Auditrisico, meer dan ooit een issue! (2)

Kornelis Mollema

SAMENVATTING Auditrisico ondervindt stijgende belangstelling in een tijd dat auditors maatschappelijk worden bekritiseerd. In recente publicaties over corporate governance wordt van de accountant aanzienlijk meer verwacht dan een cijfermatige beoordeling en komt met name de interne controle als verantwoordingsstuk van het management, te attesteren door de auditor in beeld. Ook hebben andere bestaande auditvormen behoefte aan een adequate theorie over auditrisico. In dit artikel wordt een vernieuwd model uiteengezet dat recht wil doen aan de eisen van deze tijd en beter toepasbaar is in de auditcontext van 2003.

1 Inleiding

In deel 1 van dit artikel (Mollema, 2003) werd geconstateerd dat de bestaande auditrisicotheorie, zoals die door IFAC en verschillende auteurs wordt gehanteerd, tekortschiet en methodologische zwakheden kent. Zowel vanuit nieuwe ontwerprichtlijnen voor accountants als uit de behoefte aan goed toepasbare auditrisicotheorie voor operationele en ICT-auditing, werden vier uitdagingen geformuleerd die om een antwoord vragen:

- de kritische momenten voor foute beoordeling analyseren alsmede welke factoren wanneer van toepassing zijn;
- de verwachte omvang van de schade opnemen, in plaats van te werken met 'materiële fouten';
- de reikwijdte van de auditrisicoformule¹ uitbreiden naar operationele en ICT-audit;

Prof. Dr. Kornelis Mollema RE RA heeft een carrière doorlopen in accountancy, audit management, financial control en ICT- en backofficemanagement, het grootste deel daarvan in het internationale financiële bedrijfsleven. Thans is hij parttime hoogleraar ICT-auditing aan de postdoctorale opleiding aan de EUR.

- de resultaten van bedrijfsrisicoanalyse in de theorie opnemen.

In dit artikel zal een poging worden ondernomen om hieraan uitwerking te geven. Auditrisico wordt opnieuw gedefinieerd als Professioneel Auditrisico (PAR) (paragraaf 3). Vervolgens wordt een analyse van PAR gemaakt op drie verschillende momenten:

- het aangaan van een nieuwe klantrelatie (paragraaf 4);
- het aangaan van een nieuwe opdracht binnen een bestaande relatie (paragraaf 5);
- het afgeven van een oordeel na uitvoering van een audit (paragraaf 6).

Zoals zal blijken zijn de determinanten voor PAR op deze drie momenten verschillend en complementair.

2 Kritische momenten voor mogelijk professionele foute beoordeling

Auditors worden onvermijdelijk blootgesteld aan het risico van verkeerde beoordeling wanneer zij hun auditpraktijk uitvoeren. In theorie zijn er drie kritische momenten waarop dergelijke risico's zich kunnen manifesteren, namelijk als men:

- een nieuwe klantrelatie aangaat;
- een nieuwe opdracht aanvaardt binnen een bestaande klantrelatie;
- een oordeel vrijgeeft.

Het moment van vrijgeven van een oordeel is het meest belangrijk, omdat dit onmiddellijk relateert aan het belangrijkste product van de auditor: assurance geven! Het aangaan van een nieuwe klantrelatie kan echter eveneens een professionele bedreiging zijn voor de auditor, zelfs ver voordat er sprake is van vrijgeven van een oordeel. Bijvoorbeeld als blijkt dat de klant een corrupte organisatie runt of een verleden heeft van ernstige misleiding van zijn aandeelhouders. In dergelijke gevallen kan de associatie van de naam

van de klant met die van de auditor al veel schade berokkenen.

Als tussenliggend moment treft men de acceptatie van een nieuwe opdracht binnen een bestaande relatie aan. De meest voorkomende vorm daarvan is de repeterende audit, bijvoorbeeld van de jaarrekening, of van de auditcyclus van operationele/ICT-audit. Telkens wanneer het auditproces opnieuw start, kan de auditor worden bedreigd door (gedrags)veranderingen in de organisatie. Dit kan in versterkte mate het geval zijn wanneer de bestaande klant een geheel nieuwe opdracht voorstelt, bijvoorbeeld een fraude-onderzoek, of een due diligence in verband met de voorgenomen verkoop van een bestaand bedrijfsonderdeel. In dergelijke gevallen kan blijken dat de condities waaronder een audit zal plaatsvinden, substantieel afwijken van de condities die van toepassing waren voor audits uit het verleden.

Hoewel de drie momenten van elkaar kunnen worden onderscheiden, hebben ze veel gemeenschappelijk, in het bijzonder op het gebied van schade. Als gevolg daarvan kunnen ze niet worden behandeld als totaal losstaande stappen in het planningsproces van de audit. Waar de drie momenten het meest uiteenlopen is op het gebied van het inzicht dat de auditor heeft ten tijde van de risicoanalyse. Bij het aangaan van een nieuwe klantrelatie heeft de auditor het minste inzicht. De klant is nieuw voor hem, hij heeft geen ervaring, geen dossiers uit het verleden, et cetera, en hij verkeert niet in een positie om veel research te doen naar de potentiële klant omdat niemand hem ervoor gaat vergoeden. Op het moment van acceptatie of vernieuwing van een opdracht binnen een bestaande klantrelatie is er sprake van een gunstiger situatie. De auditor weet al veel over de klant, maar minder over de voorliggende opdracht, in het bijzonder wanneer die nieuw is. Op het moment juist voorafgaand aan de uitgifte van een audit-opinie heeft de auditor het meeste inzicht. Hij is door alle fasen van de auditplanning gegaan en is in staat geweest conclusies te trekken. Soms verandert er zoveel in de organisatie of in het (gedrag van) het management dat de auditor terug moet naar de vorige fase van risicoanalyse.

