DE ROL VAN DE INTERNE AUDITOR BIJ SYSTEEMONTWIKKELING

Roger MERCKEN

Roger Mercken promoveerde in 1987 tot doctor in de Toegepaste Economische Wetenschappen (K.U. Leuven) op basis van een proefschrift over de gevolgen van de data-base benadering voor de interne controle. Hij is hoogleraar bedrijfseconomie aan de Economische Hogeschool Limburg te Diepenbeek en verricht hoofdzakelijk onderzoek op twee brede terreinen: enerzijds bedrijfseconomische aspecten van de informatica (en dan vooral op het raakvlak tussen informatica en accountancy of administratieve organisatie) en anderzijds administratieve organisatie in KMO's.

Samenvatting

De rol van de interne auditor bij de ontwikkeling van nieuwe toepassingssystemen is nog steeds niet duidelijk afgelijnd. In theoretische benaderingen leidt dat tot zeer principiële discussies. In de praktijk wordt het hele spectrum van totale afzijdigheid tot een intense, bijna onvoorwaardelijke, participatie waargenomen. Dit artikel probeert op een pragmatische wijze de grenzen van de participatie te bepalen en na te gaan welke fasen in de systeemontwikkeling daartoe het meest geschikt zijn.

Economisch en Sociaal Tijdschrift, jaargang 1989, nr. 5, blz. 541

Inleiding

Systeemontwikkelingscontroles moeten zorgen voor een betrouwbaar ontwikkelingsproces van betrouwbare toepassingssystemen. Een betrouwbaar toepassingssysteem is een systeem dat de uit te voeren functies doeltreffend uitvoert, waarbij de nodige aandacht wordt geschonken aan de beveiliging tegen niet-geautoriseerd gebruik, semantische en fysische integriteitscontroles en de controleerbaarheid («auditability»). Daarnaast zijn de ontwikkelingscontroles erop gericht die kwalitatief hoogstaande systemen op tijd en binnen het middelenbudget tot stand te brengen.

De concrete doelstellingen van systeemontwikkelingscontroles zijn ertoe bij te dragen:
- dat alle systeemontwikkelingsactiviteiten op de juiste manier zijn geautoriseerd, getest, nagekeken, gedocumenteerd, uitgevoerd en goedgekeurd;
- dat de van toepassing zijnde standaarden, procedures en richtlijnen correct geformuleerd zijn en op de juiste wijze werden toegepast;
- dat de ontwikkelde systemen de nodige controles bevatten en controleerbaar zijn;
- dat de ontwikkelde systemen onderhoudbaar zijn, en de bovengenoemde kenmerken ook na een onderhoudsbeurt bewaren.

Klassiek onderscheidt men in de systeemontwikkelingscontroles de volgende elementen:
- participatie van en goedkeuring door het management en de verantwoordelijke gebruikers;
- het opstellen en toepassen van ontwikkelingsstandaarden, met inbegrip van de standaarden op het vlak van controle en controleerbaarheid;
- het project management;
- het testen van het systeem;
- conversie-controles;
- post-installatie audit.

I. AUDITING EN CONTROLEERBAARHEID

A. Interne audit

De interne audit functie kan worden omschreven als een onafhankelijk gedifferentieerd controleorgaan dat door de hoogste ondernemingsleiding wordt ingesteld om de opzet en de werking van het interne controlesysteem te beoordelen en advies te verstrekken voor de verbetering ervan. De Internal Auditor rapporteert rechtstreeks aan de hoogste leiding of aan het Audit Comité van de Raad van Bestuur. De «officiële» definitie van het Institute of Internal Auditors: «internal auditing is a managerial control which functions by measuring and evaluating the effectiveness of other controls.» (Statement of Responsibilities of Internal Auditors, paragraaf 1) legt duidelijk de nadruk op de betekenis van interne audit als «controle op de controle». Dit geldt uiteraard ook voor de EDP-audit. De EDP-audit functie is een onderdeel van de interne audit functie dat in het bijzonder belast is met de controle op de opzet en de werking van geautomatiseerde delen van informatiesystemen. Vele auteurs definiëren EDP-auditing erg breed, doch vernauwen het toepassingsveld uiteindelijk tot het aspect betrouwbaarheid. De gezaghebbende definitie van Van Zutphen luidt als volgt: «EDP-auditing is de onafhankelijke beoordeling en bewaking van zowel de opzet als de werking van geautomatiseerde informatieverzorgende systemen, met name voor zover het betreft de aspecten betrouwbaarheid, effectiviteit en efficiency.» (Van Zutphen, 1979, blz. 97), maar constateert daarbij: «in de praktijk blijkt tot nu toe toch op de betrouwbaarheidsbeoordeling en bewaking (...) het zwaartepunt te liggen.» Dit werd trouwens door Peek (Peek, blz. 192) empirisch bevestigd.

