ICT-aspecten bij de accountantscontrole van de routinematige transactie-verwerking

J.C. Boer RE RA

In organisaties van enige omvang is de verwerking van routinematige transacties een in hoge mate geautomatiseerd proces. Deze inleiding geeft een visie op de mate waarmee en de wijze waarop de accountant systeembeoordelingen en onderzoeken van de algemene computercontroles in zijn werkzaamheden moet betrekken.

Inleiding

De werkzaamheden die nodig zijn voor de controle van de jaarrekening zijn van velerlei aard. Voor de planning van de werkzaamheden wordt veelal een onderscheid gemaakt tussen controlewerkzaamheden gericht op het verwerkingsproces van de routinematige transacties en de werkzaamheden gericht op de samenstelling van de jaarrekening. Dit artikel behandelt de accountantswerkzaamheden gericht op het vaststellen van de betrouwbaarheid van de routinematige transactieverwerking. In organisaties van enige omvang is de verwerking van routinematige transacties een, in hoge mate, geautomatiseerd proces. In de ogen van de auteur ontbreekt het echter aan een sluitende theorie die een basis legt voor de mate waarin en de wijze waarop in de accountantscontrole van de routinematige processen, de gebruikte informatietechnologie (IT) moet worden betrokken. In dit artikel wordt een aanzet gegeven voor een sluitende theorievorming. Tevens is de intentie een basis te leggen voor een praktisch werkkader voor collega's die bij de uitvoering van hun werkzaamheden met dit vraagstuk worden geconfronteerd.

Drie systeemcomponenten

De verwerking van de financiële en logistieke transactiestromen kenmerkt zich door een vaste systematiek die zich over het algemeen bij uitstek leent voor een systeemgerichte controlebenadering. Het begrip systeem moet hierbij ruim worden opgevat en bestaat uit de volgende componenten:

* de menselijke handelingen en verdeling van de verantwoordelijkheden;
* de geautomatiseerde informatiesystemen;
* de technische infrastructuur.

De wijze waarop de drie componenten afzonderlijk moeten worden beoordeeld, is in theorie en praktijk in ruime mate uitgewerkt. De inrichting van organisaties is een vraagstuk dat wordt behandeld in de literatuur met betrekking tot de administratieve organisatie. Over de opzet van internecontrolefunctionaliteiten in informatiesystemen is slechts in beperkte mate specifieke literatuur aanwezig. Door het belang dat managers hechten aan een goede controlestructuur is in de praktijk waar te nemen dat interne controle en beveiliging in implementatietrajecten als één van de randvoorwaarden worden meegenomen. Met betrekking tot de wijze waarop systemen beoordeeld kunnen worden, is een scala van methoden beschikbaar. Ook de inrichting en de beoordeling van de interne controle en beveiligingsmaatregelen in de technische infrastructuur en de daarmee verbonden administratieve organisatie zijn ruimschoots uitgewerkt.

De drie genoemde gebieden worden bij het inrichten van een audit veelal als losstaand beschouwd. De eerste systeemcomponent 'menselijke handelingen en verdeling van de verantwoordelijkheden' is een gebied dat door alle accountants kan worden afgedekt. In veel situaties is dit niet voldoende om tot een oordeel over de beheersing van de verwerking van de routinematige transacties te komen. Voor een effectieve controle zullen ook de relevante informatiesystemen en de technische infrastructuur in de beoordeling moeten worden betrokken. Wat betreft de wijze waarop dit moet worden opgepakt, wijzen accountants en IT-auditors naar elkaar zonder tot een realistisch en algemeen aanvaard werkprotocol te komen. In het *Handboek EDP Auditing* en het *Handboek Accountancy* vindt u over dit onderwerp (nog) geen artikel, in het boek *IT Auditing* van Van Biene-Hershey wordt aangegeven dat het de verantwoordelijkheid van de financial auditor is te bepalen welke IT-auditwerkzaamheden noodzakelijk zijn; verdere richtlijnen ontbreken. Ook in CobIT is niets opgenomen over de wijze waarop de objectives en audit guidelines kunnen bijdragen aan een oordeel over de betrouwbaarheid van het bovenliggende informatieverwerkende proces. Het NIVRA-studierapport 'Normatieve maatregelen voor de geautomatiseerde gegevensverwerking' handelt over de samenhang, maar er wordt aan de oplossing een uitwerking gegeven die niet aansluit op de dagelijkse praktijk. Helaas heeft het studierapport niet geleid tot de discussie die de samenstellers van het rapport hadden willen initiëren.