Klijnsmit, Sodekamp en Wallage (2003, p. 193) maken onderscheid tussen Accountant Bedrijfsrisico (ABR), dat relateert aan een onjuiste verklaring (ABR1), en het risico dat relateert aan geassocieerd worden met een klant die negatief in de belangstelling staat (ABR2). Laatstgenoemde wordt nog onvoldoende gezien als een onderscheiden risico op een onderscheiden moment.

3 Professioneel Auditrisico gedefinieerd

Professioneel Auditrisico (PAR) wordt gedefinieerd als de theoretische schade aan de professionele status van de auditor, veroorzaakt door waargenomen falen in zijn functionele optreden. Een enkele toelichting is op zijn plaats:

- *professioneel* verwijst naar de maatschappelijke status van de auditor, die hem toestaat te opereren als een gecertificeerd persoon en hem in staat stelt een inkomen te verdienen;
- *theoretische schade* dient in statistische zin te worden opgevat;
- *waargenomen falen* geeft aan dat zelfs de schijn van falen de schade al kan veroorzaken.

Auditrisico vereist een ex-ante waarde die funktioneert als een limiet waaraan het werkelijke auditrisico wordt afgemeten. PAR heeft dus eigenlijk twee waarden:

- een ex-ante waarde, fungerend als norm;
- een werkelijke waarde voortvloeiend uit de auditrisicoformule, die geconfronteerd wordt met de norm.

In de notatie verwijst PAR zonder toevoeging naar de werkelijke waarde. De ex-ante limiet wordt genoteerd als PAR_{ex_ante} .

Zoals doorgaans het geval is in definities van risico, zie bijvoorbeeld Mollema (1991), bestaat ook het professionele auditrisico uit de combinatie van kans (P van probability) en schade (D van damage). Of, in notatie, $PAR = P * D$. De schade kan kwantificeerbaar zijn of niet. Ingeval kwantificering moeilijk gaat, kan kwalificatie te hulp schieten. Hetzelfde geldt voor kwantificering van waarschijnlijkheden. De volgende tabel laat zien hoe men $P * D$ kan kwalificeren.

Tabel 1. Het berekenen van de theoretische schade D_{th} door het wegen van $P * D$

$D_{th} = P * D$ Schade (D)	Waarschijnlijkheid van optreden (P) →				
	kritisch	hoog	gemiddeld	laag	verwaarloosbaar
↓	5	4	3	2	1
5. Extreem	5	4	3	2	1
4. Zeer materieel	4	3.2	2.4	1.6	0.8
3. Materieel	3	2.4	1.8	1.2	0.6
2. Merkbaar	2	1.6	1.2	0.8	0.4
1. Verwaarloosbaar	1	0.8	0.6	0.4	0.2

De tabel kwalificeert P en D op een vijfpuntsschaal en vermenigvuldigt ze. In de cellen zijn de scores vermenigvuldigd en daarna gedeeld door vijf. Het resultaat is de theoretische schade (D_{th}), waarvoor dezelfde schaal van toepassing is als voor D. De tabel is toepasbaar voor auditrisico op elk van de drie genoemde momenten (aangaan van een nieuwe relatie, van een nieuwe opdracht binnen een bestaande relatie en uitgifte van een opinie) alsook voor het vaststellen van de ex-ante waarde van het auditrisico. De absolute omvang van de theoretische schade is niet de uiteindelijk beslissende factor. Als men de schade weegt, moet de materialiteit ervan, die direct verband houdt met de omvang van de business, worden meegenomen. Een voorbeeld:

Stel dat een zeker risico is ontdekt in een entiteit die niet meer dan 5% van de totale business uitmaakt in termen van (normale) winstgevendheid of balans-totaal. Daaruit vloeit voort dat een schade gemeten tegen de omvang van deze entiteit zelf materieel kan zijn, maar vertaald naar geconsolideerd niveau zijn materialiteit waarschijnlijk verliest. Toch is hier een waarschuwing op zijn plaats. Soms kunnen risico's die immaterieel lijken grotere risico's aantrekken, bijvoorbeeld door imago- en of merkschade. Dergelijke mogelijke consequenties moeten worden overwogen wanneer de materialiteit wordt vastgesteld. Het is nuttig om te zien welke verschijningsvormen van PAR te onderscheiden zijn en hoe tolerantiewaarden voor PAR_{ex_ante} kunnen worden gesteld.

De acht verschijningsvormen van PAR claimen geen exclusiviteit. Ze zijn simpelweg de meest voor de hand

liggende actie tegen de auditor of gebeurtenissen die hem overkomen als gevolg van verondersteld wangedrag of schromelijke veronachtzaming. De ex-ante (tolerantie)waarden verschillen per verschijningsvorm, zoals de laatstgenoemde verschilt in effect op de professionele status van de auditor. De auditor, zijn kantoor of zijn departement zal de tolerantiewaarden moeten bediscussiëren, mede afhankelijk van risico-attitude en verzekeringsmogelijkheden. Als de waarden eenmaal zijn vastgesteld, dan is scorecard 1 de toetssteen voor iedere nieuwe klantrelatie, opdracht of verklaring. De werkelijke waarden van PAR vloeien voort uit de risicoanalyse die de auditor moet doen en zal worden vergeleken met de toetssteen. Dit wordt apart uitgewerkt voor de drie kritische momenten van waargenomen professioneel falen en wordt in de volgende paragrafen 4 tot en met 6 bediscussieerd.

