Beoordeling van de interne controle in het kader van de accountantscontrole

Fred de Koning

SAMENVATTING Het Audit Risk Model heeft de laatste jaren vanuit verschillende invalshoeken ter discussie gestaan. Door de voorzitter van de SEC is eraan getwijfeld of het wel tot een voldoende effectieve vorm van accountantscontrole leidt. Anderen hebben voorgesteld het inherente risico (al dan niet tezamen met het interne-controlerisico) te vervangen door het bedrijfsrisico. Blokdijk heeft twijfels geuit of het model, en met name de toetsing van de werking van de interne controle, wel uitvoerbaar is.
In dit artikel wordt de kritiek op het Audit Risk Model geanalyseerd. De conclusie daaruit is, dat in het kader van de accountantscontrole meer aandacht aan de beoordeling van opzet en werking van de interne controle moet worden besteed, waarbij het toetsen van de werking van de interne controle, ook in geautomatiseerde omgevingen, zeer wel mogelijk is.

1 Inleiding

De Richtlijnen voor de Accountantscontrole beschrijven in Richtlijn 400 (Koninklijk NIVRA, 2000, p. 329) het Audit Risk Model, de op risicoanalyse gebaseerde benadering van de accountantscontrole. Doelstelling van het model is het beperken van het audit risk of accountantscontrolerisico, dat wil zeggen het risico dat een accountant een onjuiste accountantsverklaring afgeeft. Het accountantscontrolerisico is de resultante van het inherente risico, interne-controlerisico en het ontdekkingsrisico, of in formulevorm:

Prof. Dr. W.F. de Koning is vennoot van Mazars Paardekooper Hoffman en aldaar hoofd van de sectie Information Systems Auditing (ISA). Daarnaast is hij als hoogleraar Bestuurlijke Informatieverzorging, in het bijzonder Informatiecontrole, verbonden aan de Stichting NIVRA-Nyenrode.

$$A_R = f\,(I_R, IC_R, D_R)^1$$

Het inherente risico wordt in de Richtlijnen voor de Accountantscontrole (p. 331) omschreven als de gevoeligheid van een jaarrekeningpost voor een onjuistheid, die – afzonderlijk of tezamen met onjuistheden in andere jaarrekeningposten – van materieel belang kan zijn, onder de veronderstelling dat er nog geen interne controle heeft plaatsgevonden.
Het interne-controlerisico is het risico dat een dergelijke onjuistheid niet wordt voorkomen of hersteld door de genomen maatregelen van administratieve organisatie en interne controle.
Afhankelijk van de inschatting van het inherente risico en het interne-controlerisico dient de accountant te bepalen welke gegevensgerichte werkzaamheden hij moet verrichten om het accountantscontrolerisico tot een aanvaardbaar niveau te reduceren. Deze gegevensgerichte werkzaamheden bepalen het ontdekkingsrisico ('Detection Risk'), dat wil zeggen de kans dat de accountant een onjuistheid van materieel belang in een jaarrekeningpost niet zal ontdekken.

Het belang van het Audit Risk Model ligt vooral in het steunen op de interne controle. Door gebruik te maken van hetgeen intern al wordt gedaan aan beheersing van bedrijfsprocessen, kan de accountantscontrole doelgerichter en efficiënter worden uitgevoerd. Voorwaarde is echter wel dat de goede werking van de interne controle kan worden vastgesteld. Blokdijk (2001, p. 78) komt tot de conclusie dat dit in een geautomatiseerde omgeving niet of nauwelijks mogelijk is, anders dan door gegevensgerichte werkzaamheden. Hij stelt daarom voor de toetsing van de goede werking van de interne controle ('tests of control') als element van de risicoanalyse af te schaffen, waarmee het hele Audit Risk Model feitelijk op de helling komt te staan.

In dit artikel zal worden nagegaan in hoeverre de kritiek, die de laatste jaren op het Audit Risk Model is geuit, terecht is. In paragraaf 2 wordt aandacht besteed aan de door Levitt (1999) opgeworpen vraag of het Audit Risk Model leidt tot een voldoende effectieve accountantscontrole, waarbij het belangwekkende, door het Panel on Audit Effectiveness uitgevoerde onderzoek aan de orde komt. In paragraaf 3 wordt ingegaan op de ontwikkelingen van de laatste tijd richting bedrijfsrisico's of business risks, die suggereren, dat het Audit Risk Model te beperkt of inefficiënt is. In paragraaf 4 worden de te beoordelen interne-controlemaatregelen in kaart gebracht, waarna in paragraaf 5 wordt ingegaan op het door Blokdijk gesignaleerde probleem ten aanzien van de toetsing van de werking van deze maatregelen.

2 De effectiviteit van het Audit Risk Model

In 1999 twijfelde de toenmalige voorzitter van de Security and Exchange Commission (SEC) er in een toespraak aan of het Audit Risk Model wel tot een voldoende effectieve accountantscontrole leidde: 'In an era that calls for greater risk management, the industry has migrated to what they call the 'risk-based' model. It sounds right on target. Because of the challenges of executing these new standards well, I wonder if the public interest is better served. We cannot permit thorough audits to be sacrificed for re-engineered approaches that are marginally more efficient, but significantly less effective.' (Levitt, 1999).

