesystemen*, Compact 1991/1.

[Gils94] H.G.Th. van Gils, *Informatiebeveiliging: de tijd is rijp*, Compact 1994/1.

[Giel89] C.J.M. Gielen, *Een praktische methode voor de analyse van risico's bij automatisering*, Compact 1989/2.

[Heij91] D. Jansen Heijtmajer, *Beveiligingsbeleid geautomatiseerde informatievoorziening*, Compact 1991/3.

[Jaar91] S. Jaari, *Top Management Challenge – From Quantitative Guesses to Prudent Baseline of Security*, Proceedings IFIP Information Security, D. Lindsay (ed.), 1991.

[Kuip89] J. Kuipers, *De keuze van beveiligingsmaatregelen in een geautomatiseerde omgeving*, Compact 1989/2.

[NGI91] Nederlands Genootschap voor Informatica, *Checklist Computerbeveiliging*, Kluwer Bedrijfswetenschappen, 1991.

[NGI92] Nederlands Genootschap voor Informatica, afdeling Beveiliging, *Beveiligingsbeleid en beveiligingsplan*, Kluwer Bedrijfswetenschappen, 1992.

[NIVR89] NIVRA-geschrift 53, *Automatisering en controle Deel VII. Kwaliteitsoordelen over informatievoorziening*, Kluwer Bedrijfswetenschappen, 1989.

[NNI94] Nederlands Normalisatie Instituut, *Code voor Informatiebeveiliging*, november 1994.

[Park91] Donn B. Parker, *17 Information Security Myths Debunked*, Proceedings ISSA Security Conference, 1991.

[Rain93] R.K. Rainer et al., *Risico-analyse voor informatietechnologie*, Management en Organisatie van Automatiseringsmiddelen, 1993 no. 3.

[Regi94] Registratiekamer, *Beveiliging van persoonsregistraties*, november 1994.

[Rijk94] *Besluit voorschrift Informatiebeveiliging Rijksdienst 1994*, Staatscourant 173.

[Velt91] P. Veltman, *Systemen voor logische toegangsbeveiliging*, Compact 1991/4.

[Wely92] B.J.M. van Wely, *Beveiligingsbeleid gegevens en gegevensverwerking, een praktisch voorbeeld*, Compact 1992/2

[Wien61] N. Wiener, *Cybernetics, control and communication in the animal and in the machine*, Wiley, 1961.

Stroomlijnen en herontwerpen in een onderhoudsbedrijf: gelijktijdig en/of volgtijdig?

De beschrijving van een praktijksituatie

Drs. O.C. van Leeuwen RA en
drs. M.C. van Veen RC

Organisaties moeten zich aanpassen aan de sterk veranderende eisen van de markt en aan de eisen van de maatschappij in het algemeen. Soms kan het noodzakelijk zijn om hele bedrijfsprocessen opnieuw te ontwerpen. Hierbij kan informatietechnologie als een gegeven worden beschouwd of als aandrijving functioneren. De auteurs beschrijven deze alternatieven in de praktijksituatie van een onderhoudsbedrijf.

INLEIDING

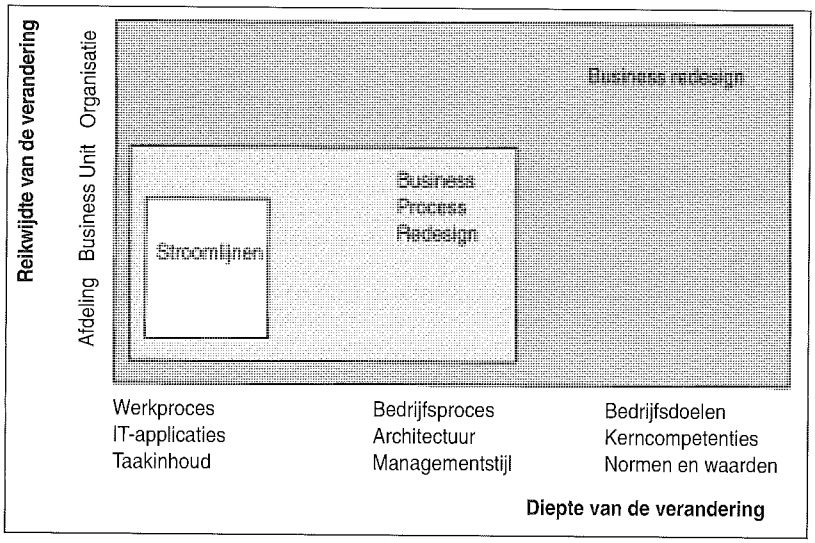
In dit artikel wordt een beeld gegeven van de weg die een onderhoudsbedrijf heeft afgelegd om, met behulp van het stroomlijnen en herontwerpen van de organisatie, te komen tot een sterk verbeterd bedrijfsproces. Hiermee werd een inhaalslag ten opzichte van de concurrentie gerealiseerd.

De organisatie in kwestie houdt zich bezig met het onderhoud van motoren en maakt onderdeel uit van een groot concern. Twee jaar geleden verkeerde het bedrijf in grote problemen: de financiële resultaten schommelden sterk, zonder dat er een goed inzicht was in de oorzaak van de verliezen. Tevens was het logistieke proces niet onder controle. Dit werd gecompenseerd door hoge (tussen)voorraden om toch nog zo goed mogelijk te kunnen voldoen aan de marktvraag.

Onder druk van de concernleiding werd besloten een project te starten dat op een aantal fronten moest zorgen voor verbeteringen. Gebruik makend van een gestructureerde aanpak werd gekozen voor een mix van korte termijn-verbeteringen en meer fundamentele aanpassingen van bedrijfsprocessen. Dit voorbeeld demonstreert dat, wanneer men processen wil herontwerpen, dit niet uitsluitend fundamenteel hoeft te gebeuren, maar dat men dit kan combineren met acties die in de categorie 'stroomlijnen' vallen. Het voordeel is dat hierdoor een sneeuwbaleffect mogelijk wordt: mensen binnen en buiten de organisatie zien op korte termijn successen en worden hierdoor gestimuleerd om met meer dan normale inzet en geloof de fundamentele veranderingen te ondersteunen en te realiseren.

In de literatuur over herontwerpen, ook wel Business Process Redesign (BPR) of Reengineering genoemd, wordt een onderscheid in ambitieniveau gemaakt. Figuur 1 geeft de verschillende niveaus weer[1].

In dit artikel wordt niet ingegaan op de vraag of BPR nieuw is of dat het oude wijn in nieuwe zakken is. Deze, in een praktijksituatie vooral academische vraag, wordt in een groot aantal andere artikelen[2] reeds behandeld.



Figuur 1. Redesign wordt op vele manieren toegepast.

DOEL VAN HET PROJECT EN BEHAALDE RESULTATEN

De overall-doelstelling van het project was om het bedrijf tot een krachtige en concurrerende marktpartij om te bouwen. Dit werd vertaald in het behalen van een drastische verlaging van het voorraadniveau van motoronderdelen, een verkorting van de doorlooptijden van motoren en een verhoging van de leverbetrouwbaarheid. De behaalde resultaten waren als volgt:

- doorlooptijd van het onderhoudsproces: -/- 33 procent (van negentig naar zestig dagen);
- voorraden: -/- 55 procent;
- leverbetrouwbaarheid van 30 procent naar 100 procent.

Informatietechnologie wordt vaak gezien als de hefboom die prestatiesprongen mogelijk maakt. Dat is waar. Deze case toont echter aan dat ook met (het verbeteren van) de bestaande systemen reeds veel mogelijk is. Te vaak worden, ons inziens, door managers de bestaande logge IT-systemen als excuus aangevoerd om hun passiviteit ten aanzien van het doorvoeren van veranderingen te rechtvaardigen.

EERST ORGANISEREN, DAN ...

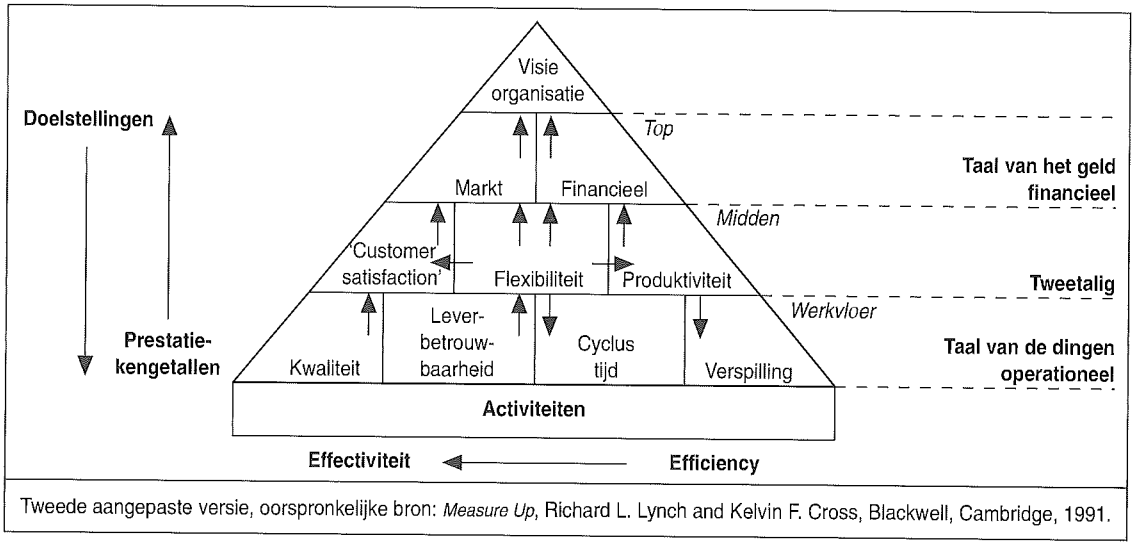
In deze paragraaf wordt een beeld gegeven van de gekozen aanpak om de projectdoelen te behalen. De hierna te behandelen stappen 1 tot en met 3 besloegen een periode van vijf maanden. Fase 4 duurde zeventien maanden. De stappen 3 en 4 worden in de volgende paragrafen nader uitgewerkt.

Stap 1: Strategie en prestatie-indicatoren bepalen

De doelstelling van het project was (zoals hiervoor vermeld) om door het verbeteren van de doorlooptijd, het voorraadniveau en de leverbetrouwbaarheid het bedrijf tot een krachtige en concurrerende marktpartij om te bouwen. Daartoe werd een omvangrijk veranderingstraject gestart. Uitgangspunt van het veranderingstraject was de strategie die erop gericht was om de internationale concurrentie in te halen in termen van prijs en prestaties. Door middel van de prestatiepiramide werd de strategie vertaald naar de werkvloer (zie figuur 2).

De piramide geeft weer op welke wijze de visie van het onderhoudsbedrijf werd doorvertaald naar prestatiekengetallen voor de werkvloer. Het meten van deze kengetallen (zoals de doorlooptijd van de reparatie van een motoronderdeel) maakt een inte-

Figuur 2. Prestatiepiramide.