4 Professioneel Auditrisico op het moment van het aangaan van een nieuwe klantrelatie (engagementrisico of PAR_{eng})

Op het moment van aangaan van een nieuwe klantrelatie moet de auditor zijn PAR wegen, of liever zijn PAR_{eng} vanuit het opstellen van een risicoprofiel voor de toekomstige klant. Knechel (2001, p. 92) geeft een lijst met vijf factoren die de aanvaardbaarheid van een nieuwe klantrelatie raken:

- management integrity;
- reputation and image;
- accounting practices;
- financial status;
- profitability (of the account).

Uit de literatuur en uit ervaring kan men zeker twaalf factoren vinden die bijdragen aan dit auditrisico (PAR_{eng}). De factoren van Knechel zijn daarin begrepen, al zijn ze opnieuw geclassificeerd en gegeneraliseerd. De lijst pretendeert niet uitputtend te zijn. Verdere research is nodig om te zien of de opgesomde factoren standhouden en of er nieuwe moeten worden toegevoegd. Scorecard 2 geeft de risicofactoren die bijdragen aan PAR_{eng} in een matrix samen met de verschijningsvormen van PAR zoals die in scorecard 1 zijn gegeven.

Eerst moeten de tolerantiewaarden voor PAR_{ex_ante} worden vastgesteld en ingevuld in scorecard 1. Vervolgens moet er een schatting worden gemaakt van de werkelijke $P * D$, met gebruikmaking van tabel 1 en ingevuld in scorecard 2 voor iedere verschijningsvorm van PAR_{eng} en dat vanuit elk van de twaalf risicofactoren. De benodigde informatie kan men verkrijgen uit research in externe bronnen, zoals ratings

Scorecard 1. Waarden voor verschijningsvormen van Professioneel Auditrisico met voorbeeldwaarden voor PAR_{ex_ante}

Verschijningsvormen van Professioneel Auditrisico	Tolerantiewaarden	Gemeten waarden
	PAR_{ex_ante}	PAR
1. Verlies aan auditinkomen	2.4	
2. Verlies van een klant/ marktaandeel	1.8	
3. Reputatieverlies	1.0	
4. Civiele aansprakelijkheid	1.0	
5. Disciplinaire actie door het professionele instituut	1.0	
6. Idem door toezichthouders	1.0	
7. Strafrechtelijke vervolging	0.2	
8. Professionele beëindiging	0.2	

Scorecard 2. Risicoprofiel van een nieuwe klantrelatie

Verschijningsvormen Professioneel Auditrisico

8. Professionele beëindiging
 7. Strafrechtelijke vervolging
 6. Maatregelen door toezichthouders
 5. Disciplinaire maatregel professioneel instituut
 4. Civiele aansprakelijkheid
 3. Reputatieverlies
 2. Verlies van een klant/marktaandeel
 1. Verlies aan auditinkomen

Risicofactoren bijdragend aan PAR_{eng}	1	2	3	4	5	6	7	8
1. Blootstelling aan hoge druk van aandeelhouders								
2. Strengere regulering van de business								
3. Twijfelachtige soliditeit van de business								
4. Ethische twijfels aan de business van de geauditeerde								
5. Blootstelling geauditeerde aan corruptie en misbruik								
6. Ernst lopende civiele, strafrecht. of fiscale procedures								
7. Twijfelachtige relatie met toezichthouders								
8. Slechte relatie met aandeelhouders/misinformatie								
9. Twijfelachtige vroegere relaties met auditors								
10. Dubieuze financiële status (ratings, winstgevendheid)								
11. Onvoldoende onafhankelijkheid auditor								
12. Gebrek aan auditor's expertise met betrekking tot soort business								
Cumulatieve score van de klant's risicoprofiel								

van analisten, auditrapporten, jaarrekeningen, financieel nieuws, juridische bronnen, de eigen kennisdatabase van de auditor, consultatie van voormalige auditors van de klant en uit een aantal interviews met representanten van de klantorganisatie. De twaalf regels in scorecard 2 moeten worden geaccumuleerd, teneinde het risicoprofiel van de toekomstige klant te verkrijgen per verschijningsvorm van PAR . De geaccumuleerde score moet worden geïmporteerd in scorecard 1. De laatste stap is de confrontatie met PAR_{eng} ($=P * D$) met PAR_{ex_ante} . Dit levert de analyse op van het Professioneel Auditrisico met betrekking tot het aangaan van een nieuwe klantrelatie, ofwel het engagementrisico. Het volgende moment is de soortgelijke analyse gereleerd aan het aanvaarden van een nieuwe opdracht binnen een bestaande klantrelatie.