Deze vraag is nader onderzocht door het Panel on Audit Effectiveness van de Public Oversight Board (een onafhankelijke instelling, die wordt gefinancierd door accountantskantoren). Daartoe is onder meer een review uitgevoerd op de door de acht grootste accountantskantoren in de Verenigde Staten bij 126 beursgenoteerde ondernemingen uitgevoerde audits. Deze reviews hebben tot een positieve conclusie geleid over de wijze waarop de audits zijn uitgevoerd: 'Overall, the findings from the QPRs[2] were favorable and did not support the view that audits are being conducted in an ineffective manner.' (Panel, 2000, p. 13).
Het Panel on Audit Effectiveness is echter wèl van mening dat het Audit Risk Model moet worden uitgebreid en beter moet worden geïmplementeerd. De uitbreidingen hebben onder meer betrekking op het beoordelen van de risico's van acceptatie en continuering van opdrachten. Het Panel beveelt aan geautomatiseerde systemen te gebruiken voor het bepalen van het 'engagement risk' (p. 17).
De kritiek ten aanzien van de implementatie heeft voor een belangrijk deel betrekking op de wijze waarop het interne-controlerisico wordt bepaald. Bij het veldonderzoek is vastgesteld dat in bijna 17% van de gevallen een serieuzere en meer inhoudelijke analyse van de 'control environment' van de onderneming had mogen worden verwacht. In circa 21% van de gevallen had de beoordeling kunnen worden verbeterd door een effectievere inzet van ICT-deskundigen (p. 25).

Het toetsen van de interne-controlemaatregelen liet in 12% van de gevallen te wensen over. Deze toetsing werd over het algemeen als tijdrovend beschouwd en sommige accountants waren van mening dat deze toetsing minder effectief was dan gegevensgerichte detailcontroles (p. 26).
Het Panel beveelt de accountantskantoren aan hoge prioriteit toe te kennen aan het verbeteren van de effectiviteit van hun werkzaamheden op het gebied van interne controle, met name wat betreft hun kennis van de informatiesystemen van hun cliënten. Het gaat daarbij om de volgende zaken (p. 29):

1 het verkrijgen van een meer diepgaande kennis van de informatiesystemen, die relevant zijn voor de financiële verantwoording en de daaraan verbonden risico's en maatregelen;
2 het identificeren en evalueren van de opzet van kritische interne controles;
3 het leggen van de relatie tussen genomen maatregelen aan de ene kant en de geïdentificeerde risico's en gegevensgerichte controles aan de andere kant;
4 het opzetten van tests op de goede werking van de interne-controlemaatregelen;
5 het beoordelen van de resultaten van deze tests;
6 het inschatten van de gevolgen voor de effectiviteit van de controle van beslissingen over de wijze waarop de tests op de interne controle zijn uitgevoerd.

Ook de kennis van automatisering bij auditors en de inschakeling van EDP-auditors moeten volgens het Panel worden verbeterd: 'The Panel sees an increasing need for auditors to have a higher level of technology skills and for more effective participation in audits by information technology specialists.' (p. 29).

De bevindingen van het Panel on Audit Effectiveness betekenen een belangrijke ondersteuning voor het Audit Risk Model en een aansporing voor accountants om er nog serieuzer mee om te gaan.

3 Van inherent risico naar bedrijfsrisico?

Van Leeuwen en Wallage (2002) stellen vast dat de traditionele risicobenadering is gericht op een analyse

van de transactiestromen en jaarrekeningposten, teneinde te beoordelen of de jaarrekening een getrouw beeld geeft. Volgens hen is het effectiever de werkelijke processen, activiteiten alsmede de relaties en interactie met de omgeving als uitgangspunt voor de risicoanalyse te nemen. Op grond daarvan bepleiten zij het inherente risico in het Audit Risk Model te vervangen door het (ruimere) business risk, door hen bedrijfsrisico genoemd.
Onder het bedrijfsrisico moeten, volgens hen, ook de risico's op het gebied van effectiviteit en efficiency van processen en de risico's ten aanzien van de naleving van wet- en regelgeving worden begrepen. Kennis van het ruimere bedrijfsrisico draagt er naar hun mening toe bij, dat een effectieve inschatting van het inherente risico plaatsvindt. Daarbij verwijzen zij naar de Enron-casus. Deze casus zou duidelijk maken dat een benadering vanuit de bedrijfsrisico's noodzakelijk is. Dat is naar mijn mening een te snel getrokken conclusie. Er is reden te veronderstellen, dat de accountants van Enron, evenals die van andere grote accountantskantoren, al volgens de methodiek van de business risks controleerden[3].