Tweede aangepaste versie, oorspronkelijke bron: *Measure Up*, Richard L. Lynch and Kelvin F. Cross, Blackwell, Cambridge, 1991.

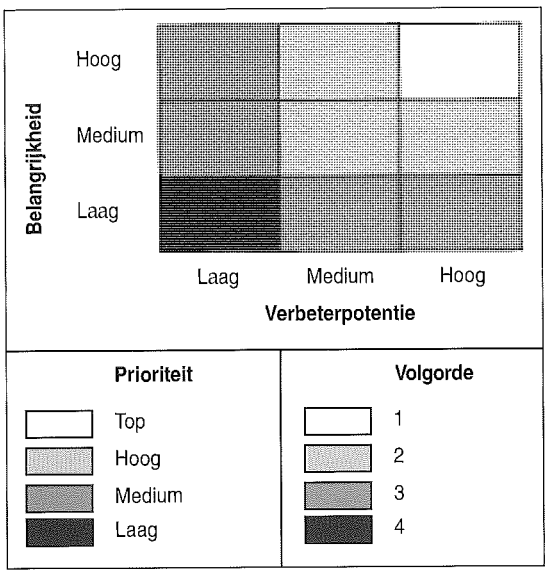
1 *M.V. Batelaan, Tien manieren om redesign te verknoeien, Holland Management Review, nummer 35, 1993.*

2 *Zie bijvoorbeeld H.G. Westendorp, Prestatiesprongen door procesherontwerp: is het slechts een modekreet of steekt er werkelijk wat achter, NIVE Management Magazine, augustus 1994.*

graal onderdeel uit van de gevolgde methode. De werkelijke prestaties van het onderhoudsbedrijf kunnen met de doelstellingen worden vergeleken, waardoor bijsturing mogelijk wordt.

Stap 2: Vastleggen van de huidige performance

Van een aantal kritische processen binnen de totale keten werd de huidige performance vastgelegd. Door de huidige performance te vergelijken met de uit de strategie afgeleide, gewenste prestaties kon de procesprioriteiten matrix worden ingevuld.



Figuur 3. Procesprioriteiten-matrix.

Stap 3: Bepalen van het ambitieniveau

Op basis van de procesprioriteiten-matrix werd besloten om te komen tot een mix van activiteiten, teneinde enerzijds het produktieproces te herontwerpen en anderzijds de informatieverstrekkende (financiële) ondersteunende processen te stroomlijnen. Hiervoor werd een implementatieplan opgesteld, waarmee de implementatie gefaseerd en gecontroleerd kon worden gerealiseerd. Ook tijdens de 'verbouwing' moet de produktie gewoon doorgaan!

Stap 4: Implementatie

Om de prestaties van het produktieproces op een concurrerend niveau te kunnen brengen, waren drastische veranderingen noodzakelijk. Voor het produktieproces en voorraadbeheer ging men uit van vooraf berekende behoeften aan onderdelen en materialen, en van vaste doorlooptijden in het produktieproces. Men hanteerde – in vaktermen – de Material Requirements Planning (MRP) filosofie. Besloten werd om dit principe volledig te verlaten en over te gaan op het uit Japan afkomstige Kanban-principe: het 'Just In Time' (= niet te vroeg en niet te laat) aanleveren van onderdelen op basis van het pull-concept (dat wil zeggen alleen als erom wordt gevraagd).

BEPALEN VAN HET AMBITIENIVEAU

In deze paragraaf wordt de gekozen mix van stroomlijnen en herontwerpen nader toegelicht, alsmede de relatie met informatietechnologie.

Het stroomlijnen van de informatieverzorgende financieel-administratieve processen

Binnen dit ambitieniveau staat het wegnemen van de geconstateerde knelpunten centraal. Er wordt zoveel mogelijk gebruik gemaakt van reeds bestaande systemen. Oplossingen worden met name in procedurele en organisatorische zin gezocht. Aanpassingen van de informatietechnologie vinden zo min mogelijk plaats. Gedurende dit traject zullen de huidige door het bedrijf gehanteerde procedures en processen worden gestroomlijnd.

Belangrijk kenmerk van deze aanpak is dat gedurende het stroomlijnen de bestaande informatietechnologie een randvoorwaarde is. Het optimaliseren vindt niet plaats door het bouwen of implementeren van nieuwe omvangrijke applicaties. Er wordt gewerkt met noodverbanden. Er vinden slechts geringe aanpassingen plaats in de informatietechnologie door het op handige wijze aan elkaar knopen van bestaande applicaties en beperkte inzet van kleine ondersteunende pakketjes (zoals stand alone-voorraadsysteempjes en spreadsheettoepassingen voor tracking en tracing van onderdelen).

Bij de ondersteunende informatieverzorgende en financieel-administratieve processen werd gekozen voor het stroomlijnen omdat de organisatie 'gewoon' moest blijven doorwerken. Dit zou bij het herontwerpen van deze processen waarschijnlijk niet meer haalbaar zijn. Bovendien waren veel van de huidige procedures, werkprocessen en componenten van de informatievoorziening nog zo complex dat met vereenvoudiging veel geld te verdienen viel.

Na afronding van het stroomlijnen van de processen is de reeds aanwezige spaghetti van bestaande systemen (met alle onderhoudsproblemen van dien) nog verder aangevuld. Op dat moment heeft de organisatie via het hierboven beschreven traject zich als het ware prototyping-achtig ontwikkeld tot een situatie die voor herautomatisering in aanmerking komt. Op basis van de gehanteerde werkprocessen kunnen nu de functionele specificaties van de nieuw te ontwikkelen systemen worden ontwikkeld. Hierdoor kunnen uiteindelijk ook grote besparingen op het vlak van de informatietechnologie worden gerealiseerd.

Volledig procesherontwerp om te komen tot een optimaal functionerende motoronderhouds- en reparatie-organisatie

Het totale functioneren van het bedrijf wordt hierbij geanalyseerd. Uitgaande van de te verrichten diensten worden alle processen die tot een dergelijke dienst bijdragen, opnieuw ontworpen. Hierbij wordt ervan uitgegaan dat de informatietechnologie niet langer een beperkende voorwaarde is. De voor het realiseren van de gewenste procesgang noodzakelijke systemen worden op basis van die procesgang herontworpen.

Bij volledig procesherontwerp bestaat de mogelijkheid om processen ook onder te brengen buiten de huidige systeemgrenzen. Hierbij kan bijvoorbeeld de mogelijkheid ontstaan dat sommige processen worden uitbesteed. Het omgekeerde is echter ook mogelijk! Processen die vroeger buiten de deur werden uitgevoerd, komen dan weer binnenshuis. Het onderhoudsbedrijf moest bij een keuze voor volledig procesherontwerp derhalve bereid zijn het functioneren van de volledige motoronderhouds- en reparatieprocessen – die deels buiten de bedrijfsgrenzen liggen – ter discussie te stellen. Dit gold in de casus onder meer voor de in- en verkoopfunctie. Dit betekent dat bestaande machtsstructuren binnen het totale concern waarvan het onderhoudsbedrijf deel uitmaakt, zullen moeten worden doorbroken. Hiervoor is heel wat moed nodig. Zeker wanneer men zich realiseert dat het daadwerkelijk bereiken van een goed werkende 'herontworpen' organisatie enige tijd kan vergen (in de casus meer dan anderhalf jaar).

Ook de informatietechnologie moest worden aangepast ten behoeve van de herontworpen processen. Dit betrof onder meer de aanschaf en implementatie van een nieuw voorraad- en produktieplanningssysteem dat geïntegreerd functioneert met een financiële voor- en nacalculatiemodule.

Gezien de potentiële voordelen van het herontwerpen van het primaire proces is besloten om in combinatie met het stroomlijnen van de financieel-administratieve processen in elk geval over te gaan tot procesherontwerp van het primaire proces. Het ter discussie stellen van de relaties met de andere onderdelen van het concern (en/of uitbesteden van processen) bleek politiek nog niet haalbaar.
Het is van groot belang gebleken aan het eind van stap 3 duidelijk te maken welk ambitieniveau voor het verbeteringstraject wordt gekozen. Door van tevoren duidelijk aan te geven wat verwacht wordt van het verbetertraject, kan tussentijds beter worden bijgestuurd en later worden vastgesteld in hoeverre de gestelde doelen ook behaald zijn. Maandelijks werd hierover gerapporteerd aan het management van de organisatie.

DE IMPLEMENTATIE

In het vervolg wordt kort aangegeven op welke aspecten het gecombineerde stroomlijn- en herontwerpproject betrekking had.

De inhoud

De meer concrete veranderingsvoorstellen hadden enerzijds betrekking op de processtructuur en anderzijds op de financieel-administratieve processen.

Processtructuur
Zoals vermeld werd besloten bij het onderhoudsproces over te gaan op het uit Japan afkomstige Kanban-principe. Dit is het precies op tijd aanleveren van die onderdelen waarom wordt gevraagd door een volgende schakel in het onderhoudsproces. Beknopt geformuleerd: bij het voorheen gehanteerde MRP-concept is het uitgangspunt dat er op basis van de voorspelling een hoeveelheid X aan voorraad op de plank moet liggen. In een Kanban-situatie zorgen zelfsturende teams ervoor dat er op het juiste moment voldoende onderdelen aanwezig zijn voor de gebruikers van de onderdelen. Het streven is op die manier enerzijds een totale voorraadverlaging te realiseren en anderzijds ervoor te zorgen dat er voldoende voorraad op de plank ligt om aan een turbulente marktvraag te kunnen voldoen.

Het produktieproces werd hiertoe opgedeeld in logische delen, waartussen kleine buffervoorraden werden gelegd. De zelfsturende teams gaan pas produceren indien het niveau van de buffervoorraad na hen in de keten 'erom vraagt'.

Aansluitend op de nieuwe inrichting van het produktieproces werd een andere organisatiestructuur geïntroduceerd, gekoppeld aan de nieuwe besturingsfilosofie van het logistieke traject. Dit resulteerde in drie units die aansluiten op de verschillende fasen binnen het reparatieproces:
- de motor-unit;
- de module-unit;
- de onderdeelreparatie-unit.

Het effect van deze veranderingen betrof onder meer het terugbrengen van doorlooptijden en voorraadniveaus en het verbeteren van de leverbetrouwbaarheid.

De financieel-administratieve processen
Aansluitend op de nieuwe organisatiestructuur en afgeleid uit de prestatiepiramide werden voor alle managers binnen het bedrijf 'scorecards' ingevuld. De 'scorecards'[3] geven een gebalanceerd beeld vanuit vier invalshoeken, zoals weergegeven in figuur 4.