5 Professioneel Auditrisico op het moment van aanvaarding van een nieuwe opdracht binnen een bestaande klantrelatie (opdrachtaanvaardingsrisico, Engels: assignment risk of PAR_{ass})

In deze situatie bestaat er al een relatie met de klant. PAR_{ass} concentreert zich op de aanvaarding van een

nieuwe of vernieuwde opdracht. Zelfs in het geval van herhaling van een audit of auditcyclus voor de tiende keer, kan de auditor blootstaan aan bedreigingen, bijvoorbeeld uit (gedrags)veranderingen in de organisatie, van het management, van de klant-attitude of van diens gedrag. In het geval dat een bestaande relatie een geheel nieuwe opdracht voorstelt, kan de auditor blootstaan aan geheel nieuwe bedreigingen. Tien risicofactoren zijn onderscheiden, voornamelijk te analyseren aan de hand van ervaringen van de auditor met de bestaande opdrachtgever/geauditeerde gedurende eerdere audits. Scorecard 3 zet de factoren in een matrix met de verschijningsvormen van PAR zoals vermeld in scorecard 1.

Opnieuw moeten eerst in iedere cel tolerantiewaarden voor PAR_{ex_ante} worden vastgesteld en ingevuld in tabel 1. Vervolgens moet een schatting worden gemaakt van de werkelijke $P * D$ en ingevuld in scorecard 3 voor iedere verschijningsvorm van PAR_{ass} , gebruikmakend van tabel 1 en dat vanuit elk van de tien risicofactoren. De laatste factor is een ietwat afwijkende. Hier loopt de auditor aan tegen een vermoede majeure verandering in het risicoprofiel van

Scorecard 3. Risicoprofiel van een nieuwe auditopdracht binnen een bestaande klantrelatie

Verschijningsvormen Professioneel Auditrisico								
8. Professionele beëindiging								
7. Strafrechtelijke vervolging								
6. Maatregelen door toezichhouders								
5. Disciplinaire maatregel professioneel instituut								
4. Civiele aansprakelijkheid								
3. Reputatieverlies								
2. Verlies van een klant/marktaandeel								
1. Verlies aan auditinkomen								
Risicofactoren bijdragend aan PAR _{ass}	1	2	3	4	5	6	7	8
1. Sterk vooroordeel/scepsis van auditdoelgroep								
2. Twijfel over management integriteit								
3. Mager risicomanagement, control & risk self assessment								
4. Magere governance/management control								
5. Slechte opvolging van voornemens tot betere org & i.c.								
6. Slechte opvolging auditaanbevelingen								
7. Hoge omvang/frequentie van fraude- en misbruikgevallen								
8. Slechte management rapportage en hands-on control								
9. Slechte behandeling auditors/mager budget								
10. Majeure verandering in de klants risicoprofiel								
Cumulatieve score voor een nieuwe auditopdracht								

de klant. Dit noopt tot een herhaling van de analyse van PAR_{eng}, met behulp van scorecard 2. De tien regels in scorecard 3 moeten worden geaccumuleerd, om het risicoprofiel te krijgen van de nieuwe auditopdracht, per verschijningsvorm van het Professioneel Auditrisico. De cumulatieve score wordt geïmporteerd in scorecard 1. De laatste stap is de confrontatie van PAR_{ass} (= P * D) met PAR_{ex_ante}. Dit geeft het Professionele Auditrisico gerelateerd aan het aanvaarden van een nieuwe of vernieuwde opdracht binnen een bestaande klantrelatie.

Het volgende moment is de analyse van het auditrisico gerelateerd aan het uitgeven van een opinie (of in accountantstermen: verklaring), als sluitstuk van de uitvoering van een complete audit of auditcyclus.

6 Professioneel Auditrisico op het moment van afgifte van een oordeel (opinierisico of PAR_{opi}), volgend op de voltooiing van een audit of een auditcyclus

Het meest voorkomende niveau van vaststellen van Professioneel Auditrisico is het moment waarop de audit is voltooid, de conclusies getrokken zijn en de auditor op het punt staat zijn oordeel af te geven. In het geval dat de bevindingen zodanig zijn dat er geen

ongekwalificeerd positief oordeel kan worden afgegeven, zal de auditor de opdrachtgever zo spoedig mogelijk daarvan moeten verwittigen en bespreken hoe men verder zal gaan. In sommige gevallen biedt uitbreiding van het auditwerk een oplossing om toch tot een ongekwalificeerd positief oordeel te leiden. In zulke gevallen moet de auditor extra budget vragen en krijgen. In andere gevallen is het de geauditeerde die actie moet nemen, bijvoorbeeld ingeval van een verkeerd toegepaste boekhoudregel in een verantwoording. In weer andere gevallen kan het obstakel niet worden weggenomen door meer auditwerk of door het management. In die situatie zijn er twee scenario's denkbaar:

- het obstakel is van beperkte significantie, in welk geval
 - een gekwalificeerd oordeel een uitweg kan bieden;
 - het obstakel is significant en staat een positief oordeel
- in de weg.

Het zou een misverstand zijn te denken dat de inschatting van Professioneel Auditrisico beperkt moet worden tot het ten onrechte uitgeven van een positief oordeel. Ontijdige of niet-uitgifte van een positief oordeel kan ernstige gevolgen hebben voor de opdrachtgever en/of de geauditeerde. Bijvoorbeeld ingeval van een oordeel over de jaarrekening van een

beursgenoteerd bedrijf, of over een te acquireren onderneming of beoogde fusiepartner, of ingeval van een third-party oordeel (over een product of dienst), dat nodig is om commercieel te overleven. De opdrachtgever, de geauditeerde of de doelgroep van het oordeel kunnen de auditor verwijten disproportionele schade te hebben veroorzaakt, door niet-tijdige uitgifte van een ongekwalficeerd positief oordeel. In dit artikel wordt deze zijde van PAR niet verder uitgewerkt.