B. Controleerbaarheid

Controleerbaarheid («auditability») heeft betrekking op de eigenschappen van het informatiesysteem, die controle op de goede werking ervan mogelijk maken (Van Zutphen, 1985, blz. 160-165). Het is niet voldoende dat een systeem betrouwbaar en beveiligd is, maar het moet deze eigenschappen ook op een controleerbare wijze bezitten. Een positieve uitspraak over de beveiliging en betrouwbaarheid van een systeem is per definitie onmogelijk als die beveiliging en betrouwbaarheid niet kan worden gecontroleerd. Controleerbaarheid is overigens een alternatief voor preventieve maatregelen die erop zijn gericht ongewenste situaties onmogelijk te maken. Uitsluiten van ongewenste gebeurtenissen kan meestal

slechts indien de betrokken gebeurtenissen op voorhand duidelijk te identificeren zijn. Alle fouten en inbreuken op voorhand voorzien is uiteraard onmogelijk. Bovendien is het steeds mogelijk de in het systeem ingebouwde preventieve controles te omzeilen. Naarmate die ontwijkingskansen belangrijker worden verschuift daarom ook het accent van een controle vooraf naar een controle achteraf en wint de kwaliteit van het controlespoor aan belang.

II. ONAFHANKELIJKHEID EN INTERVENTIE

Van bij het prille begin van de automatisering werd erkend dat de interne auditor niet voorbij kan gaan aan het systeemontwikkelingsproces. Over de aard en de diepgang van zijn interventie bestaat echter nog steeds geen eensgezindheid. Sommigen wensen die interventie absoluut te minimaliseren, teneinde de onafhankelijkheid van de auditor niet in gevaar te brengen. Anderen daarentegen verdedigen een maximale interventiepolitiek. Tot bij het begin van de jaren tachtig kon men deze discussie nog als enigszins academisch of principieel afdoen. De grote meerderheid van de toenmalige toepassingssystemen waren relatief eenvoudig, en ook achteraf, op een conventionele manier te controleren. Een eventuele niet-participatie in de systeemontwikkeling van de interne auditor hoefde m.a.w. niet tot fundamentele controleproblemen te leiden, hoewel de doeltreffendheid en de doelmatigheid van de controle wel negatief konden worden beïnvloed. Het grootste nadeel van het zich afzijdig houden was wellicht dat de interne auditor een unieke kans miste om leerervaring op te doen.

De jaren tachtig, met data-base management technieken, netwerken, gedistribueerde informatieverwerking en een begin van expertsystemen hebben voor een hele reeks van toepassingen het accent verlegd. De informatiesystemen gaan steeds meer *onvervangbare* interne controlemaatregelen omvatten. Zoals De Lange (De Lange, blz. 352-354) opmerkt: «toepassing van kunstmatige intelligentie zal uiteindelijk leiden tot dermate gecompliceerde verschijningsvormen van niet door mensen genomen beslissingen dat controle achteraf door de accountant met verbandslegging op gegevensniveau niet mogelijk of niet doelmatig zal blijken. Deze tendens leidt tot het veelvuldiger voorkomen van steeds grotere delen onvervangbare interne controle in geautomatiseerde systemen,

waardoor de accountant in steeds mindere mate kan volstaan met de toepassing van verbands- en totaalcontroles. De gegevensgerichte controlebenadering zal in toenemende mate worden vervangen door de systeemgerichte controlebenadering. De gegevensgerichte controle door verbands- en totaalcontroles zal op grond van doelmatigheidscriteria door de computer worden toegepast om die fouten tijdig te ontdekken die bij verdere voortgang niet meer kunnen worden hersteld.» Hoewel de grote meerderheid van de systemen momenteel nog steeds als puur conventioneel kan worden bestempeld, is de evolutie onmiskenbaar en onvermijdelijk.

Controleerbaarheid moet vanaf het begin in de informatiesystemen worden ingebouwd. De interne auditor dient zijn wensen tijdig en volledig kenbaar te maken. Participatie van de (EDP-)auditor is dan onvermijdelijk geworden. Toch blijft de vraag bestaan hoever de auditor daarin moet gaan.

Functioneel is de (EDP-)auditor bij de systeemontwikkeling onvermijdelijk controleur en adviseur tegelijkertijd. Dat kan zijn onafhankelijkheid in het gedrang brengen en tot een rollenconflict leiden: als adviseur ontwikkelt hij een positief samenwerkingsverband met de geadviseerde die hij helpt in zijn functie-uitoefening; als controleur spoort hij inbreuken op en rapporteert ze aan zijn opdrachtgevers. Die duale rol geldt uiteraard voor alle controlerende functies, maar zeker voor een auditor geldt dat het geven van advies er niet mag toe leiden dat hij zijn *onafhankelijkheid* prijsgeeft. De adviserende taak van de auditor is functioneel ondergeschikt aan zijn controlerende taak. Daarom is het uitgesloten dat de (EDP-)auditor wordt ingeschakeld in om het even welke operationele activiteiten. Uit de aard van het ontwikkelingsproces zelf vloeit de noodzaak voort dat de auditor de gewenste controle- en controleerbaarheidskenmerken tijdig formuleert. Eenmaal het systeem in aanbouw is of voltooid, is het aanbrengen van bijkomende controles niet enkel buitensporig duur of erg moeilijk te realiseren, doch vaak ook niet effectief. Een systeem dat niet met beveiligings- en controleerbaarheidsoogmerken werd gebouwd, kan onmogelijk via achteraf aangebrachte maatregelen waterdicht worden gemaakt. Zowel de beoordeling van de ingebouwde controles als de specificatie van de door de auditor gewenste audit modules (om het systeem controleerbaar te maken) moeten de fasering van het ontwikkelingsproces volgen. Deze noodzakelijke vroege tussenkomst van de EDP-auditor als expert in interne controle schept het gevaar dat hij adviezen gaat verstrekken die hij achteraf zelf moet beoordelen. Omdat het ontwikkelingsproces bestaat uit een groot aantal stappen, waarbij elke stap voortbouwt op de opties die in de vorige stap werden