De scorecards per manager sluiten aan op de doelen die zijn afgeleid uit de prestatiepiramide en sluiten tevens aan op de afrekencultuur die gecombineerd met de invoering van de nieuwe manier van werken van het primaire proces werd geïntroduceerd. De scorecards van de verschillende managers beslaan alle activiteiten van het onderhoudsbedrijf.

Om een beter financieel inzicht te verkrijgen werd een groot aantal bestaande knelpunten in de informatievoorziening geëlimineerd. Een belangrijk

3 *Gebaseerd op het door Kaplan en Nolan ontwikkelde concept.*

verbeterpunt hierbij was de introductie van een voor- en nacalculatiesysteem. Daarnaast was het noodzakelijk om vele noodverbanden in de bestuurlijke informatievoorziening op te tuigen. Op dit moment wordt herautomatisering van de bestuurlijke informatievoorziening overwogen.

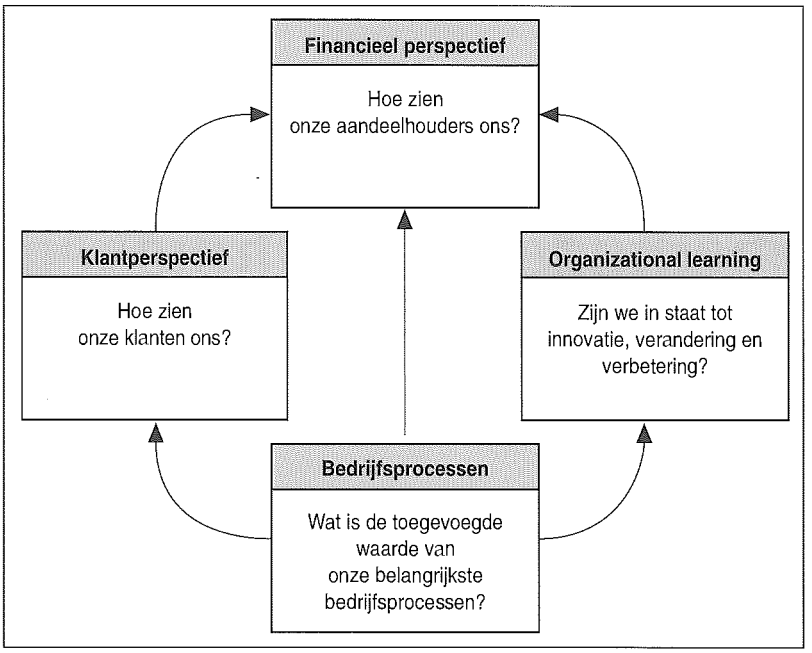
Hard en zacht

Behalve van de hierboven beschreven meer concrete veranderingsvoorstellen bleek het succes van het project voor een zeer belangrijk deel af te hangen van de manier waarop de verandering werd doorgevoerd. We hebben het dan meer over de 'zachte' kanten van organisatieveranderingen.
Want het is onvoldoende alleen managers van de noodzaak van verandering te overtuigen, het ging er in deze casus uiteindelijk om zo'n zeshonderd mensen mee te krijgen. Het valt niet mee om opeens anders te gaan werken dan je altijd gewend bent. Om die veranderingen te communiceren, is er gebruik gemaakt van logistieke games en video's. Daarin werd eerst de 'Niets doen'-variant getoond. Tegen een achtergrond van concurrentie die wél iets doet, is dit een optie met weinig perspectief. Ook werd de tegenstelling tussen de systemen MRP en Kanban getoond, door mensen reparatiematerialen door een produktieproces te laten duwen, dan wel door 'het proces' op basis van klantvraag de materialen bij andere mensen te laten wegtrekken.
Door het spelen van de games en door het kijken naar de video's is de boodschap goed overgekomen.

Behalve aan bovenstaande communicatiemiddelen is het succes van het project te danken aan goed leiderschap. Een projectteam kan namelijk nog zulke goede plannen bedenken, uiteindelijk zal het management de plannen moeten supporten en moeten zorgen dat de plannen worden ingevoerd. In dit geval heeft de general manager de plannen volledig gesteund, zowel in woord als gedrag, is hij de zeepkist opgeklommen en heeft hij persoonlijk in vele sessies door het hele bedrijf uitgelegd wat de veranderingen zijn en waarom ze nodig zijn. Hier was wel een lange adem voor nodig. De organisatieverandering werd namelijk doorgevoerd via een soort sneeuwbalmodel, waarbij opgeleide mensen de volgende groep weer moesten opleiden.

CONCLUSIES

De afgelopen jaren is er gewerkt in een constant spanningsveld tussen de noodzakelijk door te voeren verbeteringen van de organisatie en het aanpassen van de informatieverzorging (processen en informatietechnologie). De bestaande informatietechnologie is echter steeds het uitgangspunt gebleven. Het voordeel hiervan was dat de aandacht met name kon worden gericht op het effectueren van daadwerkelijke veranderingen. Het nadeel was dat niet altijd voor de beste oplossing kon worden gekozen.



Figuur 4. Balanced Business Scorecards.

De hierbij gevolgde aanpak was een combinatie van herontwerp en 'quick hits' op het gebied van de informatieverzorging en de financiële administratie (stroomlijnen) om voor geloof in eigen kunnen te zorgen. Het realiseren van aanzienlijke verkortingen in de doorlooptijd van het demonteren en assembleren van een motor, en het snel inzichtelijk krijgen van de nacalculatorische kosten van een onderhoudsbeurt ten opzichte van de voorcalculatorische kosten, zijn hiervan goede voorbeelden. Hierdoor werd een sneeuwbaleffect op gang gebracht. Wanneer de sneeuwbal eenmaal rolt, lijkt alles vanzelf te gaan. Het is echter de kunst de sneeuwbal in beweging te krijgen.

Nu het bedrijf alle in het voorgaande beschreven zaken heeft doorgevoerd en weer op concurrerend niveau is gebracht, is het geen tijd om op de lauweren te gaan rusten. Want ook de internationale concurrentie zit niet stil en is bezig met het structureel verbeteren van de prestaties. De belangrijkste concurrent heeft onlangs op een internationale beurs aangekondigd dat hij de doorlooptijd wil gaan terugbrengen tot dertig dagen!

Het bedrijf staat nu voor de opgave om deze uitdaging op te pakken en tot een volledig herontwerp van *alle* processen in hun onderlinge samenhang te komen, waarbij ervoor is gekozen dat informatietechnologie dit keer wel als hefboom zal moeten fungeren.
'Stroomlijnen en herontwerpen: gelijktijdig en/of volgtijdig.' Deze casus is een voorbeeld waarbij in eerste instantie verschillende processen gelijktijdig werden gestroomlijnd dan wel herontworpen. Dit heeft uiteindelijk de weg vrijgemaakt voor een volledig herontwerp van alle processen.

Drs. O.C. van Leeuwen RA en drs. M.C. van Veen RC Zijn beiden werkzaam bij KPMG Management Consultants. Eerstgenoemde is daarnaast als docent Organisatie van de Informatieverzorging verbonden aan de Erasmus Universiteit Rotterdam.

Het ontwikkelen van methoden en technieken van EDP-auditing

Drs. R.G.A. Fijneman RE RA

Het EDP-auditberoep staat voor de uitdaging via het ontwikkelen en structureren van tools het vakgebied verder te professionaliseren. Door middel van tools kan een gestructureerde en gefaseerde aanpak worden afgedwongen en gevolgd. De toepassing van tools leidt tot verhoging van de efficiëntie bij de uitvoering van een EDP-audit en van de acceptatie van de resultaten. Verder geldt een toolbox als marketinginstrument.

INLEIDING

Het ontwikkelen van methoden en technieken van EDP-auditing heeft de aandacht van de beroepsgroep van EDP-auditors. Zowel door de post-doctorale opleidingen EDP-auditing als door de NOREA wordt aandacht besteed aan dit onderwerp. Binnen de NOREA is een aantal studiegroepen ingesteld die invulling geven aan onderwerpen als het ontwikkelen van standaarden, het eenduidig afbakenen van het werkgebied van EDP-auditing en het ontwikkelen van aanzetten tot een EDP-auditplan.

Het is logisch dat een relatief snel groeiende beroepsgroep (momenteel zijn ongeveer vijfhonderd EDP-auditors ingeschreven bij NOREA) zich bezighoudt met het ontwikkelen van methoden en technieken om daarmee op efficiënte en effectieve wijze opdrachten uit te kunnen voeren. Methoden en technieken kunnen bovendien een belangrijke bijdrage leveren aan het waarborgen van de kwaliteit van de opdrachtuitvoering en het resulterende eindprodukt.
Dit artikel[1] beoogt een aantal achtergronden te behandelen die van belang zijn bij het verder ontwikkelen van methoden en technieken van EDP-auditing. Het artikel is in belangrijke mate gebaseerd op het afstudeerverslag 'Een toolbox voor een EDP-auditor' van drs. E.P.R. van Vroenhoven RE RA, eveneens werkzaam bij KPMG EDP Auditors. Hoewel dit afstudeerverslag dateert uit 1990 zijn hieruit aandachtspunten af te leiden die nu nog steeds of wellicht juist nu van belang zijn bij het ontwikkelen van methoden en technieken.

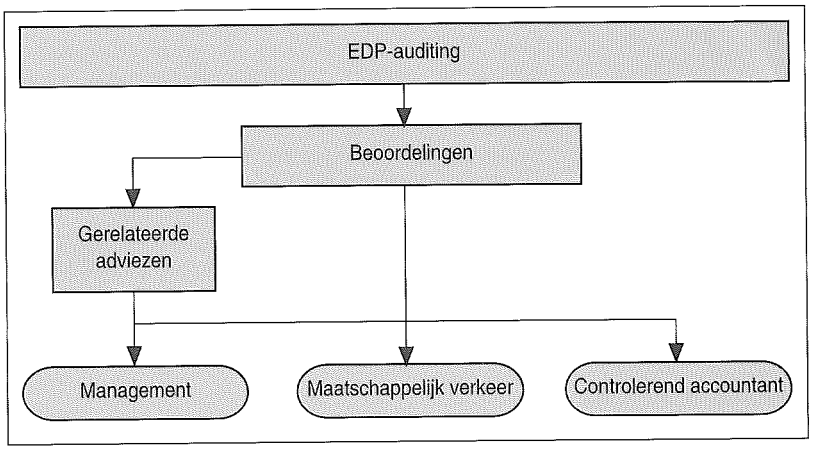
Bij nadere beschouwing van het onderwerp is direct een aantal vragen te onderkennen die om beantwoording vragen. Hierbij valt te denken aan:
- Wat zijn methoden en technieken?
- Wat omvat het vakgebied EDP-auditing?
- Wat wordt bedoeld met het ontwikkelen van methoden en technieken?