De oefening begint opnieuw met scorecard 1 met het inschatten en invullen van tolerantiewaarden voor PAR_{ex_ante} , gebruikmakend van tabel 1. De volgende stap is het analyseren van Bedrijfsrisico's (BR), Control-effect (CE) en Auditdiepte (AD). Deze analyse zal voorlopig worden gedaan zonder confrontatie met verschijningsvormen van PAR, iets dat in een latere, separate stap zal plaatsvinden.

Het Professionele Auditrisico op het moment van uitgifte van een oordeel (PAR_{opi}) heeft overeenkomsten met de traditionele auditrisicoformule. Het is een functie van drie elementen:

- Bedrijfsrisico (BR) als substituuat voor Inherent Risico (IR);
- Control (lees interne controle) effect (CE) als reciproke voor Interne Controlerisico (ICR);
- Auditdiepte (AD) min of meer als reciproke van Detectierisico (DR).

Voor de betekenis van IR, ICR en DR wordt verwezen naar deel 1 (Mollema, 2003).

$PAR_{opi} = f((BR - CE), AD)$, of in woorden: het Professioneel Auditrisico op het moment van het afgeven van een oordeel is een functie van Bedrijfsrisico minus Control-effect en van Auditdiepte. Zoals de formule al aangeeft worden de componenten ervan niet vermenigvuldigd, maar beoordeeld in de context van hun werkelijke onderlinge relatie.

Zoals het geval is met Inherent Risico, wordt Bedrijfsrisico gedefinieerd met uitsluiting van dempende interne controle-effecten. Hoewel in de praktijk zo'n strikte scheiding moeilijk te handhaven is, zal dit het model niet frustreren. In de volgende paragrafen 6.1 tot en met 6.3 worden de genoemde elementen verder bediscussieerd.

6.1 Analyse van het Bedrijfsrisico

De klassieke auditrisicoanalyse spreekt van Inherent Risico waarvan de bepalende factoren beredeneerd zijn vanuit de auditor. Klijnsmit, Sodekamp en Wallage (2003, pp. 192-193) constateren: 'Het bedrijfsrisico voor de cliënt is dikwijls verweven met Inherent Risico'.

Scorecard 4. Bedrijfsrisicomodel

Daarom achten zij het nuttig eerstgenoemde risico's 'een plaats te geven binnen een nieuw Audit Risk Model'. In het hier uitgewerkte model gebeurt dat ook door bedrijfsrisico als één van de drie componenten te benoemen van de auditrisicoformule. De typisch auditor-gerelateerde bedrijfsrisico's verdwijnen daarmee niet uit het model. Ze zijn deels terug te vinden in PAR_{eng} en PAR_{ass} en deels in de component Auditdiepte (AD).

Het bedrijfsrisicomodel is driedimensionaal, zoals zichtbaar wordt in scorecard 4. De drie dimensies tonen domeinen, gebeurtenissen en oorzaken. Een gebeurtenis is altijd ongewenst en kan plaatsvinden in een domein, veroorzaakt door iets.

De domeinen bevatten zes subcategorieën:

- productspecifiek risico, zoals renterisico of marktrisico voor een bank, langlevensrisico voor een verzekeraar of milieurisico voor een olie- en gasbedrijf;
- operationeel risico, zijnde het risico dat voortvloeit uit in-bedrijf-zijn, en niet zozeer voortvloeiend uit de producteigenschappen, zoals brandrisico, stakingsrisico, et cetera;
- informatierisico, zijnde het risico van het afgeven van foutieve informatie aan het management, aan interne of externe toezichthoudende organen, aan overheidsorganen, aan accountants en – last but not least – aan de financiële wereld;
- ICT-risico, zijnde het risico van falende ICT-ondersteuning van de productie, registratie en verantwoording, inkoop, verkoop en marketing, en informatie en communicatie;
- compliancerisico, zijnde het niet voldoen aan wet- en regelgeving, gedragscode en ethiek;
- majeure veranderingen in het opdrachtprofiel, die de auditor dwingen om PAR_{ass} opnieuw vast te stellen. Men zou kunnen beargumenteren dat in operationeel

risico informatierisico, ICT-risico en compliancerisico zijn inbegrepen. Echter, omdat deze zich hebben ontwikkeld tot afzonderlijke métiers, worden ze als aparte categorieën onderscheiden. Informatierisico is gedurende vele decennia het object geweest van financiële control en audit. Het is de focus geweest van het COSO-model gedurende vele jaren. Het COSO-model heeft relatief een grote acceptatie, maar is verouderd, zoals ook waargenomen door Root (1998). Inmiddels is in juni 2003 een eerste proeve verschenen van een update onder de naam Enterprise Risk Management Framework (COSO, 2003).

ICT-risico is een zeer gespecialiseerd domein, waarin ICT-security en ICT-audit een bestaansrecht hebben gevonden. Compliancerisico heeft een enorme vlucht genomen, als gevolg van de vele regels die een bedrijf moet naleven en van de ernstige consequenties van niet nakomen van deze regels. Veel bedrijven gaan verder dan het nastreven van voldoen aan wet- en regelgeving, door op zichzelf een gedragscode toe te passen. Zulke codes kunnen gaan over regels voor de omgang met klanten, aandeelhouders, andere belanghebbenden en personeel en over de ethische standaard waartegen een bedrijf wil worden gemeten.