genomen, zullen adviezen die in de beginfase werden gegeven in latere stappen nog moeilijk kunnen worden gekeerd.

Sommige auteurs stappen vrij licht over dat verlies aan onafhankelijkheid heen:

«Viele Revisoren schrecken bei der Vorstellung zurück, dass sie durch diese Mitwirkung Verantwortung übernehmen. Es ist sicher richtig, dass die interne Revision zu einem sehr frühen Zeitpunkt in die Mitverantwortung kommt. Dies muss aber auch von der Revision her positiv bewertet werden.» (Nagel, blz. 33)

«Many auditors are anxious about involvement at the design stage (...) they see it as jeopardising their independence. However, in reality it is no different in principle to making audit recommendations at any stage during audit work: on a later occasion the auditor hopes he will encounter systems which incorporate the recommendations he made earlier.» (Chambers, blz. 291).

Het Statement of Responsibilities of Internal Auditors is veel voorzichtiger: «Objectivity is essential to the audit function. Therefore, internal auditors should not (...) engage in any (...) activity which they would normally review and appraise and which could be reasonably construed to compromise the independence of the internal auditor. The internal auditor's objectivity need not be adversely affected, however, by determining and recommending standards of control to be applied in the development of the systems and procedures being reviewed.» (Statement, op. cit.)

In feite verlegt deze uitspraak het accent in de participatie van de auditor: hij moet geen individuele controles voorstellen of aanbevelen, doch wel algemenere controlestandaarden en -normen.

Dat een consensus nog ver zoek is blijkt bijv. uit de volgende twee uitspraken:
«participation by the Internal Audit Department in systems development is highly questionable» (De Marco, blz. 23)
«Het is de specifieke taak van de EDP-auditor ervoor te zorgen dat reeds in de eerste fasen van de systeemontwikkeling volle aandacht wordt geschonken aan de interne-controle-problematiek» (Frielink, blz. 222).

Wij hebben de indruk dat de «participationisten», althans in de literatuur, momenteel het overwicht hebben verworven. Zo schrijft Vasarhelyi (Vasarhelyi, blz. 296): «An internal auditor should be a member of the systems development team, review specifications to ensure the adequacy of proposed controls, and participate in the development of specific controls».

Wij zijn nochtans geen voorstander van een overdreven rolomschrijving. Een auditor moet zich o.i. vooral richten op zijn kernfunctie, d.i. het toezicht uitoefenen op de betrouwbaarheid en controleerbaarheid van de informatiesystemen. Dat er in het loop van het proces ook aanbevelingen op het vlak van doeltreffendheid en doelmatigheid van zowel het systeemontwikkelingsproces als de ontwikkelde systemen worden gegeven, doet geen afbreuk aan die basisfunctie. De auditor moet er zich ook voor hoeden zich in de plaats te gaan stellen van de systeemontwikkelaars. Het ontwikkelen van goede en betrouwbare informatiesystemen is in de eerste plaats hun verantwoordelijkheid, en zij moeten ervoor zorgen dat daartoe alle nodige maatregelen genomen worden, met inbegrip van de keuze van een goede systeemontwikkelingsmethode en de uitbouw van een behoorlijke kwaliteitsverzorgingsfunctie.

De wijze van *taakuitoefening* van de auditor kan variëren van (a) actieve participatie als lid van de projectgroep over (b) participatie als lid van de stuurgroep tot (c) onafhankelijke toetsing op formele beslissingspunten (bijv. bij de oplevering van het systeem) (Pon, blz. 221-227).

Wij stellen voor dat de EDP-auditor een reeks algemene *controlestandaarden* (controlenormen) voorstelt die door de ontwikkelingsafdeling *zelfstandig* worden toegepast. De ontwikkelingsafdeling moet over een eigen EDP-intern-controlespecialist beschikken. De EDP-auditfunctie zal vertegenwoordigd zijn in de stuurgroep, om op die wijze op de hoogte te blijven van de stand van zaken en zich optimaal voor te bereiden op een *onafhankelijke* toetsing op enkele belangrijke mijlpaalpunten, met de nadruk op betrouwbaarheid, beveiliging en controleerbaarheid. In de rest van het artikel zullen wij nagaan welke fasen in de systeemontwikkelingsmethodiek het meest in aanmerking komen voor die toetsingen, zonder daarbij naar volledigheid te streven.