Wellicht suggereert de titel dat voordat nader wordt ingegaan op het ontwikkelen van methoden en technieken, een overzicht van bestaande methoden en technieken wordt gegeven. Dit blijkt in de EDP-auditpraktijk van vandaag de dag echter niet of nauwelijks mogelijk te zijn. Een opsomming van beschikbare methoden en technieken wordt vanwege het gevaar van het niet volledig zijn achterwege gelaten. De hiervoor vermelde vragen zullen in deze bijdrage hopelijk in belangrijke mate worden beantwoord.

BELANGHEBBENDEN EDP-AUDITS

Het gebruik van informatietechnologie is de laatste jaren steeds meer toegenomen en ook in de toekomst zal deze trend zich zeker voortzetten. Geautomatiseerde informatiesystemen worden steeds complexer en organisaties worden meer en meer afhankelijk van het voortdurende en betrouwbare functioneren van geautomatiseerde systemen. Deze toenemende complexiteit en afhankelijkheid brengen risico's met zich mee voor de belanghebbenden.

Uit figuur 1 blijkt dat als belanghebbenden het management van een organisatie, het maatschappelijk verkeer en de controlerend accountant kunnen worden onderscheiden. Het maatschappelijk verkeer dient in de ruimste zin van het woord te worden gezien. Zo worden daar bijvoorbeeld de fiscus, de overheid, de aandeelhouders, maar ook de crediteuren en de Registratiekamer (privacy) onder verstaan.



Figuur 1. Behoefte aan EDP-auditing.

TOOLBOX

Bij de belanghebbenden bestaat mede als gevolg van de toenemende complexiteit en afhankelijkheid van automatisering een sterk groeiende behoefte aan EDP-auditing. Hiervoor zijn ervaren EDP-auditors benodigd. Het aantal ervaren EDP-auditors is echter ondanks de vijfhonderd leden van NOREA nog relatief beperkt. Deze 'onervarenheid' wordt onder andere veroorzaakt door de diversiteit en complexiteit van de werkzaamheden van de EDP-auditor, de mate waarin het vakgebied aan verandering onderhevig is en het feit dat EDP-auditing een betrekkelijk jong vakgebied is.
Een frictie tussen enerzijds de toenemende vraag naar EDP-auditing en anderzijds het nog onvoldoende aanbod van efficiënte en effectieve EDP-auditprodukten is waarneembaar in de praktijk van vandaag de dag. Vandaar dat gepoogd wordt enerzijds onervaren EDP-auditors op een effectievere manier in te zetten en anderzijds de efficiëntie van de EDP-audits zelf te verbeteren.
Een toolbox voor een EDP-auditor kan hiertoe een bijdrage leveren.

Een toolbox voor een EDP-auditor kan als volgt worden gedefinieerd:

Een toolbox voor een EDP-auditor is een goed toegankelijke verzameling tools, waarmee ondersteuning van de uitvoering en beheersing (in de vorm van een EDP-auditplan) van een EDP-audit op een effectieve en efficiënte wijze mogelijk is.

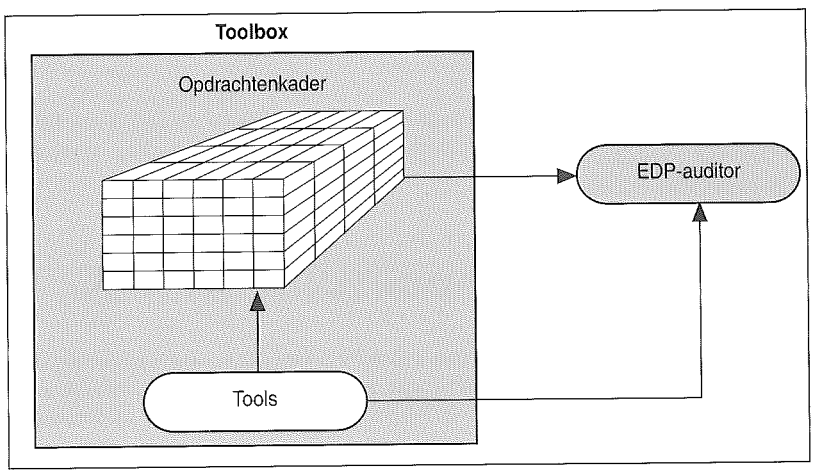
In de definitie wordt een toolbox als een 'goed toegankelijke verzameling tools' omschreven. Dit betekent dat de toolbox, naast een verzameling tools, over een mechanisme dient te beschikken dat de toegang tot de verzameling tools op een adequate wijze regelt. Bij een toolbox voor een timmerman, een gereedschapskist, is dit een handige vakindeling in de gereedschapskist. Met behulp van de vakindeling kan de timmerman snel en gemakkelijk het benodigde werktuig voor een opdracht vinden.
Evenals bij de timmerman is bij de EDP-auditor de opdrachtformulering de sleutel voor het benaderen van de toolbox. De EDP-auditor is immers op zoek naar de juiste tools voor een bepaalde opdracht. Vandaar dat de toolbox, naast een verzameling tools, een zogenaamd opdrachtenkader bevat.

Via het opdrachtenkader kan de EDP-auditor vanuit de opdrachtformulering de verzameling tools benaderen (zie figuur 2).

VOORDELEN VAN DE TOOLBOX

Voordat nader op de indeling van de toolbox wordt ingegaan, worden enige voordelen van het gebruik van een toolbox beschreven. Deze voordelen zijn ontleend aan de praktijk.

Figuur 2. Een toolbox voor een EDP-auditor.



1 Dit artikel is een bewerking van de bijdrage 'Ontwikkelingen in methoden en technieken van EDP-auditing', die als onderdeel van het congres 'De EDP-auditor up-to-date' op 13 december 1994 door de auteur is verzorgd.

Onervaren EDP-auditors zijn effectief in te zetten.
Door middel van tools kan een gestructureerde en gefaseerde aanpak worden afgedwongen en gevolgd. De begeleidende EDP-auditor en de opdrachtgever zijn in staat de activiteiten van de uitvoerende EDP-auditor te volgen en te beheersen. Daarnaast kunnen de tools een belangrijke bron bieden voor het opstellen en hanteren van de juiste normenstelsels bij de uitvoering van de opdracht. Deze standaard-normenstelsels zullen wel op de specifieke situatie dienen te worden aangepast, maar deze activiteit is door het aanwezig zijn van referentiemateriaal op effectievere wijze uit te voeren.

Verbetering efficiëntie van de uitvoering van een EDP-audit.
Het kerngezegde dat hierbij een rol speelt is 'het wiel opnieuw uitvinden'. Relatief veel tijd wordt door EDP-auditors besteed aan het bepalen van een methode van aanpak, het inrichten van de audit, het opstellen van normenstelsels en dergelijke. Naarmate een EDP-audit meer is uitgekristalliseerd en diverse tools voorhanden zijn, kan de EDP-auditor sneller tot de kern van de problemen doordringen. Hierdoor ontstaan mogelijkheden om met behoud van kwaliteit de duur van de audit te verkorten en de kosten te verlagen. Het is van belang hierbij rekening te houden met de hierna nog uit te werken typering van EDP-audits naar projectmatige en/of routinematige werkzaamheden.

Acceptatie van de resultaten van een EDP-audit.
Indien een EDP-audit kwalitatief goed is uitgevoerd, maar de resultaten worden niet geaccepteerd door de opdrachtgever, dan is de effectiviteit van de EDP-audit als minimaal te beschouwen. De acceptatie door de opdrachtgever kan worden bereikt door enerzijds inzicht te geven in het proces van uitvoering van de audit en anderzijds de gehanteerde normen bij de beoordeling expliciet te vermelden. Met behulp van tools kan de EDP-auditor deze gewenste openheid van zaken verschaffen.

Toolbox als marketinginstrument.
Voor het marketen van de diensten van een EDP-auditorganisatie is het van belang deze diensten in een tastbare vorm te kunnen tonen. Tools kunnen onder de aandacht van potentiële opdrachtgevers worden gebracht.

Deze voordelen zullen overigens in de afsluitende beschouwingen van dit artikel enigszins worden genuanceerd. Het is niet zo dat alleen een toolbox zorg draagt voor een effectieve en efficiënte EDP-auditpraktijk, daar is ook vakmanschap voor nodig.

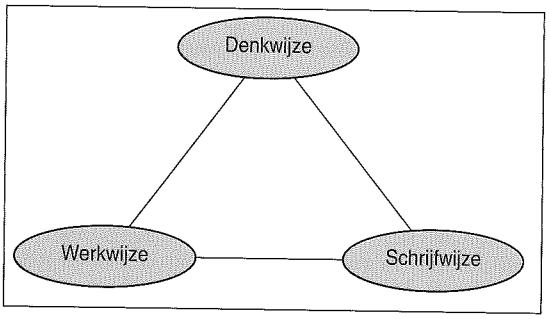
VORMEN VAN ONDERSTEUNING

Er kan een viertal vormen van ondersteuning van een EDP-audit worden onderkend, namelijk methoden, technieken, hulpmiddelen en materiekennis.

Methode

Een methode kan worden gedefinieerd als:

'Een verzameling voorschriften en regels die werkelijk worden gehanteerd of die gehanteerd zouden moeten worden bij het uitvoeren van wetenschappelijk onderzoek of bij het oplossen van een praktijkprobleem.'



Figuur 3. Elementen van een methode.

Een methode bestaat uit een denkwijze, een werkwijze en een schrijfwijze (zie figuur 3). De denkwijze geeft weer hoe tegen een probleem wordt aangekeken. De werkwijze beschrijft de procedure volgens welke de EDP-audit dient te worden uitgevoerd en de schrijfwijze geeft aan op welk moment in de procedure welke taal (vastleggingshulpmiddel) moet worden gebruikt om de resultaten vast te leggen.

Er kan zowel voor de uitvoering als voor de beheersing van een EDP-audit gebruik worden gemaakt van een methode. Wel dient in het oog te worden gehouden dat de beheersing de uitvoering ondersteunt en niet andersom. De ontwikkeling van een methode voor de uitvoering of een aanpassing van een bestaande methode dient eventueel te leiden tot een verandering van de beheersingsmethode. Het is onjuist als een beheersingsmethode als uitgangspunt voor de ontwikkeling van een nieuwe methode voor de uitvoering wordt genomen.

Bij een methode horen technieken en hulpmiddelen.

Techniek

Een techniek is een werkvorm die de methode tastbaar en herkenbaar maakt. Volgens de dikke Van Dale is het een geheel van bewerkingen of verrichtingen, nodig om iets tot stand te brengen.

Vaak worden technieken onder het mom van een methode gebruikt. Een techniek op zich is echter nog geen methode. Een methode is een wijze van denken die eventueel ondersteund kan worden met technieken.

Hulpmiddel

Een hulpmiddel is een al dan niet geautomatiseerd produkt waarmee de toepassing van de techniek doeltreffender of gemakkelijker wordt. Technieken geven aan hoe en waarvoor de hulpmiddelen kunnen worden gebruikt.
Een referentiemodel voor een bepaald soort informatiesysteem waarin een normenstelsel voor de beoordeling van dat systeem is opgenomen, kan bijvoorbeeld ook als een hulpmiddel worden gekenmerkt.