Een majeure verandering in het opdrachtprofiel kan optreden tijdens de audit of auditcyclus. In dat geval moet de auditor de vorige fase opnieuw doorlopen, dat wil zeggen het analyseren van het Professioneel Auditrisico gerelateerd aan de aanvaarding van een nieuwe opdracht (PAR_{ass}) met behulp van scorecard 3. Binnen iedere categorie moet een gedetailleerde lijst van risicocategorieën worden onderscheiden. Voor het domein van productspecifieke risico's zijn er bestaande modellen per industriële sector, zoals banken, verzekeraars, olie- en gasbedrijven, et cetera. Voor operationeel risico zijn meer recent modellen ontwikkeld, bijvoorbeeld in het bankwezen op initiatief van het Basel Comité van Banktoezichthouders. Informatierisico is universeel, zij het veel kritischer voor beursgenoteerde ondernemingen dan voor andere organisaties. Het bedrijfsrisicomodel dat de auditor gaat gebruiken kan het best worden afgeleid van bestaande modellen, zoals gehanteerd door risicomanagementfuncties en/of toegepast in Control & Risk Self Assessment (CRSA)-programma's binnen de organisatie. Indien zulke modellen ontbreken, dan zal de auditor zelf een risicoanalyse moeten opzetten. Het is van groot belang dat de auditor overeenstemming zoekt met de geauditeerde, voor wat betreft de classificatie van specifieke bedrijfsrisico's. Een enkele audit dekt zelden alle risicocategorieën. Wat het wel dekt hangt in hoge mate af van het type audit dat wordt gevraagd. Maar een auditcyclus van een intern

audit departement kan een brede range van risico's bestrijken. Hier hangt alles af van het toegepaste audit-charter.

Bovenop de kubus vindt men de zogenaamde risico-gebeurtenissen die kunnen plaatsvinden in de verschillende domeinen. Deze hebben niet de pretentie volledig te zijn. Op de rechterflank ziet men de oorzaken van bedrijfsrisico's, die zowel menselijk, technisch als omstandelijk kunnen zijn. Hun functie is om zoveel mogelijk risico's te bedenken en ook om een startpunt voor interne controlemaatregelen te vinden. Bijvoorbeeld: het risico van een materiële fout in een verantwoording wordt gevonden in de cel waar informatierisico, gebrek aan integriteit en fouten (of mismanagement) samenkomen. De aanvaarding van een hoog kredietrisico in een bank in de cel waar productspecifieke risico's, volatiliteit en mismanagement het pad kruisen. Een situatie van een gecrashte computer in de cel waar ICT-risico, disruptie en 'acts of God' samenkomen.

Vervolgens komt de vraag op wat er gebeurt in de cellen van de kubus, op het niveau van het meten van bedrijfsrisico. De confrontatie met de verschijningsvormen van PAR volgen later, na de analyse van de dempende invloed van de interne controle. In de cellen van de kubus moeten scores worden ingevuld voor de theoretische schade (D_{th}), zoals tabel 1 aangaf. Deze worden verkregen uit de vermenigvuldiging van de maximum schade (D_{max}), dat is de schade in een slechtst-denkbare scenario van optreden, en de originele waarschijnlijkheid (P_{or}), dat is de waarschijnlijkheid van optreden, beide met uitsluiting van het dempende effect van de interne controle. P_{or} is een fractie of percentage. Het resultaat wordt genoteerd als: $D_{th} = D_{max} * P_{or}$.

Zoals eerder gesteld wordt het bedrijfsrisico in eerste instantie geanalyseerd voor het dempende effect van de interne controle. Echter, de werkelijke bedrijfsrisico's waaraan het bedrijf blootstaat zijn die met inbegrip van het (dempende) interne controle-effect, hier Control-effect genoemd.

6.2 Analyse van het Control-effect (CE)

De klassieke auditrisicotheorie hanteerde ICR of (Interne) Controlerisico, zijnde het risico dat de interne controle een schade niet weet te voorkomen, noch te beperken. Hier gaat de voorkeur echter uit naar het gebruiken van Control-effect (CE), zijnde de dempende werking die interne controlemaatregelen hebben op het Bedrijfsrisico (BR), of liever op D_{th} , de

Scorecard 5. Model Bedrijfsrisico en Control-effect

theoretische schade. De reden is dat interne controle in zichzelf een set maatregelen is om risico te dempen door preventie en detectie. Interne controle kan in een model worden vervat. Er zijn verschillende van zulke modellen, waaronder COSO de meest verbreide. Het is zinvol om voor het interne controlemodel aan te sluiten bij het model dat wordt gebruikt voor risicomanagement binnen het bedrijf. Scorecard 5 toont het model voor Control-effect als een uitbreiding van het bedrijfsrisicomodel zoals getoond in scorecard 4, waardoor men inzicht heeft in de theoretische schade (D_{th}). Dan wordt voor iedere cel, en daarbinnen voor ieder onderscheiden risico het Control-effect (CE) geanalyseerd, met name voor wat betreft zijn dempende werking op de theoretische schade (D_{th}). Het dempende effect kan op twee manieren optreden:

- door de originele kans van optreden (P_{or}) naar beneden te brengen, dat wil zeggen door preventie;
- door beperking van de schade, ofwel ervoor zorgen dat D beneden D_{max} blijft door tijdige detectie en correctie.

Dit levert de residuele kans van optreden (P_{res}) en de residuele schade (D_{res}) op. De vermenigvuldiging van deze twee geeft het gewenste resultaat van de exercitie: het residuele risico uitgedrukt als residuele theoretische schade ($^{res}D_{th}$).