Vervanging van het inherent risico door het bedrijfsrisico heeft volgens Van Leeuwen en Wallage ook gevolgen voor het interne-controlerisico. Zij pleiten ervoor het interne-controlerisico te vervangen door het 'interne beheersingsrisico'[4], dat bestaat uit het strategisch beheersingsrisico en het procesbeheersingsrisico. Een inschatting van het strategisch beheersingsrisico kan een rol spelen bij de beoordeling van de overlevingskansen van ondernemingen. Met andere woorden: uitbreiding van het Audit Risk Model in de door Van Leeuwen en Wallage beschreven zin kan het risico verlagen, dat de accountant een goedkeurende verklaring afgeeft bij een op 'going concern' gebaseerde jaarrekening van een met de ondergang bedreigde onderneming. Indien zou blijken dat daar een belangrijke oorzaak van de huidige kritiek op het functioneren van accountants ligt, is uitbreiding van het Audit Risk Model (en daarmee van de door de accountant uit te voeren werkzaamheden) een zinnige zaak. Naar mijn mening kan een dergelijke stelling echter nog onvoldoende worden onderbouwd. Bovendien bestaat het gevaar, dat door alle aandacht voor de strategische risico's de aandacht voor procesbeheersingsrisico's vermindert.

Lemon c.s. hebben onderzoek gedaan naar de in gebruik zijnde auditmethodieken bij de grotere accountantskantoren in Engeland, Canada en de Verenigde Staten (2000). Zij komen daarbij tot de conclusie dat in veel gevallen methoden worden gevolgd, die uitgaan van business risks, door hen gedefinieerd als 'the risk that the audited entity will fail to achieve its objectives' (p. 1).
De beoordeling van het inherente risico en het interne-controlerisico wordt in deze benadering grotendeels vervangen door een beoordeling van business risks. Door de ondervraagde kantoren worden daarvoor de volgende argumenten aangevoerd (pp. 12-13):

- onjuiste accountantsoordelen zijn niet zozeer het gevolg van het niet kunnen ontdekken van fouten in de jaarrekening, als wel van problemen op het terrein van de bedrijfsvoering, zoals doorbreking van de continuïteit of fraudes;
- het Audit Risk Model leidt tot 'overauditing' en is derhalve inefficiënt;
- door toenemende automatisering zijn de te controleren vastleggingen betrouwbaarder;
- de benadering vanuit de business risks leidt tot meer toegevoegde waarde voor de cliënt;
- de beoordeling van corporate governance vraagt om een breder begrip van de business risks;
- het 'engagement risk' krijgt meer aandacht.

Lemon c.s. signaleren dat de benadering vanuit de business risks ertoe kan leiden, dat er minder aandacht wordt besteed aan het testen van interne-controlemaatregelen op procesniveau. Dat zou kunnen worden gerechtvaardigd door meer aandacht voor zogenaamde management controls (p. 18). Zij vrezen echter, dat toezichthoudende instanties moeite zullen hebben om de methode van de business risks te accepteren, met als argument dat deze methode minder effectief is dan de conventionele risicobenadering (p. 23). Deze angst is zeker niet ongegrond gezien de aanbevelingen van het Panel on Audit Effectiveness om meer aandacht te besteden aan de evaluatie van de interne-controlemaatregelen.

Concluderend kan worden gesteld, dat uitbreiding van het Audit Risk Model met een beoordeling van het 'engagement risk' en strategische risico's zinvol kan zijn, indien zou blijken dat daar een belangrijke oorzaak zou liggen van de huidige kritiek op het functioneren van accountants. Vervanging van of minder aandacht voor het interne-controlerisico is echter strijdig met de bevindingen van het Panel on Audit Effectiveness.

4 Te beoordelen interne-controlemaatregelen

De Richtlijnen voor de Accountantscontrole (2000) geven in Richtlijn 400 (p. 331) aan, dat de accountant

voldoende inzicht in de administratieve organisatie en interne controle (AO/IC) dient te verkrijgen. Administratieve organisatie wordt daar gedefinieerd conform Starreveld: 'Het geheel van maatregelen met betrekking tot het systematisch verzamelen, ordenen, vastleggen en verwerken van gegevens gericht op het verstrekken van informatie ten behoeve van het besturen en het doen functioneren van een huishouding, alsmede ten behoeve van de verantwoording die daarover moet worden afgelegd.' Dit is een lastige, ingewikkelde definitie, die Starreveld in eerste instantie voor het begrip 'administreren' gebruikte. Anders dan in de tijd waarin de definitie van Starreveld is ontstaan[5], heeft administratieve organisatie nu alles te maken met geautomatiseerde informatiesystemen. Het object van onderzoek is verplaatst van 'boeken en bescheiden' naar 'informatiesystemen, die gericht zijn op het verstrekken van administratieve, logistieke en bestuurlijke informatie' (De Koning, 2000a, p. 11).

Merkwaardigerwijs is er naast Richtlijn 400 (RAC400) ook nog een Richtlijn 401 (RAC401), getiteld 'Controle in een omgeving waarin gebruik wordt gemaakt van geautomatiseerde informatiesystemen'. Deze richtlijn geeft aanwijzingen in geval een controle wordt uitgevoerd in een omgeving waarin 'een computer van welke grootte dan ook, door de huishouding wordt gebruikt voor de verwerking van financiële gegevens welke voor de controle van belang zijn…' (p. 363). Zouden er nog omgevingen zijn waar dit niet het geval is? Ik vermoed van niet. Wij mogen dus aannemen, dat RAC401 nagenoeg altijd van toepassing is, hetgeen ervoor pleit RAC400 en RAC401 samen te voegen.