Materiekennis

Materiekennis kent vele verschijningsvormen. In het verleden was materiekennis veelal opgeslagen in een archief of bibliotheek, tegenwoordig kunnen manuals en dergelijke worden opgenomen op CD-ROM. Daarmee kan de ontsluiting van deze materiekennis eenvoudiger plaatsvinden.

Deze vormen van ondersteuning kunnen in de toolbox worden ondergebracht. Via het opdrachtenkader zal de ontsluiting van de toolbox gerealiseerd dienen te worden.

Om te komen tot een invulling van de toolbox wordt overigens gepleit voor een sterk pragmatische invalshoek. Dit betekent dat ondanks bovenstaande vierdeling in vormen van ondersteuning, dit wellicht theoretische verschil bij de concretisering van de toolbox minder stringent gehanteerd kan worden. Relevant materiaal uit uitgevoerde EDP-audits (zoals plannen van aanpak, normstellingen, voorbeeldrapportages) kan vaak met een geringe aanpassing worden omgevormd tot een algemene tool. Een tool bestaat dan uit één of meer vormen van ondersteuning. Natuurlijk dient wel te worden voldaan aan het noodzakelijke anonieme karakter van dergelijke informatie in relatie tot de gewenste geheimhouding van klant- c.q. opdrachtspecifiek auditmateriaal. Een pragmatische invalshoek zal bij de invulling van de toolbox centraal dienen te staan, zeker als de veelheid van indelingen van het opdrachtenkader in de volgende paragraaf in ogenschouw wordt genomen.

OPDRACHTENKADER VOOR DE TOOLBOX

Het opdrachtenkader biedt een basis voor het afbakenen van een EDP-audit. Bij het kiezen van de indelingscriteria voor het opdrachtenkader dient, naast de hoofddoelstelling van het opdrachtenkader, met een tweetal (sub)doelstellingen rekening te worden gehouden, namelijk:
- alle combinaties van de criteria dienen betekenis te hebben, dat wil zeggen moeten daadwerkelijk een opdracht(soort) zijn;
- alle mogelijke opdracht(soort)en moeten door middel van de criteria kunnen worden weergegeven.

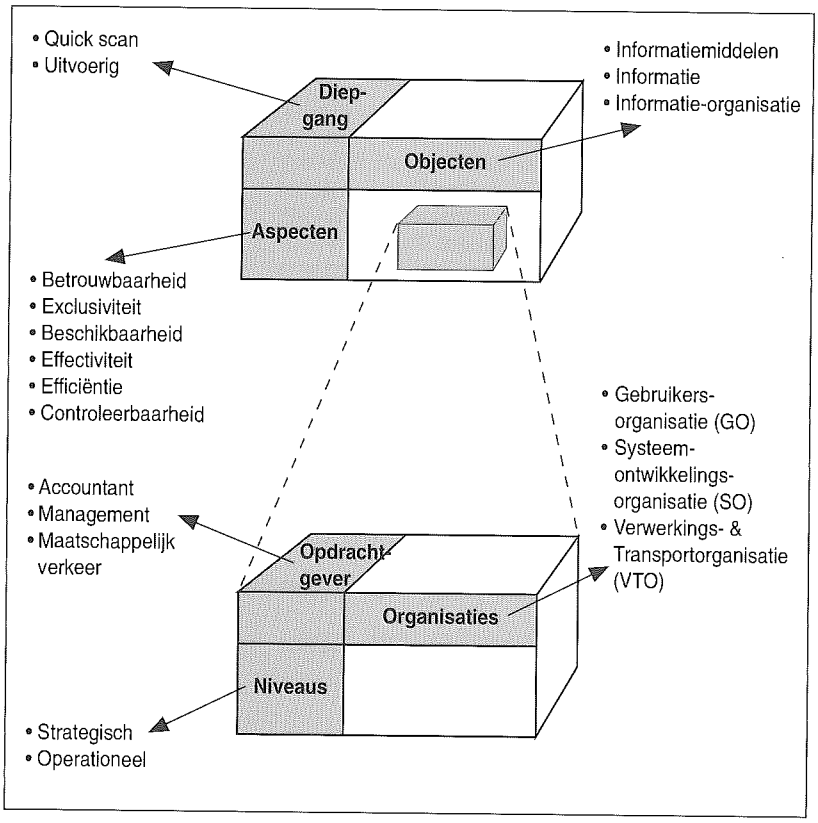
Het blijkt dat deze twee doelstellingen niet samengaan. Om de eerste doelstelling te bereiken zou het aantal criteria tot een minimum moeten zijn beperkt. Het nastreven van de tweede doelstelling heeft echter tot gevolg dat het aantal criteria toeneemt. Zoals bekend, is EDP-auditing een zich nog sterk ontwikkelend vakgebied. Vandaar dat gekozen dient te worden voor een ruime opzet van het opdrachtenkader, hetgeen betekent dat de tweede doelstelling bij de selectie van indelingscriteria wordt nagestreefd. Dit houdt in dat (vrijwel) alle mogelijke opdracht(soort)en kunnen worden weergegeven door middel van de criteria. Dit heeft echter als consequentie dat niet alle combinaties van de criteria een bepaalde betekenis hebben.

Bij de invulling van de toolbox moet een sterk pragmatische invalshoek worden gekozen.

De hierna volgende indeling bestaat uit een zestal criteria en is op basis van een combinatie van criteria die in de literatuur voorkomen (NIVRA 53, indelingen uit EDP-auditingopleidingen en dergelijke), tot stand gekomen. De criteria luiden als volgt:
a. diepgang;
b. object;
c. aspect;
d. opdrachtgever;
e. organisatiesoort;
f. organisatorisch niveau.

a. Diepgang

Het eerste onderscheid in de opdrachten van een EDP-auditor kan worden gemaakt op basis van de diepgang van het onderzoek. De ondersteuning van een diepgaand onderzoek zal wezenlijk verschillen van een quick scan ofwel een globaal onderzoek. Gezien het karakter van een quick scan-onderzoek, namelijk een kort, indicatief onderzoek, zal bij het ontwikkelen van tools voor dergelijke onderzoeken met name behoefte bestaan aan adequate pre-auditlijsten (vooraf in te vullen door de beoordeelde) en concrete vragenlijsten.
Dit criterium vertoont raakvlakken met de in EDP-auditpraktijk gebruikte indeling in opzet, bestaan en werking. Een quick scan-onderzoek zal zich naar zijn aard voornamelijk richten op de opzet van de beheersingsmaatregelen. Een diepgaand onderzoek biedt de mogelijkheden om ook aandacht te schenken aan bestaan en werking, afhankelijk van de specifieke opdrachtformulering.
Bij de uitwerking van het criterium diepgang kan of wellicht moet de relatie worden gelegd met begrippen als tolerantie en materialiteit.



Figuur 4. Opdrachtenkader voor een toolbox voor een EDP-auditor.

b. Object

Het tweede criterium is het auditobject. De objecten waar een EDP-audit zich daadwerkelijk op richt zijn informatiemiddelen (hardware, software), informatie en informatie-organisatie.

c. Aspect

Het volgende indelingscriterium is het aspect (de aspecten) van onderzoek. Een onderzoek naar de betrouwbaarheid zal waarschijnlijk anders zijn dan een onderzoek naar de effectiviteit en zal dus ook andere ondersteuning nodig hebben. Een indeling in aspecten kan zijn betrouwbaarheid, exclusiviteit, beschikbaarheid, controleerbaarheid, effectiviteit en efficiëntie.

d. Opdrachtgever

Als vierde criterium kan de opdrachtgever worden onderscheiden (managers, accountants en een derde/maatschappelijk verkeer). De invulling van een opdracht is vaak anders bij de diverse opdrachtgevers. Zo zal een onderzoek naar de betrouwbaarheid van een informatiesysteem in opdracht van het management op de bedrijfsrisico's zijn gericht, terwijl hetzelfde onderzoek in opdracht van de controlerend accountant meer zal zijn gericht op het risico dat een accountant onterecht een goedkeurende verklaring afgeeft. Een derde als opdrachtgever kan bijvoorbeeld voorkomen in de situatie van een cliënt van een servicebureau. Door het afgeven van een zogeheten 'third party announcement' bij de kwaliteit van verwerking van het servicebureau, treedt feitelijk de derde indirect als opdrachtgever op.

e. Organisatiesoort

Het vijfde criterium betreft de organisatiesoort. Een drietal organisaties wordt onderscheiden waarin een EDP-audit kan worden uitgevoerd: de gebruikersorganisatie, de systeemontwikkelingsorganisatie en de verwerkings- en transportorganisatie. Door de organisatie als indelingscriterium te onderkennen kan meer diversiteit in de mogelijke opdrachten worden aangebracht. Zo betekent de combinatie informatiesysteem en systeemontwikkelingsorganisatie (bijvoorbeeld: wordt een systeem goed ontwikkeld?) duidelijk iets anders dan de combinatie informatiesysteem en gebruikersorganisatie (bijvoorbeeld: functioneert het informatiesysteem goed?).

f. Organisatorisch niveau

Het laatste criterium is het organisatorische niveau. Hierbij kan onderscheid worden gemaakt tussen het strategische en het tactisch/operationele niveau. Een audit op strategisch niveau is primair gericht op het topmanagement; de resultaten zijn in principe bestemd voor het topmanagement en van belang voor de lange termijn. Daarentegen is een audit op (tactisch/)operationeel niveau primair gericht op het middenkader; de resultaten zijn dan ook in principe bestemd voor het middenkader en van belang voor de korte en middellange termijn.

De invulling van het onderzoek zal afhankelijk zijn van het organisatorische niveau. Een onderzoek op strategisch niveau naar de effectiviteit van de informatiesystemen zal volledig anders zijn dan hetzelfde onderzoek op operationeel niveau. Zo zal men bij het eerste onderzoek bijvoorbeeld de applicatieportfolio bekijken, terwijl bij het tweede onderzoek bijvoorbeeld de output die persoon x van het informatiesysteem krijgt, zal worden onderzocht.

Met deze indelingscriteria (zie figuur 4) is het mogelijk de verschillende opdracht(soort)en van een EDP-auditor in te delen en de diverse tools aan de opdracht(soort)en toe te wijzen. Een combinatie van alle criteria, waarbij één criterium meermalen kan voorkomen, houdt een opdracht(soort) in. Zo kan bijvoorbeeld de hardware (informatiemiddel) binnen de verwerkings- en transportorganisatie op beschikbaarheid en betrouwbaarheid, op operationeel niveau, op grond van een opdracht van het management uitvoerig worden onderzocht. Een tool kan ook op basis van de onderscheiden criteria worden ingedeeld en aldus voor één of meer opdracht(soort)en geschikt zijn.