Tabel 1 hielp al eerder de theoretische schade D_{th} te berekenen. Nu kan dezelfde tabel worden gehanteerd voor het inschatten van de residuele theoretische schade ($^{res}D_{th}$). Vervolgens kan men $^{res}D_{th}$ per domein aanhouden tegen de verschijningsvormen van Professioneel Auditrisico, zoals scorecard 6 laat zien.

De risico's verschijnen als $^{res}D_{th}$ per domein en tellen op tot een cumulatief risico per verschijningsvorm van PAR. Deze waarden zijn input voor scorecard 8 (zie hierna) die is gebaseerd op scorecard 1. Daarmee is men aangekomen bij conclusies over het Professioneel Auditrisico met betrekking tot het afgeven van een oordeel (PAR_{opi}), met inbegrip van alle effecten van het interne controlesysteem. De vergelijking met $PAR_{ex-ante}$ moet wachten tot nadat de auditdiepte is geanalyseerd en vastgesteld.

6.3 Analyse van de Auditdiepte

Bij het analyseren van het Professionele Auditrisico op het moment van afgifte van een oordeel (PAR_{opi}), is de laatste stap die men moet zetten het kijken naar de Auditdiepte (AD). De vereiste auditdiepte is gedefinieerd als de inspanningen die de auditor moet verrichten om tot voldoende onderbouwing te komen

Scorecard 6. Risicoprofiel voor het afgeven van een audit-opinie

Risicodomeinen	Product specifiek risico	Operationeel risico	Informatie risico	ICT risico	Compliance risico	Accumulatie
Verschijningsvormen van PAR_{opi}						
Verlies aan auditinkomen						
Verlies van een klant / marktaandeel						
Reputatieverlies						
Civiele aansprakelijkheid						
Disciplinaire actie door het prof. instituut						
Idem door toezichthouders/rechtbanken						
Strafrechtelijke vervolging						
Professionele beëindiging						

Scorecard 7. Vereiste auditdiepte als functie van residueel theoretische schade $resD_{th}$

Scorecard 8. Vaststellen Professioneel Auditrisico bij het afgeven van een oordeel (PAR_{opi})

	tolerantie	gemeten	vereiste	werkelijke
Versijningsvormen van Professional Auditrisico bij het afgeven van een oordeel	waardes PAR_{ex_ante}	waardes PAR_{opi}	audit diepte	audit diepte
Verlies aan auditinkomen				
Verlies van een klant/ marktaandeel				
Reputatieverlies				
Civiele aansprakelijkheid				
Disciplinaire actie door het profess. instituut				
Idem door toezichthouders/ rechtbanken				
Strafrechtelijke vervolging				
Professionele beëindiging				

voor het afgeven van een positief oordeel. Deze parameter wordt voornamelijk bepaald door de resultaten van het inschatten van BR en CE, of in termen van de doelvariabele, van het residuele risico. In woorden: zoveel te meer er op het spel staat en zoveel te minder het dempende effect van de interne controle is, des te meer auditinspanningen de auditor zal moeten leveren om tot een ongekwalificeerde positieve opinie te komen. Dit is echter alleen waar binnen zekere grenzen. Als eenmaal het residuele risico een zekere grenswaarde overschrijdt, voortvloeiend uit de originele schade of uit een gebrek aan interne controle, wordt

het ineffectief om additionele auditinspanningen aan te wenden. Het resultaat zal toch een negatief oordeel zijn. Scorecard 7 illustreert dit.

De scorecard laat zien dat de Auditdiepte zal moeten toenemen wanneer de theoretische schade toeneemt. $resD_{th}$ is uitgezet op een vijfpuntsschaal, zoals de verticale as laat zien. In het centrum van scorecard 7 kunnen additionele auditinspanningen een gebrek aan interne controle compenseren. Dit is vooral waar in de context van financiële audit, maar ook daar slechts beperkt. De interne controle is zo'n alles omvattend systeem dat materiële deficiënties al snel de auditcapaciteit ver overstijgen. Als $resD_{th}$ eenmaal erg materieel wordt, ziet de auditor zich al snel geconfronteerd met een hopeloos perspectief, waarin additionele auditinspanningen geen of nauwelijks effect hebben. Met behulp van scorecard 7 werd de vereiste auditdiepte vastgesteld. Nu moet de auditor de werkelijke auditdiepte vaststellen, die ook een functie is van een aantal persoonlijke keuzes van de auditor, van zijn kennis van de business, van de coöperatieve opstelling van de geauditeerde en van het beschikbare budget. De werkelijke auditdiepte wordt uitgezet op dezelfde vijfpuntsschaal als de vereiste auditdiepte. Zowel de vereiste als de werkelijke auditdiepte wordt geïmporteerd in scorecard 8 (zie hierna) en geconfronteerd met de verschijningsvormen van PAR.

6.4 Vaststellen van PAR_{opi}

De laatste stap in de exercitie is te beslissen over het Professionele Auditrisico in verband met het afgeven van een oordeel (PAR_{opi}).