Samenhang

Tot nu toe zijn publicaties met betrekking tot de betekenis van de betrouwbaarheid van de informatie- en communicatietechnologie (ICT)[1] in het kader van de accoun-

1) Kort samengevat alle techniek die wordt gebruikt voor het verwerken van gegevens (programmatuur, netwerken, hardware, enz.).

tantswerkzaamheden gericht op het certificeren van de jaarrekening sterk beredeneerd vanuit de ICT. De betrouwbare werking van de general ICT controls moet worden vastgesteld als randvoorwaarde om in de controle te kunnen steunen op de beheersingsmaatregelen die deel uitmaken van de geautomatiseerde informatiesystemen.

Vaststellen van de betrouwbaarheid van ICT vanuit de gebruikersomgeving is logischer dan vanuit de verwerkingsomgeving.

Over het algemeen wordt er in de literatuur zonder meer van uitgegaan dat de betrouwbare *werking* van de ICT moet worden vastgesteld. Naast het ontbreken van een onderbouwing waarom de beoordeling zich op de werking moet richten, laten de budgetten voor de accountantscontrole een dergelijk onderzoek niet toe. Nu mag een budget vaktechnisch gezien geen belemmering zijn om werkzaamheden niet uit te voeren, maar een toename van de accountantswerkzaamheden past niet in het doel van het gebruik van ICT: 'het minder arbeidsintensief maken van processen en het efficiënt kunnen afhandelen van grote transactievolumes'. (Met als kanttekening de randvoorwaarde dat de ICT op een adequate wijze is georganiseerd.)
In de praktijk zien we dan ook dat accountants, uitzonderingen daargelaten[2], om de problemen met betrekking tot het vaststellen van de betrouwbaarheid van de ICT heen lopen. Uit gesprekken met vele vakgenoten is op te maken dat zij hun oordeel over de betrouwbaarheid van de door de cliënt gebruikte ICT veelal baseren op de mate waarin zich in het verleden incidenten hebben voorgedaan. Bij gebrek aan incidenten wordt nogal eens teruggevallen op de veronderstelling dat het proces betrouwbaar is verlopen. In deze redenering wordt dus impliciet gesteund op de wijze waarop de gebruikers in staat zijn geweest de betrouwbaarheid van de gegevensverwerking vast te stellen.

2) Bij banken, door het DNB-memorandum.

Het verschil tussen theorie en praktijk is ontstaan doordat in de theorievorming niet is geredeneerd vanuit de gebruikersomgeving. Zoals hierna zal worden aangetoond, wordt de onduidelijkheid weggenomen door te redeneren vanuit de gebruiker, via de systemen naar de ICT-infrastructuur. Deze redenering geeft een duidelijk inzicht welke beoordelingswerkzaamheden met welke diepgang moeten worden uitgevoerd.
Voor de theorievorming ligt een startpunt in de gebruikersomgeving meer voor de hand dan een start vanuit de ICT; dit kan worden beargumenteerd vanuit de doelstelling van de accountantscontrole. Het doel is de getrouwheid van de jaarrekening vast te stellen. Een 'halffabrikaat' is de informatie die uit de routinematige processen komt; de betrouwbaarheid van het 'halffabrikaat' is één van de grondstoffen om tot een getrouwe jaarrekening te komen. Een zelfstandig oordeel over de werking van de systemen en de ICT-organisatie wordt, uit hoofde van de jaarrekeningcontrole, niet aan de accountant gevraagd en deze heeft een dergelijk oordeel, zoals uit het vervolg van dit artikel blijkt, vaktechnisch gezien ook niet nodig.