Het is van belang te refereren aan de eerdere ver-

melding om bij de uitwerking van de toolbox vanuit een pragmatische invalshoek te werken. Bovenstaand opdrachtenkader kan daarbij wel als een 'kapstok' worden gebruikt, waarbij het overigens denkbaar is dat het aantal onderscheidende criteria wordt beperkt.

VOORBEELDEN VAN TOOLS

Tools zijn er in vele soorten en maten. Diverse informatica-, maar ook auditorganisaties hebben in de loop der jaren checklists, methoden en technieken ontwikkeld. Deze tools kunnen door EDP-auditors worden aangewend voor de uitvoering van hun werkzaamheden. Traditioneel gezien is veel aandacht geschonken aan de beveiliging van de automatisering en de daarbij behorende tools. EDP-audittools op het gebied van efficiëntie en effectiviteit zijn veel minder ver ontwikkeld.

Ondanks de grote hoeveelheid tools bestaat er binnen de beroepsgroep van EDP-auditors nog weinig consensus over algemeen erkende en bruikbare tools. Dit wordt onder andere veroorzaakt door:
- de vele ontwikkelingen in informatietechnologie en de daarbij gehanteerde informaticanormen. Normen en standaarden rondom informatietechnologie zijn nog sterk in beweging, waardoor eenduidige EDP-auditnormen moeilijk te bepalen zijn;
- onduidelijkheid over het begrip tools en de toegevoegde waarde daarvan voor een professionele dienstverlener. Er is een continu dilemma aanwezig tussen het ontwikkelen van tools en het als professional optreden;
- beperkte georganiseerdheid van de EDP-auditors, hetgeen nu via de impulsen van de NOREA kan worden veranderd.

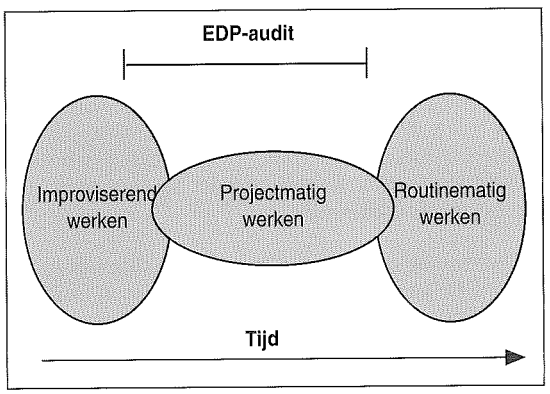
Bij het afwegen van de noodzaak tot het ontwikkelen van tools via de beroepsgroep is het van belang onderscheid te maken tussen beheersmatige en inhoudelijke ondersteuning.

TOOLS EN BEHEERSMATIGE ONDERSTEUNING

Voordat duidelijk kan worden welke EDP-auditactiviteiten met behulp van tools kunnen worden ondersteund, dient allereerst bekend te zijn hoe in een organisatie die EDP-auditactiviteiten verricht (verder EDP-auditorganisatie genoemd), wordt gewerkt.

Een drietal soorten van werken, namelijk routinematig, improviserend en projectmatig werken, kan worden onderscheiden. Van routinematig werken is sprake wanneer een bepaald resultaat herhaaldelijk dient te worden bereikt onder gelijkblijvende omstandigheden en met gelijkblijvende middelen. Routinematig werken is gericht op oplossingen en op efficiëntie. Improviserend werken is daarentegen probleemgericht, waarbij flexibiliteit hoog in het vaandel staat. Er wordt dan ook improviserend gewerkt indien er sprake is van iets volstrekt nieuws. Projectmatig werken ligt tussen deze twee uitersten in. Indien een opdracht veel nieuwe elementen bevat, mensen uit verschillende disciplines het resultaat samen moeten bereiken, er eenmalig een maximale prestatie moet worden geleverd en de middelen beperkt zijn, zal projectmatig werken voor de hand liggen. Projectmatig werken is met name gericht op effectiviteit.

Een EDP-audit kan veelal als projectmatig werken worden gekenmerkt (zie figuur 5). Vele opdrachten bevatten nieuwe elementen. De mate waarin nieuwe elementen aanwezig zijn bepaalt of de manier van werken naar het improviserende of juist het routinematige werken tendeert. Daarnaast zal er veelal sprake zijn van beperkte middelen, zal er steeds opnieuw een maximale prestatie moeten worden geleverd en zal vaak moeten worden samengewerkt met functionarissen uit andere disciplines.



Figuur 5. Verband tussen improviserend, projectmatig en routinematig werken in de tijd.

Naarmate een bepaald soort opdracht vaker wordt uitgevoerd, zal de manier van werken steeds meer het routinematig werken gaan benaderen. In de loop van de tijd kan de EDP-audit daardoor duidelijk het karakter van een routinematige aanpak gaan vertonen. Hierin schuilt echter ook het gevaar dat de daarvoor ontwikkelde tools sjabloonmatig zonder rekening te houden met de specifieke situatie worden toegepast.

TOOLS EN INHOUDELIJKE ONDERSTEUNING

Op het gebied van de inhoudelijke ondersteuning zijn, zoals eerder vermeld, diverse tools voorhanden.
Om deze tools verder te stroomlijnen zijn de genoemde studiegroepen binnen NOREA actief. Zo wenst de studiegroep Standaarden te komen tot een normering van kwaliteitseisen te stellen aan informatietechnologieprodukten en -processen. Deze

Drs. R.G.A. Fijneman
Is werkzaam als senior EDP-auditmanager bij KPMG EDP Auditors. Hij beschikt over een brede auditervaring bij een veelheid van organisaties (verschillende typologieën). De laatste jaren zijn door hem vele (strategische) adviesopdrachten op het gebied van de automatisering uitgevoerd, met name ter ondersteuning van het management in organisaties.
Hij is als docent betrokken bij opleidingen van het NIVRA (administratieve organisatie) en van de Katholieke Universiteit Brabant (post-doctoraal EDP-auditing en post-doctoraal Accountancy).

standaarden dienen een belangrijke basis te vormen bij de inhoudelijke uitwerking van tools voor EDP-auditing.
De rol van de overige studiegroepen ligt deels op het gebied van het uitwerken van de beheersmatige ondersteuning, deels echter ook op het gebied van de inhoudelijke ondersteuning. Een nadere concretisering van hun activiteiten zal in de komende tijd gestalte krijgen.

MOTIVERING VOOR ONTWIKKELINGEN IN TOOLS EN EVENTUELE BEPERKINGEN

Zowel de inhoudelijke als de onderscheiden beheersmatige activiteiten, ofwel de uitvoering en de beheersing van een EDP-audit, kunnen worden ondersteund met behulp van tools. Voor de inhoudelijke EDP-auditactiviteiten geldt enerzijds dat de ondersteuning in de vorm van tools en daarmee het belang van de tools toenemen naarmate een bepaalde EDP-audit meer het routinematig werken benadert en anderzijds dat de activiteiten juist door toepassing of ontwikkeling van tools meer routinematig worden. De wijze van gebruik van tools voor de beheersing van een EDP-audit zal moeten worden aangepast aan de manier van werken (meer improviserend of meer routinematig) bij een bepaalde EDP-audit.

De beslissing om een tool voor bepaalde inhoudelijke of beheersmatige activiteiten te gaan ontwikkelen kan op basis van een aantal factoren worden genomen, zoals:
- het aantal en de kwaliteit van soortgelijke al beschikbare tools;
- de omvang van de huidige en toekomstige werkzaamheden waarop de tool betrekking heeft;
- het aantal beschikbare ervaren EDP-auditors voor de desbetreffende activiteiten.

Indien bijvoorbeeld blijkt dat een bepaalde opdrachtsoort uit het opdrachtenkader voor een toolbox niet goed is ondersteund, de werkzaamheden sterk gaan groeien en het aantal beschikbare ervaren mensen laag is, dan betekent dit dat op korte termijn een tool moet worden ontwikkeld. Bij het ontwikkelen van tools dient nadrukkelijk ook rekening te worden gehouden met de eerder vermelde voordelen van het gebruik van tools.

Naast de vele voordelen van ondersteuning met behulp van tools dient de EDP-auditor echter ook de beperkingen hiervan in te zien. Tools ontstaan vaak doordat iemand in de praktijk tegen een probleem oploopt. Het probleem wordt opgelost en later blijkt deze oplossing ook van toepassing in andere situaties. De oplossing wordt geformaliseerd en op schrift gesteld: de tool is ontstaan.

De EDP-auditor dient echter in het oog te houden dat de bruikbaarheid van de tool bij een bepaalde EDP-audit zal afhangen van diverse situationele factoren (soort opdracht, omgeving, soort opdrachtgever, e.d.). De tool is immers ontstaan in een bepaalde omgeving en daardoor ook vaak gebonden aan de karakteristieken van de concrete problemen van die omgeving. Een tool is een oplossing op zoek naar geschikte problemen.

Het door Mintzberg aangeduide 'pigeonholing process' kan zich hierbij voordoen. Dit proces houdt in dat de professional in de professionele bureaucratie, i.c. de EDP-auditor, opdrachten zoveel mogelijk probeert te vertalen naar standaardprogramma's of tools.

Het gevaar daarbij is dat de EDP-auditor zich te veel richt op de tools die hij in zijn toolbox heeft en te weinig op de behoefte van de opdrachtgever.

Ondanks het feit dat een tool niet geschikt is voor de desbetreffende opdracht past de EDP-auditor de tool toch toe. De EDP-auditor is ten onrechte overgeschakeld van projectmatig werken naar volledig routinematig werken. Het resultaat is een ontevreden opdrachtgever en een minimale effectiviteit van de EDP-audit. Het gevaar dat dit zich voordoet wordt nog eens vergroot door het feit dat tools vaak door relatief onervaren EDP-auditors worden toegepast. De ervaren EDP-auditor die de beheersing van een opdracht op zich heeft genomen, dient aan dit gevaar dus extra aandacht te besteden.

CONCLUSIE

Het EDP-auditberoep staat voor de uitdaging via het ontwikkelen en structureren van tools het vakgebied verder te professionaliseren. Via de NOREA bestaat het platform daarvoor.

Een laatste opmerking ten slotte: de tool voert geen EDP-audit uit, dat doet de EDP-auditor al dan niet met behulp van tools. Luisteren, analyseren, beschrijven en formuleren is en blijft mensenwerk. De kwaliteit van de EDP-audit blijft afhankelijk van de vakbekwaamheid (dit is niet: ervaring), de houding en de creativiteit van de EDP-auditor. Naast een toolbox spelen dus ook elementen als opleiding, procedures en dergelijke een rol bij de kwaliteit van de produkten of diensten van een EDP-auditorganisatie.

Deze menselijke, professionele invalshoek moet het EDP-auditberoep behoeden voor het zich conformeren aan het gezegde 'If all you have is a hammer, everything looks like a nail'.