Onder 'interne-controlemaatregelen' verstaat RAC400 de uitgangspunten en de procedures, die de leiding van de huishouding – in aanvulling op de controleomgeving – heeft opgezet om de specifieke doelstellingen van de huishouding te bereiken. De volgende specifieke interne-controlemaatregelen worden genoemd (pp. 333-335):

- Het maken, beoordelen en goedkeuren van aansluitingen.
- Het nagaan van de rekenkundige juistheid van de (grootboek)rekeningen.
- Het beheersen van de toepassingen en algemene opzet van de geautomatiseerde gegevensverwerking, door bijvoorbeeld het opzetten van interne-controlemaatregelen met betrekking tot:
  - wijzigingen in computerprogramma's;
  - toegang tot gegevensbestanden.
- Het gebruikmaken en periodiek beoordelen van controlerende tussenrekeningen en van tussentijdse proef- en saldibalansen.
- Het goedkeuren en controleren van documenten.
- Het vergelijken van interne gegevens met externe informatiebronnen.
- Het aansluiten van kasopnames, inventarisaties van waardepapieren en voorraden met de grootboekrekeningen.
- Het beperken van de fysieke toegang tot eigendommen en administratie.
- Het vergelijken en analyseren van de financiële resultaten met budgetten.

RAC401 gaat niet expliciet in op interne-controlemaatregelen. Met alle respect voor de opstellers van de RAC moet mij van het hart, dat in RAC400 een toch wel erg beperkte visie wordt gegeven op de interne-controlemaatregelen in een moderne omgeving. Het zijn – met uitzondering van het derde gedachtebolletje – voornamelijk attentiepunten om na te gaan of de boekhouder of controller zijn werk wel goed gedaan heeft. Bovendien roept een en ander nogal wat vragen op:

- Maakt de boekhouder zelf aansluitingen of doet het financiële informatiesysteem dat?
- Gaan wij nog steeds de 'rekenkundige juistheid van (grootboek)rekeningen' na of gaan wij na of het financiële informatiesysteem op dat punt goed functioneert?
- Betreft het 'goedkeuren en controleren van documenten' externe documenten, uit de computer afkomstige documenten of records in computerbestanden?
- Hoeven wij ten aanzien van de informatiesystemen alleen maar te letten op 'toegangsbeveiliging tot gegevensbestanden' en de procedures ten aanzien van 'wijzigingen in computerprogramma's' ook wel genoemd 'change management'?
- Waarom staat er niet dat de accountant moet nagaan welke controles in de toepassingsprogrammatuur zijn opgenomen, de zogenaamde 'application controls'?
- Hoeven wij niet naar andere 'general controls' te kijken, zoals systeemontwikkelingsprocedures, implementatieprocedures, test- en acceptatieprocedures, beheersprocedures, fysieke beveiliging en dergelijke?

Knechel (2001) spreekt in dit verband over 'process level controls', die zijn gericht op de betrouwbaarheid van verantwoordingsinformatie en bescherming van activa tegen verduistering. De volgende categorieën interne-controlemaatregelen worden door Knechel (p. 216) genoemd:

- Performance reviews;
- Processing controls, nader te onderscheiden in:

- General controls;
- Application controls;
- Physical controls;
- Segregation of duties.

De *performance reviews* omvatten het vergelijken van de gemeten prestaties met standaarden, waaronder resultaten van voorgaande periodes, begrotingen en budgetten, externe vergelijkingscijfers, en dergelijke.
De term *general controls* werd oorspronkelijk alleen gebruikt in de context van geautomatiseerde systemen. In principe worden hiermee de beheersingsmaatregelen rondom geautomatiseerde systemen bedoeld, die gelden voor alle applicaties. Volgens Knechel is deze term ook in ruimere zin toepasbaar en heeft dan betrekking op de wijze waarop processen worden ontworpen en beheerst.
Ook de term *application controls* stamt uit de automatisering. Daar zijn de application controls de beheersingsmaatregelen in en rond toepassingsprogrammatuur (applicaties). Knechel omschrijft de application controls als beheersingsmaatregelen, die betrekking hebben op de manier waarop afzonderlijke taken worden uitgevoerd en transacties worden behandeld in een proces.
Physical controls beperken de toegang tot activa, die gevoelig zijn voor ontvreemding, en tot gegevens, die gevoelig zijn voor vervalsing.
Segregation of duties betreft het scheiden van ongewenste combinaties van functies, zoals:

- bewaring en administratie;
- beschikken en bewaren;
- uitvoering van transacties en administratie;
- administratie en gegevensverwerking.

Dit kan worden gezien als een moderne variant op de indertijd door Starreveld (1970, p. 136) beschreven scheiding tussen de functies: beschikken, uitvoeren, bewaren, registreren en uitvoeren.

Ook de opsomming van Knechel blijft echter erg beperkt. Elders in de literatuur kunnen wel opsommingen worden gevonden van alle mogelijke en onmogelijke interne-controlemaatregelen in geautomatiseerde omgevingen. Zie bijvoorbeeld: Code voor Informatiebeveiliging (NNI, 2000), CobiT (IT-Governance Institute, 2000), ITIL Security Management (1999) en Overbeek (2000). Een groot deel van de daar genoemde maatregelen is ook relevant in het kader van de accountantscontrole. Studierapport 34 van het NIVRA (Koninklijk NIVRA, 1995) vermeldt de specifiek voor de accountantscontrole relevante maatregelen, maar is helaas al weer enigszins gedateerd.