In de volgende paragrafen worden de genoemde componenten (menselijke handelingen, informatiesystemen en technische infrastructuur) nader uitgewerkt. De opbouw van het betoog is zo gekozen dat duidelijk wordt waarom bepaalde controlewerkzaamheden noodzakelijk zijn. Begonnen wordt met de menselijke controlehandelingen gevolgd door de beheersingsmaatregelen in de informatiesystemen. Deze opbouw wijkt af van de logische volgorde waarin de beoordelingswerkzaamheden over het algemeen worden uitgevoerd. De uitvoering van de werkzaamheden zal beginnen met de beoordeling van de informatiesystemen. Deze volgorde is nodig omdat anders niet kan worden bepaald welke inherente en internecontrolerisico's aan het systeem zijn verbonden en welke geprogrammeerde controles door gebruikers moeten worden opgevolgd. De verificatie van de veronderstelling van een adequate automatiseringsorganisatie en betrouwbare technische infrastructuur in de planningsfase van de controle wordt in dit artikel als laatste behandeld, in de praktijk is dit dikwijls de eerste stap. In de praktijk wordt hierdoor voorkomen dat te laat wordt vastgesteld dat de opzet van de automatiseringsorganisatie en technische infrastructuur niet aan de eisen voldoet.

Menselijke (controle)handelingen

Onbetrouwbare registraties van de logistieke en financiële transacties leiden ertoe dat informatievoorziening aan het management niet meer overeenkomt met de werkelijkheid, hetgeen het risico met zich meebrengt dat besluiten worden genomen die niet leiden tot een optimale bedrijfsvoering (bijvoorbeeld grondstoffen worden te vroeg of te laat besteld). Onafhankelijk van de wijze van gegevensverwerking blijven functionarissen binnen een organisatie verantwoordelijk voor de juistheid en volledigheid van de informatieverwerking. Vanuit deze verantwoordelijkheden worden binnen organisaties maatregelen getroffen om de betrouwbaarheid te waarborgen. Voorbeelden hiervan zijn invoer-, verbands- en uitvoercontroles.

Ook al is informatieverwerking in hoge mate geautomatiseerd, er blijven uitzonderingssituaties bestaan die niet (geheel) door het systeem afgehandeld kunnen worden. Ondanks de geprogrammeerde controles en de general ICT controls kunnen fouten ontstaan als het systeem in situaties komt waarmee bij de ontwikkeling en het testen geen rekening is gehouden. Verder is het mogelijk dat door onvolkomenheden in het testen fouten onopgemerkt blijven. Dit is in zijn geheel niet denkbeeldig; dat het onmogelijk is om informatiesystemen volledig te testen behoeft voor de meeste lezers geen toelichting. Naast de in de vorige alinea aangehaalde controlemaatregelen gericht op de normale procesgang, zal het management controlemaatregelen hebben getroffen om vast te stellen dat systeemfouten tijdig worden gesignaleerd.

De routinematige processen resulteren in informatie die de basis legt voor het opstellen van de jaarrekening. De accountantscontrole richt zich in deze fase van de controle op het vaststellen van de betrouwbaarheid van deze informatie. De eerste stap is de vaststelling van de wijze waarop de organisatie zelf de betrouwbaarheid van deze informatie bewaakt. De tweede stap is het kennisnemen van de binnen de organisatie uitgevoerde analyses om de betrouwbaarheid van de in de informatiesystemen vastgelegde gegevens vast te stellen.
Bij accountants is over het algemeen veel kennis en ervaring aanwezig voor het uitvoeren van de hiervoor beschreven gebruikerscontroles (door Starreveld c.s. aangeduid met 'informatiecontrole[3]'; omdat dit de doelstelling van de controle duidelijk weergeeft zal deze term in het vervolg van het artikel worden gebruikt).
Indien de accountant bij zijn beoordeling tot de conclusie komt dat de controlewerkzaamheden door de gebruiker onder de maat zijn, zal hij de organisatie aanzetten tot het uitvoeren van de noodzakelijke analyses of zelf overgaan tot het uitvoeren van aanvullende controlewerkzaamheden. De hier bedoelde accountantswerkzaamheden bestaan uit het uitvoeren van cijferanalyses (waaronder het leggen van verbanden) en gerichte detailcontroles.
De doelstelling van dit onderdeel van de accountantscontrole is zekerheid te verkrijgen over de getrouwheid van de door de informatiesystemen opgeleverde informatie. Bewust is gekozen voor de formulering 'getrouwheid ... informatie', hetgeen betekent dat geen absolute zekerheid nodig is maar zekerheid die ligt binnen de controletolerantie. Zolang het de informatie zelf betreft is het tolerantiebegrip goed hanteerbaar. Voor de beoordeling van systemen en organisaties ligt het hanteren van toleranties moeilijker. Hierop wordt in de volgende paragrafen teruggekomen.