EDP AUDITORIUM

VOOR HET EERST HACKER DOOR NEDERLANDSE RECHTER VEROORDEELD

O.A.A. Somefun, met medewerking van mw.mr.drs. A.W. Duthler en drs. P. Veltman RE RA

Veroordeling op grond van computervredebreuk

Op 2 maart 1995 heeft de arrondissementsrechtbank te Utrecht de 22-jarige R.O. veroordeeld tot een geldboete van *f* 5.000 en een voorwaardelijke gevangenisstraf van zes maanden met een proeftijd van twee jaar voor het plegen van computervredebreuk (hacken). R.O. had kans gezien om zonder toestemming binnen te dringen in computers van een vijftal universiteiten, een bedrijf in Venlo en een aantal instellingen in IJsland en de Verenigde Staten.

Het bijzondere van deze uitspraak is dat het de eerste veroordeling betreft die gebaseerd is op artikel 138a Wetboek van Strafrecht (WvSr) (computervredebreuk). Het artikel maakt onderdeel uit van de op 1 maart 1993 in werking getreden Wet computercriminaliteit. Zoals de naam reeds aangeeft heeft deze wet als doelstelling computercriminaliteit te voorkomen en te bestrijden. Artikel 138a WvSr stelt strafbaar met een maximum-gevangenisstraf van zes maanden en een geldboete van *f* 10.000 als schuldig aan computervredebreuk, 'hij die opzettelijk wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens of in een deel daarvan'. Voorwaarde is dat daarbij enige beveiliging wordt doorbroken, of dat de toegang wordt verworven door 'een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid'.

In lid 3 van artikel 138a WvSr wordt aan het voorgaande nog een strafverzwarende omstandigheid toegevoegd. Indien computervredebreuk wordt gepleegd door tussenkomst van de telecommunicatie-infrastructuur en de dader vervolgens met het oogmerk zich wederrechtelijk te bevoordelen gebruik maakt van de verwerkingscapaciteit van een geautomatiseerd werk, of door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde, bedraagt de straf een hechtenis van maximaal vier jaar of een boete van *f* 25.000.
In deze zaak was sprake van het onbevoegd binnendringen door R.O. in een computer van een universiteit, waarna R.O. door tussenkomst van deze computer zich de toegang tot computers van andere universiteiten en instellingen wist te verschaffen.

Verdediging

De advocaat van R.O. voerde vijf verweren aan tegen hetgeen R.O. ten laste was gelegd. De verweren hielden in (1) dat R.O. slechts ooggetuige was van het binnendringen door een ander; (2) dat R.O. niet op heterdaad was betrapt, waardoor de vervolging onrechtmatig was; (3) dat aan de eisen van strafvervolging niet was voldaan omdat 'enige beveiliging' aan de computer ontbrak; en (4) dat er geen sprake was van het gebruik maken van een 'valse sleutel'. Tot slot voerde de advocaat het verweer aan (5) dat het ten laste gelegde feit niet strafbaar is, omdat het niet onder artikel 138a WvSr valt. Onderstaand wordt op deze vijf verweren en de reactie van de rechtbank ingegaan.

Ad 1. Andere hacker
De advocaat van R.O. voerde als eerste verweer aan dat R.O. niet aan het hacken was toen hij achter een computer op de universiteit werd aangetroffen, maar slechts aan het meekijken was op zijn eigen beeldscherm hoe iemand anders op een andere universiteit bezig was in te breken. R.O. was dus slechts ooggetuige van het binnendringen door een ander in een computer. Dit verweer werd verworpen op grond van een getuigeverklaring dat de inhoud van de onderzochte logfiles onverenigbaar is met de stelling van de advocaat.

Ad 2. Betrapt op heterdaad
Vervolgens voerde de advocaat aan dat er geen redelijk vermoeden van schuld kon bestaan (wat een voorwaarde is voor strafbaarheid) aangezien R.O. niet op heterdaad was betrapt. Dit zou betekenen dat de aanhouding en alles wat daarna volgde onrechtmatig zou zijn. Dit verweer vond ook geen gehoor, aangezien de systeembeheerder van de universiteit waar R.O. was binnengedrongen, R.O. ingelogd op het computersysteem van deze universiteit aantrof. R.O. werd dus wel degelijk op heterdaad betrapt, aldus de rechter.

Ad 3. Enige beveiliging
In het derde verweer kwam de wettelijke eis tot 'enige beveiliging' aan de orde. Indien het systeem niet volgens de eisen van de wet is beveiligd, kan een indringer niet worden vervolgd, althans niet op grond van artikel 138a WvSr lid 1a.
Volgens de advocaat was het niet duidelijk of er wel een beveiliging aanwezig was. Door deze onduidelijkheid zou niet kunnen worden bewezen dat R.O. een beveiliging had doorbroken. Als er toch sprake mocht zijn van een beveiliging diende

deze door de universiteit aangescherpt te worden, omdat enige tijd daarvoor ook al een computerinbraak had plaatsgevonden. Het argument dat de eerdere inbraak duidt op onvoldoende beveiliging werd verworpen door de rechter, omdat daarbij gebruik werd 'gemaakt van een geheel andere account van een ex-werknemer'. R.O. had gebruik gemaakt van een account van een werknemer die nog werkzaam was op de universiteit.
Volgens de rechtbank was aan de beveiligingsvoorwaarde voor strafbaarheid voldaan. Aangezien R.O. een 'account – bestaande uit een gebruikersnaam en een password – toebehorend aan een ander' meermalen heeft misbruikt, is sprake geweest van het doorbreken van 'enige beveiliging'.

Ad 4. Valse sleutel
Aan het voorgaande verweer werd door de raadsman toegevoegd dat de verdachte geen gebruik had gemaakt van een valse sleutel om binnen te dringen, welk feit ook onderdeel uitmaakte van de tenlastelegging. De rechtbank wijst dit verweer af door te verwijzen naar vaste rechtspraak waar het onbevoegd gebruik maken van een sleutel deze sleutel vals maakt. De verdachte was niet gerechtigd of gemachtigd de account van een ander zonder diens toestemming te gebruiken en heeft derhalve gebruik gemaakt van een valse sleutel.

Ad 5. Strafbaarheid
Tot slot wordt door de advocaat van de verdachte aangevoerd dat het door zijn cliënt gepleegde feit niet strafbaar is, omdat in de tenlastelegging wordt gesproken van 'het binnendringen in een computer' en niet van 'het binnendringen in een geautomatiseerd werk'. Volgens de raadsman is in artikel 80 sexies WvSr, het definitie-artikel van geautomatiseerd werk, niet omschreven dat onder een geautomatiseerd werk ook computers moeten worden verstaan.
De rechtbank verwerpt dit verweer, omdat volgens de memorie van toelichting (MvT) het begrip geautomatiseerd duidt op 'een functioneren van het werk, dat voor een deel onafhankelijk is van menselijk ingrijpen. Hieronder vallen onder meer computers of netwerken van aan elkaar verbonden computers.'
De wetgever heeft met het oog op mogelijke nieuwe technologische ontwikkelingen de term geautomatiseerd werk gebruikt in plaats van computer. Indien dergelijke ontwikkelingen zich voordoen is vervolging nog steeds mogelijk ([NORE94], p. 68).

Interpretatie vonnis

Zoals uit bovenstaande beschrijving van de verweren blijkt, zijn alle verweren door de rechtbank verworpen. De rechtbank verklaarde bewezen dat R.O. zich schuldig heeft gemaakt aan computervredebreuk in de zin van artikel 138a WvSr.
In onderstaande beschouwing wordt nader ingegaan op enkele overwegingen van de rechtbank. Aangezien voor deze bespreking van het vonnis slechts de verkorte versie ter beschikking stond, blijft een aantal vraagpunten onbeantwoord.

Ad 1. Andere hacker
Het verweer van de advocaat dat een andere hacker de inbraak zou hebben uitgevoerd, wordt door de rechtbank verworpen op grond van een getuigeverklaring dat de inhoud van de onderzochte logfiles onverenigbaar is met deze stelling.

Nu is bekend dat logfiles manipuleerbaar zijn, en een hacker die in staat is de door de advocaat beweerde acties uit te voeren (het geven van commando's – vermoedelijk met PC-anywhere – vanaf een andere locatie, waarvan R.O. via zijn beeldscherm ooggetuige was) moet zeker in staat worden geacht tot zulke manipulaties.
Aangezien in het verkorte vonnis slechts een beperkte omschrijving van het bewijsmiddel is opgenomen, kan niet worden nagegaan hoe de onverenigbaarheid met de stelling van de advocaat is beargumenteerd, en in hoeverre de manipuleerbaarheid van de logfiles in overweging is genomen.

Ad 3. Enige beveiliging
Met een beroep op de memorie van toelichting stelt de rechtbank dat voor het voldoen aan de eis van het doorbreken van enige beveiliging, het van belang is 'of degene die de computer binnendringt door het doorbreken van de beveiliging, heeft blijk gegeven de wetenschap te hebben gehad dat hij een beveiligd systeem binnendringt en doelbewust enige inspanning heeft gedaan de beveiliging te doorbreken'. De rechtbank was van mening dat aan die voorwaarde voor het ontstaan van strafbaarheid was voldaan, 'nu de verdachte meermalen een account – bestaande uit een gebruikersnaam en een password – toebehorend aan een ander heeft misbruikt'.

Theoretisch is denkbaar dat de account slechts diende voor 'accounting'-doeleinden, dat wil zeggen om de kosten van computergebruik door te belasten, maar niet om de computer, of bestanden en programma's binnen de computer, te beveiligen tegen onbevoegde toegang. Het gebruik maken van andermans account zou dan niet zozeer het doorbreken van enige beveiliging zijn, als wel het zich wederrechtelijk bevoordelen ten koste van een ander. Aannemelijk is echter dat ook sprake is van 'enige beveiliging' bij een account voor accounting-doeleinden.
Ook is denkbaar dat de toegang openstond voor gasten, met een account als 'gast gast'. Zou R.O. ook een strafbaar feit hebben gepleegd als hij zich had aangemeld als 'gast' in plaats van zijn eigen gebruikersnaam? Of behoort een dergelijke account niet toe aan een ander, maar aan een ieder?

Behandeling van het wetsontwerp
De discussie over het vereiste beveiligingsniveau voor strafbaarheid zal nog wel enige tijd voortduren. Ook ten tijde van het wetsonderwerp is hierover uitvoerige gedachtenwisseling geweest.

Volgens de MvT hoeft er niet meer te zijn dan een mimimale, doch wel een daadwerkelijke beveiliging ([TK91], p. 16). De MvT spreekt hier ook wel van een reële beveiligingseis, waarbij het niet nodig is dat zij adequaat is. Met een adequate beveiliging wordt bedoeld dat het evenwicht tussen de mate van beveiliging en het te beveiligen belang gelijk is. Een beveiliging die bijvoorbeeld is aange-

bracht door middel van een elektronisch bordje 'verboden toegang', met als enige doelstelling het mogelijk maken hackers te vervolgen, is een zogenaamde pro forma beveiliging en is niet voldoende beveiliging in de zin van artikel 138a WvSr, volgens de MvT.