5 Het toetsen van de werking van de interne controle

Blokdijk (2001) is van mening dat de theorie, die aan ISA400[6] ten grondslag ligt, geen sluitend geheel van controlemaatregelen oplevert en daarmee geen deugdelijke grondslag voor de accountantsverklaring (p. 79). De kritiek van Blokdijk komt er in wezen op neer, dat het beoordelen van de werking van de interne controle alleen op indirecte wijze mogelijk is, dat wil zeggen door de resultaten van de interne controle, de cijfers dus, aan een onderzoek te onderwerpen. In een in *De Accountant* van januari 2001 (Rothuizen, 2001, p. 238) weergegeven discussie pleit Blokdijk ervoor het toetsen van de internal control uit het risicoanalysemodel weg te laten, omdat het beoordelen van de werking van de interne controle ófwel niet mogelijk zou zijn ófwel met dezelfde controlemiddelen wordt uitgevoerd als de controle op het cijfermateriaal.

Door andere auteurs wordt erop gewezen, dat het toetsen van de werking van de interne controle niet eenvoudig is. Zo stelt Hartjes (2001, p. C.6.1-06): 'De echte problemen ontstonden als het erom ging de werking van geautomatiseerde beheersingsmaatregelen vast te stellen. Dit is geen vraagstuk, dat specifiek is voor automatisering: ook in handmatige processen is het altijd een uitdaging voldoende basis te vinden voor de uitspraak, dat de processen hebben gewerkt.'
In de praktijk blijkt dan ook, dat EDP-auditors hun oordelen te vaak op een beoordeling van de opzet en het bestaan baseren en te weinig aandacht besteden aan de goede werking van de genomen maatregelen (De Koning 2000b, p. 25). Een vergelijkbare constatering komen wij tegen bij Boer (1999).

Het feit dat het beoordelen van de werking van de AO/IC lastig is, betekent echter niet dat daar zonder meer aan kan worden voorbij gegaan. Zo wijst ook Fijneman (1999, p. 50) erop, dat bij een systeemgerichte controlebenadering de goede werking van geprogrammeerde controles moet worden nagegaan.

Blokdijk is nagegaan, welke controlemiddelen door RAC400 worden aangereikt voor de beoordeling van de AO/IC. Dat zijn:

- Onderzoek van documenten, die ten grondslag liggen aan bepaalde transacties of andere gebeurtenissen.
- Informeren naar en het waarnemen van de uitvoering van maatregelen van interne controle.
- Opnieuw uitvoeren van maatregelen van interne controle.

Het *onderzoek van documenten* wordt door Blokdijk slechts als een zinvolle controle aangemerkt, indien de accountant een post uit de verantwoording controleert met een document, waarbij hij tevens nagaat of het document wel voldoende bewijskracht heeft. Blokdijk gaat er kennelijk vanuit, dat onder 'documenten' alleen boekingstukken moeten worden verstaan. Echter, als het erom gaat de goede werking van de interne controle vast te stellen, zou ook naar andere documenten kunnen worden gekeken, zoals documenten, die worden gebruikt in het kader van change management (de 'interne controle op de wijzigingen in de programmatuur'). Daarbij kan bijvoorbeeld worden gedacht aan een wijzigingsverzoek (request for change) van een gebruiker. Nagegaan kan worden waar het document is ontvangen, hoe het is geregistreerd, wie zich over het verzoek heeft gebogen, welke conclusies daaruit zijn getrokken, wie het document heeft goedgekeurd of afgekeurd, welke vervolgactie er is ondernomen, et cetera.

Blokdijk besteedt zelf ook aandacht aan het change management. De accountant kan volgens hem nagaan welke wijzigingen na testen zijn geautoriseerd. Dat heeft volgens hem ook zin om zijn kennis van het systeem van de gegevensbewerking te actualiseren. Maar volgens Blokdijk blijft de knagende vraag of er ook ongeautoriseerde wijzigingen zijn opgetreden. Ten aanzien daarvan kan de accountant nagaan 'welke maatregelen periodiek intern worden getroffen'. Of en in hoeverre accountants hiervoor tegenwoordig zelf over mogelijkheden beschikken, is hem niet bekend. Hij wil zich daar ook niet in verdiepen, aangezien deze 'systeemgerichte arbeid' slechts het bestaan van het systeem betreft en niet de werking daarvan. Ik meen hieruit te mogen opmaken, dat Blokdijk zoekt naar mogelijkheden om te kunnen vaststellen dat de maatregelen die getroffen zijn om de productie-library (het bestand, waarin de productieprogrammatuur is opgeslagen) af te schermen, goed functioneren. Dat is tegenwoordig zeer wel mogelijk. Bij gebruik van daartoe bestemde programmatuur (library control programmatuur) worden alle wijzigingen op de productie-library gelogd. Deze wijzigingen kunnen periodiek door een intern controleur of een andere onafhankelijke functionaris worden beoordeeld. De accountant zou achteraf kunnen vaststellen (aan de hand van de loggegevens) of deze controle goed heeft gefunctioneerd. Dat valt onder de categorie 'opnieuw uitvoeren'.
Het ontgaat mij waarom Blokdijk het hier heeft over controles op het bestaan en niet op de werking van de interne controle. Wellicht is de definitie van opzet, bestaan en werking het discussiepunt. Als Blokdijk een andere inhoud geeft aan het begrip 'werking van de interne controle', in die zin dat alleen over een goed functionerende interne controle gesproken mag worden als de cijfers juist en volledig zijn, dan is duidelijk waarom er verschillen van mening zijn. Het gaat er dan niet om de goede werking van de interne controle vast te stellen, maar om vast te stellen, dat het geheel aan interne-controlemaatregelen permanent tot goede resultaten heeft geleid. Dat kan niet de bedoeling zijn van de beoordeling van de AO/IC.