Door het uitvoeren van informatiecontroles stelt de gebruiker van het systeem de betrouwbare werking doorlopend vast. Dit doet de gebruiker vanuit zijn/haar eigen verantwoordelijkheid ten aanzien van de juistheid en volledigheid van de informatieverwerking. Deze informatiecontrole is een prima aangrijpingspunt voor de accountantscontrole. Zowel voor de gebruiker als voor de accountant geldt dat de controles in het informatiesysteem van voldoende gehalte moeten zijn om deze te kunnen gebruiken voor de vaststelling van de betrouwbaarheid van de informatieverwerking. Het informatiesysteem zal de internecontrolefunctionaliteit in zich moeten hebben die nodig is om de betrouwbare werking te kunnen vaststellen. De systeembeoordeling die nodig is om vast te stellen dat alle foutkansen worden afgedekt (in accountantstermen de volledigheid en juistheid van de controlemaatregelen), wordt in de volgende paragraaf uitgewerkt.

Om de waarnemingen met betrekking tot de toereikendheid van de internecontrolemaatregelen in de informatiesystemen om te kunnen vormen tot een beeld dat geldt voor een langere tijdsperiode, is het noodzakelijk dat:
* de toegangsautorisatiemechanismen adequaat zijn;
* de verwerkingslogica (de programma's) niet ongeautoriseerd verandert.

Deze maatregelen liggen binnen de automatiseringsorganisatie. Om de toereikendheid van de maatregelen vast te stellen zal in aanvulling op de beoordeling van de door de gebruikers uitgevoerde informatiecontroles en de systeembeoordeling, een beoordeling van de general ICT controls plaats moeten vinden. De mate waarin dit nodig is, zal in één van de volgende paragrafen worden uitgewerkt.

Beheersingsmaatregelen in informatiesystemen

Over de wijze waarop controles binnen de organisatie moeten worden uitgevoerd, is van oudsher binnen het accountantsberoep veel ervaring opgedaan; dit aspect krijgt ook ruimschoots aandacht in de accountantsopleiding. Anders ligt het bij de beoordeling van de volledigheid van de controlefunctionaliteiten in de systemen die ten grondslag liggen aan de informatievoorziening. Hiervoor is inzicht nodig in de toereikendheid van de geprogrammeerde controles.

De controles in het informatiesysteem moeten zodanig zijn ontworpen dat zij de operationele gebruiker en het management de mogelijkheid bieden de informatieverwerking onder controle te houden. Belangrijke controlepunten zijn:
* de acceptatie van de ingevoerde gegevens (zowel handmatig als digitaal);
* de volledigheid en juistheid van door het systeem geïnitieerde acties;
* de volledigheid en juistheid van de opgeslagen gegevens;
* de informatieverstrekking (zowel leesbaar als digitaal).

Een gedetailleerde behandeling van deze onderdelen valt buiten de reikwijdte van dit artikel. Thans wordt volstaan met het verwijzen naar normenkaders die op deze punten bij systeemonderzoeken worden gehanteerd.

De internecontrolemaatregelen in de geautomatiseerde onderdelen van de informatiesystemen worden aangeduid met geprogrammeerde controles. Deze controles zijn niet direct zichtbaar. Het is één van de functionaliteiten van het geautomatiseerde deel van de gegevensverwerking. Om inzicht te krijgen in de geprogrammeerde controles moet kennis worden genomen van het systeem. Dit kan door middel van documentatie maar ook door demonstraties en gesprekken met gebruikers. Het in zijn volle omvang doorgronden van een informatiesysteem is geen eenvoudige opgave.