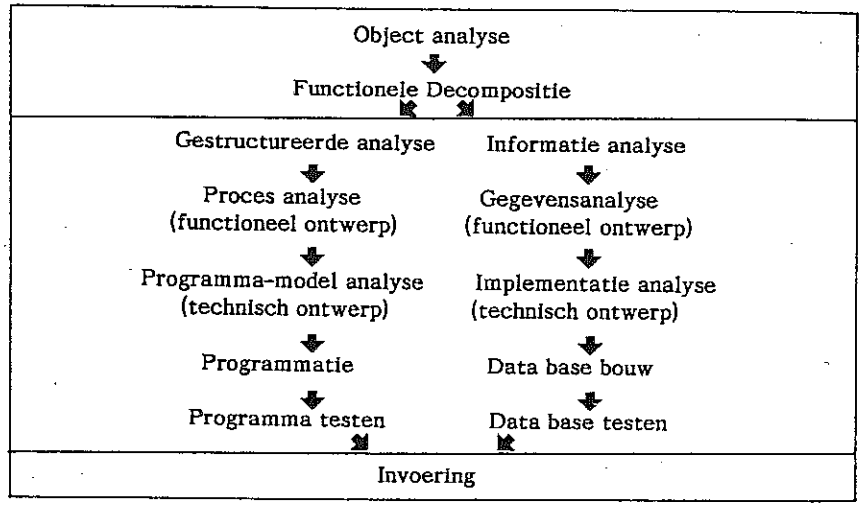
III. CONTROLEPUNTEN IN DE SYSTEEMONTWIKKELINGSMETHODOLOGIE

A. Systeemontwikkelingsmethodologie

Het uitbouwen van een systeem van interne controle wordt in al zijn aspecten beïnvloed door de gebruikte *systeemontwikkelingsmethodologie.* Uiteraard gaat onze aandacht daarbij vooral uit naar een streven om die fasen in de methodiek te identificeren die bijzonder geschikt zijn voor het inlassen van *controlepunten,* en naar het specificeren van de aard van de controles die het meest zijn aangewezen.

Recente systeemontwikkelingsmethodologieën vervangen de conventionele benadering (systeemanalyse, systeemontwerp, programmering, testen) door een oplossing die een duidelijk onderscheid maakt tussen enerzijds *data* en *processen,* en anderzijds tussen een gerichtheid op *conceptuele* (reële wereld) en *implementatie* («computerwereld») aspecten. Wij zullen ons in dit artikel uitsluitend richten op de datacomponent (cfr. figuur 1).

Figuur 1: Schematische voorstelling van de systeemontwikkelingsmethodologie

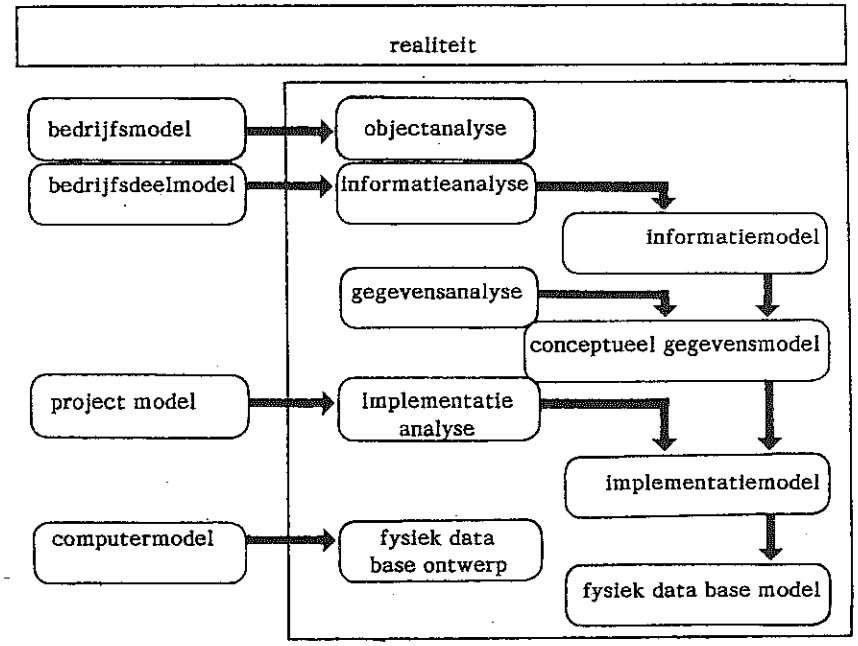


Vertrekkende van de objectanalyse, die het volledige bedrijf als analysevoorwerp heeft, beperken de daarop volgende fasen zich telkens tot een nauwkeurig afgelijnd onderdeel van het voorwerp van de vorige fase. Op deze wijze kan men vrij snel tot operationele resultaten komen, zonder daardoor evenwel te vervallen in het oude probleem van de geïsoleerde ontwikkeling van toepassingssystemen. Elk nieuw ontwikkeld systeem kadert in een globale aanpak op het hogere niveau, wat borg staat voor een goede integratie.