Ook ten aanzien van de logische toegangsbeveiliging onderkent Blokdijk, dat controles op de werking van de interne controle mogelijk zijn. Hij schrijft daarover: '…de accountant (zou) de in de computer vastgelegde bevoegdheden kunnen laten afdrukken.' Daarmee wordt volgens hem echter nog geen zekerheid verkregen over tussentijdse wijzigingen. Deze zekerheid zou te bereiken zijn 'indien voor deze tussentijdse wijzigingen intern dezelfde procedure wordt gevolgd als voor wijzigingen in de programmatuur, zodat de accountant kennis kan nemen van de schriftelijke autorisaties van wijzigingen in de toegangsbevoegdheden' (p. 74). De combinatie van deze twee controlemaatregelen zou volgens Blokdijk de accountant een belangrijk mate van zekerheid leveren. Dat is een juiste constatering. Daar kan nog aan worden toegevoegd, dat het in de praktijk ook mogelijk blijkt het autorisatiesysteem zo op te zetten, dat de historie wordt vastgehouden.

Het lijkt er dus op, dat Blokdijk zelf een controle op de goede werking van de interne controle heeft ontdekt. Hij komt echter tot de volgende conclusie: 'Vaak ontbreekt die interne controle echter, met name bij kleinere ondernemingen waar een systeembeheerder veelal op informele basis bevoegdheden toekent, zonder behoorlijke vastlegging.' Dat roept bij mij de vraag op waar de 'natuurlijke adviesfunctie' van de accountant blijft. In geval van het niet goed functioneren van een van de essentiële maatregelen van interne controle in een geautomatiseerde omgeving mag van de accountant worden verwacht, dat hij er bij de leiding van de onderneming op aandringt dat maatregelen ter verbetering worden genomen. De conclusie moet wellicht zijn, dat het toetsen van de werking van de interne controle niet is weggelegd voor passieve accountants!

Er zijn in een geautomatiseerde omgeving nog veel meer documenten, die gecontroleerd kunnen worden. Voorbeelden daarvan zijn: aanvragen voor het

toekennen van autorisaties op het systeem, verslagen van projectvergaderingen, verslagen van uitgevoerde tests en inspecties, formele acceptaties van opgeleverde systemen, service level agreements (SLA's) met dienstverleners, zoals rekencentra, et cetera. Al deze documenten kunnen de accountant informatie geven over de goede werking van de interne controle. Daarbij zie ik nog af van verslagen van uitgevoerde controles vanuit een verbijzonderde interne-controlefunctie.

Het *informeren naar en het waarnemen* van de uitvoering van maatregelen van interne controle levert volgens Blokdijk nauwelijks bewijskracht op voor de werking van de interne controle gedurende de gehele periode. Daarbij moet evenwel worden bedacht, dat ook bij gegevensgerichte controles doorgaans niet alles wordt gecontroleerd, maar steekproeven worden genomen. Het op onaangekondigde tijdstippen waarnemen van de wijze waarop de interne controle wordt uitgevoerd, kan wel degelijk tot een goed beeld van de werking van de interne controle leiden. Denk bijvoorbeeld aan maatregelen van fysieke beveiliging, backupprocedures, uitwijktests, et cetera. Het 'informeren naar' kan eveneens informatie over de werking van de interne controle opleveren, vooral als bij meerdere functionarissen naar gevolgde procedures wordt geïnformeerd. De accountant of EDP-auditor voert geen justitieel onderzoek uit, hij moet een redelijke zekerheid hebben dat de voorgeschreven procedures in de praktijk worden nageleefd. Geïnterviewden zouden onwaarheden kunnen vertellen, maar gecontroleerden kunnen ook documenten vervalsen of parafen op facturen namaken. Een volledige zekerheid krijgen wij maar zelden, het is bijzonder inefficiënt daarnaar te streven.