Voorts werd aan een dergelijke beveiliging door de minister een dynamisch karakter verbonden. Door de veranderende techniek is het mogelijk dat wat eens een adequate beveiliging was, in een later stadium niet meer adequaat zal zijn. Hetzelfde kan zich voordoen bij een reële beveiliging. Een beveiliging die eens aan de eisen van een minimale beveiliging voldeed, kan door veranderingen in de techniek op een bepaald moment niet meer als een minimale beveiliging worden aangemerkt. Er zou dan geen sprake meer zijn van een reële beveiliging, met als gevolg dat vervolging niet meer mogelijk zou zijn, omdat niet meer aan de wettelijke eis van 'enige beveiliging' zou zijn voldaan.

Dit laatste punt trof enige kritiek tijdens de behandeling in de Tweede Kamer. In de memorie van antwoord op de Wet computercriminaliteit (MvA) wordt naar aanleiding van deze kritiek deels afstand genomen van de omschrijving van reële beveiliging:
'Ik neem hiermee afstand van de uitlatingen in de memorie van toelichting dat het moet gaan om een reële beveiliging en van de daaraan verbonden beschouwing over het dynamische karakter van de beveiliging, althans wat betreft de strafrechtelijke relevantie daarvan', aldus de minister ([TK91-1], p. 32).

De eis van een reële beveiliging wordt dus afgezwakt in de MvA. In de Nota Naar Aanleiding van het Eindverslag wordt de inhoud van de afzwakking nader toegelicht. Er wordt in deze nota een expliciet handelen vereist van de rechthebbende van de computer. 'Er zal een kenbare drempel moeten bestaan zodat onbevoegden zich niet simpelweg de toegang kunnen verschaffen. Deze drempel bestaat uit een maatregel die erop gericht is het systeem te beschermen tegen het binnendringen door onbevoegden. Wat de inhoud van een dergelijke maatregel is laat zich moeilijk omschrijven, daar deze kan variëren naar tijd, plaats, stand van de techniek en de inhoud van de gegevens die beveiligd moeten worden' ([TK92-1], p. 18). Hier wordt vermoedelijk mee bedoeld dat indien technische veranderingen het eenvoudiger maken om een beveiliging te doorbreken, hier niet automatisch de conclusie aan moet worden verbonden dat niet meer aan de eisen van 'enige beveiliging' is voldaan. Dit betekent dat, anders dan wat uit de eerdere omschrijving in de MvT voortvloeide, in een dergelijke situatie vervolging van de indringer nog wel mogelijk is.

Ad 4. Valse sleutel
Het verweer van de advocaat dat geen gebruik is gemaakt van een valse sleutel wijst de rechtbank af met een verwijzing naar vaste rechtspraak. De rechtspraak waarnaar vermoedelijk wordt verwezen, is opgenomen in de MvA. Het betreft een arrest van de Hoge Raad van 20 mei 1986 (NJ 1987, 130), waarin werd beslist dat een huissleutel een valse sleutel is indien deze wordt gebruikt tot opening van een slot door iemand die daartoe niet gerechtigd is. Het is niet noodzakelijk dat ten aanzien van de sleutel enige beveiligingsmaatregel is genomen en het is voldoende dat tegen de wil van de rechthebbende de sleutel uit zijn macht verloren is gegaan. De MvA voegt hier nog aan toe dat indien de hacker een password van een bulletinboard haalt en daarmee vervolgens computervredebreuk pleegt, hij ook strafbaar is. Het maakt hierbij niet uit of er sprake is van nalatigheid van de zijde van de computerbeheerder, die ondanks dat hij weet dat het password openbaar is, nalaat de beveiliging aan te passen ([TK91-1], p. 31).
In de MvA geeft de Minister van Justitie nog als toelichting: 'Ik ga er daarbij van uit dat een password een sleutel is die de gebruiker toegang geeft tot het systeem of tot een deel daarvan' ([TK91-1], p. 31).

Voor een goed begrip van deze problematiek is het van belang te onderkennen dat een password op twee verschillende manieren voor beveiliging kan worden gebruikt:
- object-gebonden, dat wil zeggen dat het password is gekoppeld aan het beveiligde object, en dat iedereen die (al dan niet legitiem) kennis heeft van het password, het beveiligde object kan binnendringen. Het 'password' is een 'passeerwoord'. Deze functie van een password is inmiddels in onbruik geraakt;
- subject-gebonden, dat wil zeggen dat het password is gekoppeld aan het subject (de persoon) dat het beveiligde object wil binnendringen. Het password dient ter verificatie van de identiteit van het subject en is vergelijkbaar met een paspoort (als middel om de identiteit te bewijzen). Of het subject, nadat de identiteit is geverifieerd, daadwerkelijk binnen mag, hangt af van de bevoegdheden die zijn gekoppeld aan de gebruikersnaam (identiteit).

De Minister van Justitie, en de rechtbank in navolging van hem, lijken te zijn uitgegaan van eerstgenoemd gebruik van een password, terwijl in casu kennelijk sprake was van de tweede functie. Dit zou inhouden dat niet zozeer sprake was van het gebruiken van een valse sleutel, als wel van het aannemen van een valse hoedanigheid.

Voor de bewezenverklaring van de tenlastelegging zou het overigens geen verschil maken. In de tenlastelegging was ook het aannemen van een valse hoedanigheid aangevoerd.

Slotbeschouwing

Aangenomen dat het eerste verweer terecht is afgewezen – hetgeen aannemelijk is, het verhaal over de andere hacker klinkt nogal onwaarschijnlijk – lijkt de bewezenverklaring van computervredebreuk terecht, zij het mogelijk op de verkeerde gronden. Zoals uit bovenstaande beschouwing blijkt, zou doorslaggevend zijn het aannemen van een valse hoedanigheid, hetgeen in de tenlastelegging was opgenomen, maar waartegen geen verweer is aangevoerd. Het doorbreken van een beveiliging is aannemelijk, maar er kunnen vraagte-

kens bij worden geplaatst, terwijl het gebruiken van een valse sleutel op een misvatting van de password-functie in deze casus lijkt te berusten.

Voor zover bekend is inmiddels hoger beroep aangetekend tegen het vonnis van de rechtbank. Wellicht zal in dit hoger beroep meer duidelijkheid ontstaan over de gerezen vraagpunten.

Literatuur

[NIVR93] NIVRA, *Computercriminaliteit: De wetgeving, de gevolgen voor bedrijven en de accountant*, NIVRA-geschrift nr. 62, Kluwer Bedrijfswetenschappen, 1993.

[NORE94] NOREA, *Studierapport, De Wet computercriminaliteit*, mei 1994.

[NVIR91] NVIR-studiegroep computercriminaliteit, *Rapport computercriminaliteit, Een reactie op het wetsontwerp Computercriminaliteit*, juli 1991.

[TK90] Tweede Kamer, vergaderjaar 1989-1990, *Memorie van Toelichting*, 21 551, nr. 3.

[TK91-1] Tweede Kamer, vergaderjaar 1990-1991, *Memorie van Antwoord*, 21 551, nr. 6.

[TK91-2] Tweede Kamer, vergaderjaar 1990-1991, *Nota van Wijziging*, 21 551, nr. 7.

[TK91-3] Tweede Kamer, vergaderjaar 1990-1991, *Gewijzigd Voorstel van Wet*, 21 551, nr. 8.

[TK92-1] Tweede Kamer, vergaderjaar 1991-1992, *Eindverslag*, 21 551, nr. 10.

[TK92-1] Tweede Kamer, vergaderjaar 1991-1992, *Nota Naar Aanleiding van het Eindverslag*, 21 551, nr. 11.

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.

1 20e jaargang 93/1 lente 1993

Netwerkmanagement, de organisatorische opzet en financiële beheersing
Ir. E.J. Evelo

Akzo en telecommunicatie, de organisatorische ontwikkeling
H. Reijn

SURFnet, beveiliging in een open netwerk
E. Zegwaart

Beveiliging van digitale kieslijnen
Drs.ing. D. Brouwer

Secure Cash Management; an audit perspective
M. Kennett BA

Nieuwe ontwikkelingen in de cryptografie: Kerberos en Digital Signature Standard
Drs. T.P. de Vries

Beveiligingsperikelen rondom Novell NetWare
J.L. Ramos Najera

2 20e jaargang 93/2 zomer 1993

Informatietechnologie duur? I/T Assessment: een beproefde methode voor het beoordelen van effectiviteit en efficiëntie van de informatieverzorging
Drs. B.T. Janssen, ing. W.J.D. Koot en ir. E.J. Mutsaers

Prioriteitenstelling met Decision
Dr. P.J. van Meel RI

De audit van een IT-investeringsaanvraag
Drs.ing. S.R.M. van den Biggelaar en drs. P.P.M.G.G. Brouwers

Verzekerbaarheid van automatiseringsrisico's
Mw.mr.drs. A.W. Duthler

Beveiligingsstandaard voor informatiesystemen
Prof.dr.ir. R. Paans RE

Global electronic mail: integratie van elektronische post met X.400
Ir. A. van Kooij

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 systeem-ontwikkeling
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 multi-disciplinaire 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-management-systemen
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

4 21e jaargang 94/4 winter 1994

Geautomatiseerde gegevensbewerking en jaarrekeningcontrole
R.A. Jonker RA

De invloed van informatietechnologie op de interne-controleprincipes
J.C. Boer RE RA

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
Informatiebeveiliging van theorie naar praktijk
Drs. P. Veltman RE RA

Informatie(beveiligings)beleid in concernverband
Prof. A.W. Neisingh RE RA

1 22e jaargang 95/1 lente 1995

Internetworking; beheerproblematiek en security-risico's
H. Roos RA en ir. M.T.H. Heesbeen

Geïntegreerd netwerkbeheer
Ing. W.A.A. Zoon

Client/server geconcretiseerd
J.C. van Praat RE RA

Radio-LAN's in de praktijk
Ir. B.J. Busropan, ir. G.J. de Groot, ir. W. Hollemans, ir. E.C. den Toom en ir. A. Verschoor

3DAS-kenmerk, een uniek middel voor identificatie en authenticatie
Ir. W.H.M. Sipman RI

2 22e jaargang 95/2 zomer 1995

Het beheer van PC-netwerken
Drs.ing. R.F. Koorn CISA

Multimedia nader bekeken
Drs. A.M. Buren

Introductie van een bancair systeem in een wide area netwerk-omgeving
W.N.P. Zethof RE RA

GEBIT. Gestructureerd Evalueren van de Baten van IT-investeringen
Mw. M.S. Hablous