Met de nadruk op de controleaspecten van het specifiek data-georiënteerd gedeelte zullen wij proberen aan te geven welke aspecten in de diverse fasen relevant zijn voor het verrichten van controles, c.q. het inbouwen van controlesystemen.

De analyse- en ontwerpfase werd door Vandenbulcke (Vandenbulcke, blz. 41) uitgewerkt als in figuur 2.

Figuur 2: Schematische voorstelling van de datacomponent



In elk stadium wordt gewerkt op een deelverzameling van het object in het vorige stadium. Hierna zullen wij kort ingaan op de inhoud van de opeenvolgende fasen m.b.t. de datacomponent, met telkens een situering t.o.v. de daarmee overeenstemmende procescomponent.

B. Fasering

1. Objectanalyse en functionele decompositie

Een *objectanalyse* (of bedrijfsanalyse) is een analyse van het objectsysteem (het bedrijf, de realiteit waarvan/waarvoor een automatiseringsinspanning gebeurt) met het doel aard en omvang van de te automatiseren deelsystemen af te lijnen en aan de deelsystemen een prioriteit toe te kennen in het kader van het automatiseringsplan op lange termijn. Het voorwerp van deze analyse is de organisatie als geheel. Uitgangspunt is een studie van de onderneming die weergeeft hoe een organisatie werkt en wat vereist is om die werking te ondersteunen.
Bedrijfsprocessen worden ondersteund door, en communiceren via, informatie-elementen. Op deze wijze kan een interactie/isolatiematrix van de verschillende bedrijfsprocessen worden opgesteld. Bedrijfsprocessen die een beroep doen op veel gemeenschappelijke gegevens kunnen worden samengenomen in deelsystemen waarvoor een informatiesysteem zal worden ontwikkeld.

Door «business processen» als uitgangspunt te kiezen, vertoont deze fase van de methodologie nogal wat overeenkomst met audit-technieken als «*transaction flow auditing*». In beide methodes gaat men uit van fundamentele bedrijfsprocessen die over de grenzen van organisatorische indelingen en de daarrond gebouwde toepassingssystemen heen, doorheen de hele organisatie worden bestudeerd. Zulks opent nieuwe perspectieven voor de samenwerking tussen de systeemontwikkelingsafdeling en de interne auditor. De diepgang van de objectanalyse en vooral de hierop volgende functionele decompositie levert erg interessant materiaal op voor een evaluatie van de bestaande toestand van het interne-controlesysteem. In zowel de controle-, de automatiserings- als de EDP-audit-literatuur wordt aan die mogelijkheid evenwel voorbijgegaan. In de systeemontwikkelingsmethodes wordt meestal een evaluatiefase van de bestaande toestand opgenomen, zonder echter specifiek aandacht te schenken aan interne controle. In de EDP-audit-methodologie vindt men wel richtlijnen voor een evaluatie van de toegepaste ontwikkelingsmethodes, doch *niet* voor het gebruik van de analyseresultaten voor controledoeleinden.

Tijdens de functionele decompositie worden de in het deelsysteem voorkomende functies tot een *activiteitenprofiel* ontleed. Hierbij wordt gebruik gemaakt van een afbakening van deelsystemen zoals deze op grond van de objectanalyse is verkregen. Het *activiteitenprofiel* geeft aan welke de activiteiten zijn waarvoor representatieve personen in functies verantwoordelijkheid dragen en vormt het uitgangspunt voor informatie- en gestructureerde analyse.

Activiteitenprofielen die vanuit interne-controlestandpunt incompatibel zijn door vermenging van de aspecten beschikken, bewaren, registreren, uitvoeren en controleren of de plaatsing van een volledig transactietraject onder de bevoegdheid van één functionaris, kunnen hier betrekkelijk eenvoudig worden geïdentificeerd. Evalueren van het interne-controlesysteem behoort tot de opdracht van de interne-auditafdeling. Er is o.i. geen enkele reden om in deze fase geen gebruik te maken van de specialistische kennis ter zake van de Internal Auditor. Die evaluatie brengt de onafhankelijkheid van de auditor op geen enkele wijze in het gedrang.

De auditor die de *bestaande* organisatie en functieomschrijvingen beoordeelt en zwakke punten signaleert blijft volledig in zijn onafhankelijke rol. Naar onze mening is het veel doeltreffender en doelmatiger het interne-controlesysteem goed af te stellen *voordat* nieuwe informatiesystemen worden ontwikkeld, dan achteraf in die systemen allerlei beveiligingen in te bouwen. Aan het ontwikkelen van nieuwe informatiesystemen kan een herverdeling van verantwoordelijkheden worden gekoppeld, waarbij controletechnisch onverenigbare taken worden vermeden.

Om conflicten tussen de verschillende activiteiten op te sporen werden in de literatuur verschillende hulpmiddelen voorgesteld (Mercken, 1987), maar dit valt buiten het doel van dit artikel.