Voor een beoordeling van de verwerking van de routinematige transacties binnen de kaders van de accountantscontrole past een integrale beoordeling van alle in het systeem opgenomen beheersingsmaatregelen niet. Dit zou, binnen de doelstelling van de accountantscontrole, veel te veel omvatten, hetgeen niet efficiënt is. Een toespitsing moet worden gemaakt op de processen die raakvlakken hebben met de informatiestromen die van belang zijn voor de accountantscontrole. Op basis van risicoanalyse moet worden bepaald welke maatregelen noodzakelijk zijn om te waarborgen dat de geautomati-

3) De controle op de betrouwbaarheid van door het informatiesysteem geproduceerde informatie.

seerde informatieverstrekking een betrouwbare afspiegeling is van de werkelijkheid.
De systeembeoordeling is gericht op de opzet en het bestaan van alle op basis van de risicoanalyse noodzakelijk geachte controle- en beveiligingsfunctionaliteiten. De werking behoeft in deze fase van de controle niet te worden vastgesteld. Het vaststellen van de werking is een onderdeel van de hiervoor beschreven informatiecontrole. Een niet-adequate werking zal door de gebruikers worden gesignaleerd in de vorm van ontbrekende controle-informatie en/of geconstateerde fouten. Het als zelfstandig onderdeel vaststellen van de werking is, uit hoofde van de jaarrekeningcontrole, niet zinvol. De jaarrekeningcontrole richt zich op de getrouwheid van informatie en niet op de betrouwbaarheid van systemen.

Er kan nog een andere redenering worden gevolgd waaruit blijkt dat de oordeelsvorming over de werking van de controlemaatregelen in een informatiesysteem een station te ver is. Het vaststellen van de werking van informatiesystemen vindt door de gebruikers plaats op basis van de analyses van de uitkomsten. Als vastgesteld is dat de informatie voldoende betrouwbaar is, is het voor de jaarrekeningcontrole niet nodig om terug te gaan naar het systeem. De systeembeoordeling hoeft niet verder te gaan dan de beoordeling van de toereikendheid van de controles om de betrouwbaarheid van de informatie te kunnen beoordelen. De context van deze beoordeling wordt bepaald door een risicoanalyse uit het oogpunt van de accountantscontrole.

De diepgang van de beoordeling van de general ICT controls toont een belangrijk gat tussen de theorie en de praktijk.

Indien tot de conclusie wordt gekomen dat de interne-controlefunctionaliteit onvoldoende is, zal samen met de gebruiker gezocht moeten worden naar een oplossing. Compensatie door extra gebruikerscontroles zal lang niet altijd mogelijk zijn, omdat de benodigde controle-informatie ontbreekt. Aanpassen van het systeem, het ontwikkelen van queries of het gebruik van audit-software is de enige oplossing die dan nog resteert.

Naast inzicht in de geprogrammeerde controles moet er zekerheid zijn dat het systeem niet ongeautoriseerd kan veranderen en dat de gegevens alleen binnen de aangegeven autorisatie worden vrijgegeven voor inzage of bewerking. Indien dit niet bewust wordt beheerst, kunnen de conclusies uit de informatiecontroles niet worden gebruikt als graadmeter voor de algehele betrouwbare werking.

Technische organisatie

De general ICT controls zijn de basis voor een betrouwbare geautomatiseerde gegevensverwerking. Deze controles zijn er onder meer op gericht te waarborgen dat de functionaliteit van de programmatuur geen ongeautoriseerde wijziging ondergaat en dat de gegevens slechts op een geautoriseerde wijze kunnen worden gemuteerd. Naast de betrouwbaarheid zijn de controles ook bedoeld om de toereikendheid van de continuïteitsmaatregelen te waarborgen. Het betreft maatregelen om te voorkomen dat gegevens verloren gaan en dat herstel van de gegevensverwerking langer duurt dan vanuit het bedrijfsproces toelaatbaar wordt geacht.

Het uitgangspunt is dat gegevensverwerkende processen betrouwbaar moeten verlopen. Een professionele organisatie streeft ernaar foutloos te werken. De gevolgen van fouten en het herstellen van fouten brengen extra kosten met zich mee. Ondersteuning bij de realisatie van betrouwbare processen kan door een gespecialiseerde accountant of IT-auditor worden verleend. Dit zijn advieswerkzaamheden die geen onderdeel uitmaken van de reguliere accountantscontrole.