Het *opnieuw uitvoeren* van maatregelen van interne controle is volgens Blokdijk niet mogelijk voor onvervangbare maatregelen van interne controle, waaronder volgens hem de eerste vastlegging van gebeurtenissen valt. De accountant kan de daarbij plaatsvindende interne controle niet herhalen, omdat hem de technische of commerciële deskundigheid ontbreken, en/of omdat hij niet voortdurend aanwezig kan op plaatsen waar zich relevante gebeurtenissen afspelen.
Mijns inziens is het onderscheid tussen vervangbare maatregelen van interne controle en onvervangbare maatregelen enigszins achterhaald. Een voorbeeld van een onvervangbare maatregel van interne controle zou bijvoorbeeld een controle op de kwaliteit van ontvangen goederen kunnen zijn. Achteraf is deze controle niet na te bootsen. Wel zullen er keuringsrapporten zijn en wellicht documenten, waaruit blijkt dat goederen retour zijn gezonden. Blokdijk noemt de controle van dergelijke documenten de vaststelling of uiterlijke kentekenen van interne controle. De conclusie daaruit kan volgens hem slechts zijn dat de interne controle lijkt te hebben plaatsgevonden. Echter, indien de accountant over onvoldoende technische of commerciële deskundigheid beschikt, zal zijn oordeel nooit verder kunnen reiken. Zelfs al staat hij erbij, dan zal hij nog niet weten of de interne controle goed is uitgevoerd. Het is wellicht moeilijk te accepteren voor sommige accountants, maar zij zullen moeten leren leven met enkele onzekerheden.

In het Handboek EDP-auditing zijn door mij achttien controlemiddelen voor EDP-auditors beschreven (De Koning, 1998, C.4.2-01), die in tabel 1 zijn weergegeven. In het kader van de jaarrekeningcontrole gaat het met name om technieken, waarmee een oordeel kan worden verkregen over integriteit, exclusiviteit (functiescheidingen!) en beschikbaarheid van de gegevensverwerking. Een groot deel van de in de tabel vermelde controletechnieken kan worden gebruikt om de goede werking van internecontrolemaatregelen vast te stellen, denk bijvoorbeeld aan beoordeling van systeemoutput, gebruik van analysehulpmiddelen (specifieke softwareprogramma's ter beoordeling van instellingen en logfiles op computersystemen), beoordeling broncode (code review), testen en dergerlijke.

Elders (De Koning, 2000b) ben ik ingegaan op de controleerbaarheid van informatiebeveiliging. Informatiebeveiliging heeft duidelijke relaties met interne controle, hoewel beide begrippen niet helemaal samenvallen. Om de goede werking van in geautomatiseerde systemen opgenomen beveiligingsmaatregelen te verifiëren, zijn waarnemingen op het systeem feitelijk onmisbaar. Een van mijn conclusies was dan ook, dat er meer moet worden gelogd op computers (p. 25). Er moet worden nagegaan wat er allemaal op het systeem gebeurt. Logging wordt nogal eens kritisch bekeken, omdat het capaciteit vereist en het de performance negatief kan beïnvloeden. De oplossing daarvoor is: selectief loggen, bijvoorbeeld de wijzigingen op de productie-library of de wijzigingen in kritische bestanden of tabellen, zoals een prijzentabel. Logging vereist analysehulpmiddelen voor het maken van selecties of het vergelijken van wat er daadwerkelijk is gebeurd met daarvoor gehanteerde normen (zoals het gebruik van programma's ten opzichte van toegekende autorisaties).

Tabel 1. Matrix kwaliteitsaspecten/controletechnieken

Kwaliteitsaspect / *Controletechniek*	Doelgerichtheid	Doelmatigheid	Integriteit	Exclusiviteit	Beschikbaarheid	Controleerbaarheid
1. Waarneming ter plaatse				X	X	
2. Tijdstudie	X	X				
3. Lijncontroles			X			X
4. Interviews	X	X	X	X	X	X
5. Documentatie	X	X	X	X	X	X
6. Schematechnieken	X		X			
7. Bewijsstukken			X	X	X	
8. Systeemoutput	(X)	(X)	X	X	X	X
9. Analysehulpmiddelen			X	X		X
10. Code review	(X)		X		X	
11. Testen	X		X			
12. Softwarematige technieken		X			X	
13. Audit-software			X	X		X
14. Cijferbeoordeling		X				
15. Functiepuntanalyse		X				
16. Verbandscontroles			X			
17. Schriftelijke verklaring						X
18. Enquêtes	X	X	X	X	X	

6 Conclusies

Het Audit Risk Model is, blijkens de onderzoeken van het Panel on Audit Effectiveness, in principe een goede basis voor een effectieve accountantscontrole. Wellicht dienen het 'engagement risk' en het strategische beheersingsrisico aan het model te worden toegevoegd. Vervanging van het inherente risico (en het interne-controlerisico) door het bedrijfsrisico leidt ertoe, dat te weinig aandacht aan de opzet en werking van de interne controle wordt besteed en is daarmee strijdig met de conclusies van het Panel on Audit Effectiveness.

De werking van de genomen interne-controlemaatregelen is veelal toetsbaar, ook in sterk geautomatiseerde omgevingen. Voorwaarde daarvoor is wel dat bij de opzet en inrichting van de geautomatiseerde systemen rekening gehouden moet worden met het wenselijke audit-trail. Daartoe zal meer gebruik moeten worden gemaakt van automatische loggingen van acties op geautomatiseerde systemen.