2. Informatie-analyse

Het activiteitenprofiel is het startpunt voor de gestructureerde analyse en de informatie-analyse. Doel van de *gestructureerde analyse* is het aangeven van de globale in- en uitgaande informatiestromen die tussen de activiteiten van functies bestaan. Het resultaat daarvan is een dynamisch functiemodel van het betreffende deelsysteem. Doel van de *informatie-analyse* is het aangeven van informatie- en informatiestructuurelementen die nodig zijn voor het uitvoeren van een activiteit. Het resultaat ervan is een informatiemodel dat de relevante informatiebehoeften van de geautoriseerde gebruikers van het deelsysteem weergeeft binnen de vereisten van de activiteiten waarvoor zij verantwoordelijkheid dragen. Informatie-analyse maakt hierbij rechtstreeks gebruik van de resultaten van functionele decompositie.

De informatie-analyse bestaat uit 2 fasen: informatie-analyse van activiteiten en ontwerp van het informatiemodel.

a) informatie-analyse van activiteiten

Tijdens deze fase worden activiteiten geanalyseerd in verband met de geïmpliceerde informatiebehoeften, waarna de informatiebehoeften worden ontleed in informatie-elementen (entiteitentypen, kenmerken van entiteitentypen) en informatiestructuurelementen (associaties tussen kenmerken van entiteitentypen).

b) ontwerp van het informatiemodel

De in de vorige deelfase opgespoorde informatie- en informatiestructuurelementen dienen te worden gesynthetiseerd tot een informatiemodel voor het afgelijnde deelsysteem.

Naar onze mening heeft de fase van de informatie-analyse *minder controlebelang*. Uiteraard is ze uiterst belangrijk in het kader van de systeemontwikkeling, doch er hoeven hier vanuit controle-oogpunt t.o.v. de complementaire gestructureerde analyse geen bijkomende normen of werkwijzen te worden opgelegd. Andere fasen zijn beter geschikt voor het controlewerk.

3. Gegevensanalyse (data-analyse)

De in de vorige fase op globaal niveau voorgestelde modellen worden in de opvolgende fase van procesanalyse en data-analyse tot op het laagste niveau gedetailleerd. Doelstelling van de *procesanalyse* is het analyseren van de functies op taakniveau en het aangeven van de frequentie waarmee, het tijdstip waarop en de voorwaarden waaronder die taken moeten worden verricht. Het resultaat daarvan is een procesmodel. Complementair onderneemt men de *data-analyse*. Het doel van deze fase is: «het representeren van informatiebehoeften door middel van gegevens en gegevensstructuren die zijn samengevat in een stabiel, effectief en automatiserings-onafhankelijk conceptueel gegevensmodel.» (Vandenbulcke, blz. 45).

Daarbij worden drie doelstellingen nagestreefd:

- het opstellen van een éénduidige functionele specificatie van elk informatie-element;
- het zodanig structureren van de gegevensverzameling dat onregelmatigheden bij updaten, schrappen en toevoegen worden voorkomen;
- het beperken van de kansen op herstructurering bij toekomstige uitbreiding van de gegevensverzameling.

De invloed van de kwaliteit van de data-analyse op de betrouwbaarheid van de ontwikkelde informatiesystemen is zeer groot en een *concentratie* van de *controle*werkzaamheden in deze fase is dan ook aangewezen.

Wij stellen daartoe twee duidelijk verschillende voorschriften voor:

- de bij het *specificatie-onderzoek* gehanteerde methodiek moet voldoende plaats inruimen voor het vastleggen van de kwaliteitsparameters van de informatie, het opstellen van éénduidige *bevoegdheidsschema's* (wie is verantwoordelijk voor wat?) en de specificatie van *controlevoorzieningen;*
- bij de verdere fasen dient gebruik te worden gemaakt van een *betrouwbare methodiek* voor het structureren van een gegevensverzameling.

In de fase van de data-analyse zijn drie *deelfasen* te onderscheiden:

a) data-specificatie (standaardgegevensnamen)

Veel gebruikte entiteiten en kenmerken krijgen standaardgegevensnamen en hun betekenis wordt vastgelegd, in overleg met de betrokken gebruikers en automatiseringsdeskundigen. Op dat ogenblik kan ook inzicht worden verkregen in de bestaande gegevens*redundantie*. Een onderscheid moet worden gemaakt tussen werkelijke en vermeende overeenkomsten, en overtolligheid die men specifiek inbouwt om de controleerbaarheid te verhogen. Daar een van de doelstellingen van de data-base benadering precies is ongewenste gegevensovertolligheid te vermijden, is het voor de auditor van het grootste belang tijdig aan te geven welke redundantie hij onmisbaar vindt om zijn controle doeltreffend te kunnen uitoefenen.