In het algemeen legt de diepgang van de beoordeling van de general ICT controls een belangrijk gat tussen de theorie en de praktijk bloot. In de theorie wordt gewoonlijk gesteld dat de werking moet worden beoordeeld. In de praktijk wordt in het kader van de accountantscontrole zeer pragmatisch met het beoordelen van automatiseringsorganisaties omgegaan en blijft de beoordeling veelal beperkt tot opzet en bestaan. Ligt het knelpunt in de praktijk (wordt het niet goed gedaan) of moet de theorievorming nader worden gedifferentieerd? In de volgende alinea's worden enkele aspecten rond deze vragen toegelicht.

Bij de controle van de verwerking van de routinematige transacties is het werkprogramma van de accountant, bij een systeemgerichte controle, toegesneden op het vaststellen van een betrouwbare gegevensverwerking. Doorredenerend zou dit betekenen dat de accountant opzet, bestaan *en werking* van de automatiseringsorganisatie zou moeten beoordelen. De automatiseringsorganisatie is één van de componenten uit het totale systeem dat bepalend is voor de betrouwbaarheid van de vastlegging en verwerking van de routinematige transacties. Het vaststellen van de voortdurend betrouwbare werking van een automatiseringsorganisatie vereist een 'zware' audit. Indien deze audit geïsoleerd wordt uitgevoerd, is het vertalen van de bevindingen naar de betekenis voor de betrouwbaarheid van de door de geautomatiseerde systemen opgeleverde informatie niet eenvoudig. In de praktijk doen zich regelmatig afwijkingen voor in de werkprocedures en vinden beveiligingsincidenten (veelal vergissingen) plaats. Het tolerantiebegrip kan hierop echter niet worden toegepast. De tolerantie geldt voor de informatie en kan niet worden doorvertaald naar het systeem. Dit komt doordat een kleine afwijking van de werkwijze of een minieme afwijking in de beveiliging vergaande gevolgen kan hebben voor de betrouwbaarheid van de uitkomsten van de gegevensverwerking en de opgeslagen gegevens. Het kan echter ook zo zijn dat de afwijking geen enkel gevolg heeft voor de kwaliteit van de informatieverwerking en de betrouwbaarheid van de opgeslagen gegevens. Slechts een analyse van de gevolgen van de verstoring voor de betrouwbaarheid van de informatieverstrekking kan hierin helderheid verschaffen. Deze analyse komt, voorzover het de jaarrekening betreft, overeen met de in een vorige paragraaf uit-

eengezette informatiecontrole! Deze informatiecontrole wordt door de gebruikers uitgevoerd en leidt direct tot een beeld van de betrouwbaarheid van het informatiesysteem, hetgeen in de ogen van de auteur duidelijk maakt dat in het kader van de jaarrekeningcontrole een specifiek onderzoek naar de *werking* van de automatiseringsorganisatie niet nodig is. De werking wordt indirect vastgesteld door middel van de informatiecontroles.

Voor de jaarrekeningcontrole is belangrijk dat sprake is van een beheerst verwerkingsproces. Indien het stelsel van geprogrammeerde controles en informatiecontroles adequaat is, zullen fouten hierdoor uiteindelijk aan het licht komen. Echter, fouten maken extra correctie-inspanning noodzakelijk en veel fouten vertroebelen de controle-informatie. Om fouten te voorkomen moet er zekerheid zijn over het bestaan van een verwerkingsorganisatie die onder controle is. Indien de inrichting van de verwerkingsorganisatie niet aan de minimale betrouwbaarheidseisen voldoet, dan is er onvoldoende basis om op de geprogrammeerde controles te steunen voor het signaleren van mogelijke fouten in de verwerking. Aan een beoordeling van de opzet en het bestaan van de betrouwbaarheidsmaatregelen binnen de automatiseringsorganisatie zal dus niet voorbij kunnen worden gegaan.