Literatuur:

Blokdijk, J.H., (2001), De effectiviteit van de systeemgerichte aanpak in de accountantscontrole, in: *Maandblad voor Accountancy en Bedrijfseconomie*, maart, pp. 71-80.

Boer, J.C., (1999), ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking, in: *Jubileumuitgave 25 jaar Compact.*

Fijneman, R.G.A., (1999), *De betekenis en inhoud van 'jaarrekening ICT-auditing' als onderdeel van de jaarrekeningcontrole*, dissertatie, Tilburg.

Hartjes, S.J., (2001), EDP-audit in het kader van de jaarrekeningcontrole, in: *Handboek EDP-auditing*, Kluwer, Deventer.

IT-Governance Institute, (2000), *CobiT 3th edition.*

IT Infrastructure Library, (1999), *Security Management.*

Koning, W.F. de, (1998), Methoden en technieken voor EDP-auditing, in: *Handboek EDP-auditing*, Kluwer, Deventer (een recentere versie is opgenomen in het Handboek AIV, 2001).

Koning, W.F. de, (2000a), *Bestuurlijke Informatieverzorging, in het bijzonder informatiecontrole*, Breukelen.

Koning, W.F. de, (2000b), De controleerbaarheid van informatiebeveiliging, in: *de EDP-auditor, 3*, pp. 24-26.

Knechel, W.R., (2001), *Auditing: assurance & risk*, Cincinnati, Ohio.

Koninklijk NIVRA, (1995), *Normatieve maatregelen voor de geautomatiseerde gegevensverwerking in het kader van de jaarrekeningcontrole*, NIVRA-studierapport 34, Amsterdam.

Koninklijk NIVRA, (2000), *Richtlijnen voor de Accountantscontrole*, Editie 2000, Amsterdam.

Leeuwen, O. van en Ph. Wallage, (2002), Moderne controlebenaderingen steunen op interne beheersing, in: *Maandblad voor Accountancy en Bedrijfseconomie*, maart, pp. 82-90.

Lemon, W.M., K.W. Tatum en W.S. Turley, (2000), *Developments in the audit methodologies of large accounting firms.*

Levitt jr, A., (1999), *Remarks to the Panel on Audit effectiveness of the Public Oversight Board*, October 7 (www.sec.gov/news/speech/speecharchive/1999/spch310).

Nederlands Normalisatie Instituut (NNI), (2000), *Code voor Informatiebeveiliging*, Delft.

Overbeek, P.L., E. Roos Lindgren en M.E.M. Spruijt, (2000), *Informatiebeveiliging onder controle*, Amsterdam.

Panel on Audit Effectiveness of the Public Oversight Board, (2000), *Report and Recommendations* (www.pobauditpanel.org/download.htm).

Rothuizen, W., (2001), Kritische noten bij actuele ontwikkelingen, in: *De Accountant*, januari, pp. 238-243.

Soeting, R, W.F. de Koning, O.C. van Leeuwen, H. van Nimwegen, en E. Veldhuizen, (1997), *Interne controle en Informatiecontrole*, Amsterdam.

Starreveld, R.W., (1970), *Leer van de administratieve organisatie, deel 1: algemene grondslagen*, 4e druk, Alphen aan den Rijn.

Wilschut, K.P.G., (1990), Het denkmodel achter de risicoanalyse in de accountantscontrole, in: *De Accountant*, oktober, p. 86 e.v.

Wolde, J. ten, (1991), Bepaling controlemix bij accountantscontrole, in: *De Accountant*, oktober, p. 85 e.v.

Noten

1 Begin jaren negentig is in De Accountant uitgebreid over het model gediscussieerd door onder meer Wilschut (1990) en Ten Wolde (1991). Een van de conclusies was dat de voorheen gehanteerde notatiewijze ($A_R = I_R$ x IC_R,x D_R) mathematisch onjuist is en tot misverstanden aanleiding geeft.

2 QPR staat voor Quasi Peer Review. De onderzoeksmethode verschilde van een normale peer review. Er is met name ingegaan op de effectiviteit van het Audit Risk Model, waartoe ondermeer interviews met uitvoerenden zijn gehouden (p. 11).

3 Lemon c.s. (2000) hebben vastgesteld dat de meerderheid van de grote accountantskantoren het beoordelen van het business risk expliciet in hun methode hebben opgenomen (p. 15).

4 'Interne beheersing' is een vertaling van het Engelse 'internal control'. Het Nederlandse begrip 'interne controle' heeft altijd een beperktere strekking gehad dan 'internal control'. Om aansluiting te verkrijgen met internationale opvattingen hebben Soeting c.s., waaronder Van Leeuwen (1997), voorgesteld het begrip 'interne controle' in dezelfde zin als 'internal control' te gebruiken en voor het oudere, beperktere begrip de nieuwe aanduiding 'informatiecontrole' te hanteren.

5 De definitie is inhoudelijk nog hetzelfde als die in de uitgave van 1970 van het werk van Starreveld (p. 15).

6 ISA400 is de richtlijn van de International Federation of Accountants (IFAC), die in de Richtlijnen voor de Accountantscontrole van het Koninklijk NIVRA is bewerkt tot RAC400.