b) data-structuur manipulatie

Bij de huidige ontwikkelingsstand kan het gebruik van de zgn. normalisatiestappen als dwingend worden voorgeschreven, aangezien deze methode haar theoretische en praktische superioriteit duidelijk heeft bewezen. Deze methodologie is een stapsgewijs proces waarmee men in staat is om een willekeurige informatiebehoefte te verdelen in een aantal genormaliseerde groepen. Het voordeel van de normalisatie is dat een aantal anomalieën bij het toevoegen, weglaten of wijzigen van gegevens worden voorkomen. Onvolledige normalisatie kan achteraf volkomen onverwachte, en dus per definitie door het testprogramma en het interne-controlesysteem niet voorziene problemen veroorzaken. Dergelijke problemen zijn uiterst moeilijk op te sporen en kunnen bij eventueel herstel tot ingrijpende herstructureringen leiden. Niet toepassen van normalisa-

tie, of een equivalente techniek, moet o.i. beschouwd worden als een ernstige bedreiging van de betrouwbaarheid van de aldus ontwikkelde informatiesystemen. Indien men bij de systeemontwikkeling om efficiëntie- of andere redenen afwijkt van de genormaliseerde resultaten, is het de taak van de auditor erop toe te zien dat men de gevolgen van die afwijking grondig heeft onderzocht en gedocumenteerd. Het opstellen van semantische integriteitsregels (controles op het realiteitsgerichte karakter van de gegevens) en formele controleregels heeft slechts zin na afloop van de normalisatie, daar deze normalisatie de structuur van de gegevens erg kan veranderen.

c) conceptueel gegevensmodel

Hier is geen specifieke audit-inbreng.

4. Programmamodel-analyse en implementatie-analyse

Doelstelling van de fase programmamodel-analyse (processen) en implementatie-analyse (data) is het opstellen van het *technisch ontwerp* van het deelsysteem. De voorgaande fasen waren gericht op het «wat», terwijl deze fase gericht is op het «hoe». Door middel van de programmamodel-analyse worden de procesmodellen omgezet in programmamodellen. Een programmamodel is een gedetailleerde beschrijving van de modules waaruit het programma zal bestaan en hun onderlinge verhouding (interfaces en oproepsequenties). Het doel van de implementatie-analyse is het documenteren van het conceptueel model (of een onderdeel ervan) met kenmerken betreffende de verwachte aard en het gebruik van de gegevens en gegevensstructuren. Men onderzoekt de wijze waarop processen (programmamodellen) het conceptueel model gebruiken ter ondersteuning van activiteiten. Per procesmodel, gesitueerd binnen het betreffende kader, wordt een antwoord gegeven op vragen betreffende de gebruikskenmerken (waar, hoe, met welke frequentie/cyclus).

Beveiligings- en controlevereisten kunnen nu erg *specifiek* worden gedetailleerd, waardoor deze fase een *hoog controlebelang* verwerft: de toepassing van de geldende algemene beveiligings-, controle- en controleerbaarheidsrichtlijnen wordt hier geconcretiseerd.

Drie deelfasen worden onderscheiden:

- basis-implementatie-analyse;
- statische implementatie-analyse;
- dynamische implementatie-analyse.

Enkel de eerste deelfase heeft o.i. een specifiek controlebelang.

Na afloop van de basis-implementatie-analyse beschikt men over een volledig, gedetailleerd overzicht van de geautoriseerde informatiebehoeften. De toepassing van het principe van de kleinste benodigde machtiging («need to know») leidt ertoe dat het informatiesysteem dusdanig moet zijn ingericht dat voldaan wordt aan alle geautoriseerde gegevensbehoeften, doch ook niet meer dan die behoeften. Daar de analyse van de beveiligingsbehoeften erg gedetailleerd moet gebeuren, ligt het voor de hand die analyse te baseren op een *formeel toegangscontrolemodel* (Mercken, 1988). De modelmatige voorstelling van de beveiligingsbehoeften laat toe de toegangscontroleregels op te slaan in de vorm van een toegangscontrole data-base, die dan op een eenvoudige manier kan worden ondervraagd.

In dit stadium kan de auditor als deskundige in de interne controle een produktieve inbreng doen.

Een aanpak in twee fasen is hier aangewezen. In een eerste stap wordt een kruisclassificatie van activiteiten (gegroepeerd per functie) tegenover gegevens- en gegevensstructuurelementen gemaakt. Dat kan praktisch gezien enkel door een goed DD/DS worden afgeleverd. In de tweede stap worden de resultaten van de vorige stap omgezet in concrete beveiligingsvereisten op het vlak van toegangscontroles.

Dit is ook de meest geschikte fase om voorstellen te doen m.b.t. de concrete uitwerking van de in de vorige fase voorgestelde semantische integriteitsregels en formele controles. Dit gebeurt nog steeds op een modelmatige manier, die m.a.w. onafhankelijk is van de gekozen uitvoeringstechnieken. Door het niet-technische karakter van deze fase is het voor de auditor goed mogelijk in deze fase te participeren en de voorgestelde regels te evalueren. Men hoeft geen deskundige in data-base technieken te zijn om een oordeel te kunnen uitspreken over de mate waarin het ontwerp rekening heeft gehouden met de aspecten controle, beveiliging en controleerbaarheid. Voorwaarde hiertoe is wel een strikte scheiding tussen ontwerp- en uitvoeringsbekommernissen.