Change management (inclusief testen) en logische toegangsbeveiliging zijn uit oogpunt van de beheersing van de werking van informatiesystemen de belangrijkste processen. Het eerste moet voorkomen dat er verschillen ontstaan tussen de door de gebruiker, mede op grond van de aanwezige controlefunctionaliteit, geaccepteerde systemen en de in werkelijkheid operationele systemen. De logische toegangsbeveiliging moet waarborgen dat slechts geautoriseerde transacties in de gegevensbestanden/databases worden verwerkt. Uit hoofde van de jaarrekeningcontrole dienen deze twee processen ten minste te worden beoordeeld. Bij de beoordeling van de opzet en het bestaan van de automatiseringsorganisatie in het kader van de jaarrekeningcontrole moeten met betrekking tot de processen zowel de procedures, de beveiligingsmaatregelen als de internal control[4] worden betrokken. Zonder de werkprocedures en beveiligingsmaatregelen als onbelangrijk terzijde te schuiven, dient het accent van de beoordeling te liggen op de internal control. De internal control is overkoepelend en vormt het sluitstuk van de inrichting van de organisatie. De controlemaatregelen en de correctieprocedures vormen het herstellend vermogen van de organisatie.

In deze paragraaf is geconstateerd dat er een verschil is tussen de theorie en de praktijk bij de beoordeling van automatiseringsorganisaties in het kader van de jaarrekeningcontrole. De vraag in hoeverre de theorie of het dagelijks handelen bijstelling behoeft, is een knelpunt in de praktische betekenis. Op basis van het voorgaande behoeft vooral de theorievorming een bijstelling. Echter, ook de dagelijkse praktijk kan efficiënter, en wel door het onderzoek vooral te richten op het change management en de logische toegangsbeveiliging. De beoordeling van deze processen moet zich, naast de inrichting van deze procedures, vooral richten op het bestaan van internal control, gericht op de goede werking van de genoemde procedures.

Samenvatting

Op dit moment ontbreekt het aan een eenduidig standpunt over de diepgang van de noodzakelijke beoordeling van informatiesystemen en automatiseringsorganisaties in het kader van de accountantscontrole. De praktijk gaat hiermee anders om dan de theorie. De praktijk neemt in zijn redenering de uitkomsten van de gegevensverwerking als uitgangspunt, de theorie werkt daarentegen over het algemeen meer vanuit de gebruikte ICT. De conclusie is dat in het kader van de jaarrekeningcontrole de beoordeling van de gebruikte IT niet gericht hoeft te zijn op de werking. De betrouwbaarheid van de uitkomsten van de gegevensverwerking wordt vastgesteld op basis van de informatiecontroles gebaseerd op een fundament van geprogrammeerde controles en internal control binnen de automatiseringsorganisatie. De geprogrammeerde controles en general ICT controls zijn de voorwaarde om informatiecontroles te kunnen uitvoeren. Het vaststellen in hoeverre aan deze voorwaarde wordt voldaan, kan beperkt blijven tot de opzet en het bestaan; de werking wordt gelijktijdig met het vaststellen van de betrouwbaarheid van de uitkomsten (de informatiecontrole) vastgesteld. Impliciet is met het vaststellen van de betrouwbaarheid van de uitkomsten ook vastgesteld dat de werking van informatiesystemen en de technische infrastructuur betrouwbaar is geweest. Voor de jaarrekeningcontrole is dit minder interessant omdat de werking van deze elementen in dit kader geen afzonderlijk object van onderzoek is.
Dit artikel is bedoeld als bijdrage aan de discussie waartoe het studierapport 'Normatieve maatregelen voor de geautomatiseerde gegevensverwerking' van het NIVRA de betrokkenen heeft willen aanzetten. De auteur staat open voor reacties op zijn zienswijze en zal gaarne meewerken aan verdere publicaties over dit onderwerp.

Literatuur

[Bien95]
Margaret E. van Biene-Hershey, *IT Auditing, An Object Oriented Approach*, Delwel, 1995.

[ISAC96]
ISACA, *CobiT: Control objectives for information and related Technology*, 1996.

[Koed96]
Mw. M.J.A. Koedijk RA en mw. W.A. de Munck RA, *System Review Services*, Compact 1996/3.

[Limp97]
Limperg Instituut, *Interne controle en Informatiecontrole*, Kluwer Bedrijfsinformatie, 1997.

[NIVR95]
Koninklijk NIVRA, studierapport *Normatieve maatregelen voor de geautomatiseerde gegevensverwerking*, 1995.

4) Voor de Engelse term is gekozen om een duidelijk onderscheid te maken met het engere begrip interne controle. Met internal control wordt naast controle ook aangeduid het bijsturen en het correctief aanpassen van de organisatie en procedures.