5. Fysiek data-base ontwerp

Op de fase van het technisch ontwerp volgt de *bouwfase*. Programmamodellen worden door middel van gestructureerde programmeringstechnieken omgezet in operationele programma's die, ingevolge de data-base benadering, refereren aan de fysieke data-bases, zonder echter de gegevensbeschrijving in het programma zelf te verwerken. De omzetting van het implementatiemodel naar een performant fysiek data-model is niet zo rechtlijnig omwille van performantie-overwegingen en de door het

DBMS opgelegde structuurbeperkingen. Naast overwegingen op het vlak van de hardware staat hier het data-base model (ook data-base architectuur genoemd) centraal. Het data-base model bepaalt hoe men de gegevens- en gegevensstructuurelementen in een data-base kan organiseren. De in de praktijk gehanteerde data-base modellen (IMS-hiërarchisch, netwerk, relationeel) vertonen nogal wat verschillen op het vlak van de controle- en beveiligingsmogelijkheden. Ook binnen één data-base model, zoals bijv. het relationele, zijn er grote verschillen tussen de verschillende Data-Base Management Systemen. Deze fase is sterk technisch bepaald. Voor de auditor komt het erop aan bij de afloop van deze fase vast te kunnen stellen of de door hem beoordeelde modelmatige controles op de juiste wijze werden uitgevoerd. Gezien het technische karakter van deze fase is het aangewezen hier te kunnen beschikken over duidelijke implementatiestandaarden, waaraan door de automatiseringsafdeling strikt de hand wordt gehouden. De toetsing door de auditor zal dus enerzijds gebaseerd zijn op het vaststellen van de mate waarin de EDP-afdeling beschikt over, en zich houdt aan, de betreffende standaarden, en anderzijds uit het testen van de eerder opgestelde regels.

Besluit

De interne auditor in het algemeen en de EDP-auditor in het bijzonder dienen betrokken te zijn bij de ontwikkeling van nieuwe systemen. Een afwachtende houding aannemen om nadien de ontwikkelde systemen in alle onafhankelijkheid te kunnen beoordelen is niet te verdedigen. Bij geavanceerde systemen is het gevaar groot dat niet-participatie zal leiden tot onherstelbare gebreken op het vlak van betrouwbaarheid, beveiliging en controleerbaarheid. De onvervangbare rol van de auditor op het vlak van vooral het laatste kenmerk is zonder meer duidelijk. Een overdreven participatie, zoals die in sommige enquêtes en EDP-audit werken tot uiting komt, waarbij de auditor actief aan de concrete ontwikkeling deelneemt, moet echter eveneens worden vermeden. Een audit is en blijft een onafhankelijke controle op de controle. Eveneens pleiten wij voor een voorzichtige opstelling op het vlak van de te controleren aspecten. De nadruk moet liggen op betrouwbaarheid, beveiliging en controleerbaarheid. Budgetcontrole, de efficiëntie van de gebruikte ontwikkelingsmethodiek e.d. zijn uiteraard belangrijke elementen, die echter eerder tot een specifieke DP-audit moeten worden gerekend dan tot de hier besproken «normale» participatie van de auditor.

Bibliografie

CHAMBERS, A.D., «Current Strategies for Computer Auditing Within an Organisation», *The Computer Journal,* vol. 24(4), 1981, blz. 290-294.

DE LANGE, H., «De betekenis van EDP-auditing voor de functie van de externe accountant», *De Accountant,* nr. 7, maart 1989, blz. 352-354.

DE MARCO, V.F., «EDP Development! Should The Internal Auditor Participate?», *The Internal Auditor,* juni 1979, blz. 19-25.

FRIELINK, A.B., «De rol van de accountant bij het automatiseringsgebeuren», *De Accountant,* december 1983, blz. 218-225.

HYDE, G.E., «Role Models for Internal Auditing», *The Internal Auditor,* april 1980, blz. 65-72.

MERCKEN, R., *De invloed van de data base benadering op de interne controle,* doctoraal proefschrift, KU-Leuven, 1987, 346 blz.

MERCKEN, R., «Toegangscontrole in een data base omgeving», *Accountancy en Bedrijfskunde* (kwartaalschrift), juni 1988, blz. 19-39.

NAGEL, K., «Ordnungsmässigkeit und Revisionsfähigkeit der Datenverarbeitung», *IBM Nachrichten,* nr. 246, 1979, blz. 29-35.

PEEK, W.G., «EDP audit in de openbare accountantspraktijk», *De Accountant,* november 1983, blz. 190-193.

PON, J.W., «De participatie van de controlerend accountant in de systeemontwikkeling», *De Accountant,* november 1978, blz. 221-227.

SAWYER, L.B., «Janus or The Internal Auditor's Dilemma», *The Internal Auditor,* december 1980, blz. 19-27.

Statement of Responsibilities of Internal Auditors, The Institute of Internal Auditors, 1976.

VANDENBULCKE, J.A., *Data base systemen voor de praktijk* (derde editie), Kluwer, Deventer-Antwerpen, 1984, 262 blz.

VAN ZUTPHEN, L.C., «EDP Audit – Quo Vadis?», *De Accountant,* oktober 1979, blz. 196-102.

VAN ZUTPHEN, L.C., «EDP Auditing; een poging tot verduidelijking», *MAB,* november/december 1985, blz. 160-165.

VASARHELYI, M.A., LIN, T.W., *Advanced Auditing,* Addison-Wesley Pub. Cy, 1988.