In scorecard 8 worden de toleranties voor PAR (PAR_{ex_ante}) uit scorecard 1 geïmporteerd. De gemeten waarden voor PAR zijn verkregen uit scorecard 6. Nu kan men de beide vergelijken en zien of PAR_{opi} beneden PAR_{ex_ante} uitkomt, wat de auditor vertelt of het effect van de residuele theoretische schade per verschijningsvorm van het Professioneel Auditrisico de limietwaarden al dan niet heeft overschreden. Tegelijk wordt de werkelijke Auditdiepte vergeleken met de vereiste. De confrontatie van Auditdiepte met verschijningsvormen van PAR gebeurt om te bepalen welke daarvan worden getriggerd door de discrepantie. Wanneer de werkelijke Auditdiepte achterblijft bij de vereiste moet de auditor zich realiseren dat zijn Professionele Auditrisico aanzienlijk toeneemt. Het is voor een professionele beroepsbeoefenaar voor de raad van tucht of voor de civiele rechter moeilijk uit te leggen waarom hij beneden zijn eigen standaard

heeft gepresteerd. Een tekort aan budget zal de auditor niet voorzien van het juiste excuus.

7 Samenvatting

De stappen gezet in het vaststellen van PAR_{opi} kunnen als volgt worden samengevat:

- Stap 0: Bepaal de tolerantiewaarde voor PAR_{ex_ante} in scorecard 1, gebruikmakend van tabel 1.
- Stap 1: Analyseer $P_{or} * D_{max}$ voor iedere cel van scorecard 4 en gebruikmakend van de techniek van tabel 1. Gewogen voor materialiteit verkrijgt men de theoretische schade D_{th} per risicocategorie.
- Stap 2: Importeer de resultaten in scorecard 5.
- Stap 3: Analyseer het dempend effect van de interne controle op P_{or} en D_{max} resulterend in P_{res} en D_{res} voor iedere cel van scorecard 5 en gebruikmakend van de techniek van tabel 1.
- Stap 4: Vermenigvuldig P_{res} and D_{res} resulterend in het residuele risico, uitgedrukt als residuele theoretische schade $^{res}D_{th}$.
- Stap 5: Vergelijk de aldus verkregen $^{res}D_{th}$ per risico categorie met de verschijningsvormen van PAR_{opi} , gebruikmakend van scorecard 6.
- Stap 6: Accumuleer de risicoscores per domein tot de eindscore in scorecard 6 en importeer de resulterende waarden in scorecard 8.
- Stap 7: Importeer de tolerantiewaarden PAR_{ex_ante} van scorecard 1 in scorecard 8.
- Stap 8: Bepaal de vereiste auditdiepte, als functie van de residuele theoretische schade $^{res}D_{th}$ met behulp van scorecard 7. Importeer de resultaten in scorecard 8.
- Stap 9: Evalueer de werkelijke Auditdiepte en vul het resultaat in in scorecard 8.
- Stap 10: Evalueer het Professionele Auditrisico, door vergelijking van PAR_{opi} met PAR_{ex_ante} en de werkelijke auditdiepte met de vereiste.

Nu de analyse is voltooid, valt te evalueren wat is toegevoegd aan de auditrisicotheorie. De beste manier om dat te doen is te zien of daadwerkelijk antwoorden zijn gevonden op de in de inleiding (paragraaf 1) gestelde uitdagingen, ontleend aan deel 1 (Mollema, 2003). Deze waren:

- 1 de kritische momenten voor foute beoordeling analyseren alsmede welke factoren wanneer van toepassing zijn;
- 2 de werkelijke omvang van de schade in de formule opnemen, in plaats van te werken met materiële fouten;
- 3 de reikwijdte van de formule uitbreiden naar operationele en ICT-audit;

4 de resultaten van bedrijfsrisicoanalyse in de theorie opnemen.

ad 1. Feitelijk zijn drie momenten onderscheiden waarop Professioneel Auditrisico manifest kan worden:

- aangaan van een nieuwe klantrelatie;
- aanvaarden van een nieuwe opdracht binnen een bestaande klantrelatie;
- afgeven van een oordeel na voltooiing van de audit of auditcyclus.

ad 2. Door introductie van theoretische schade is de werkelijke omvang van de schade in de formule opgenomen.

ad 3. De theorie die in dit artikel is ontwikkeld, is voornamelijk gebaseerd op Risicomanagement- en CRSA-modellen, zoals men die tegenwoordig tegenkomt in bepaalde industriële sectoren. Daarmee is de scope van de formule verbreed tot andere types audit, zoals operationele en ICT-audit. Door het onderscheiden van informatierisico als aparte categorie, is de financiële audit als toepassingsdomein van de theorie niet verloren gegaan.

ad 4. Door Inherent Risico te vervangen door Bedrijfsrisico als gehanteerd door de eigen risicomanagementafdeling van de onderneming en/of in haar CRSA-sessies, is het bedrijfsrisico daadwerkelijk in de Auditrisicoformule opgenomen.

Zoals zichtbaar wordt zijn de vier uitdagingen beantwoord, waarmee hopelijk een bijdrage is geleverd aan vernieuwing van auditrisicotheorie. ■

Noot

- 1 $AR = (IR + ICR) + DR$, of voluit Auditrisico = (inherent risico + interne controle risico) + detectierisico.

Literatuur:

- Arens, A.A, R.J. Elder en M.S. Beasley, (2003), *Auditing and Assurance Services, an integrated approach*, 9th edition, Prentice Hall, New Jersey.
- COSO Committee, (2003), *Enterprise Risk Management Framework Released for Comment*, AICPA, New York, te vinden op www.erm.coso.org.
- Hayes, R. en A. Schilder, (1999), *Principles of Auditing*, McGraw-Hill Publishing Company, London.
- International Federation of Accountants, (2003a), *International Standards on Auditing 200 Objective and General Principles Governing an Audit of Financial Statements*, te vinden op www.ifac.org.
- International Federation of Accountants, (2003b), *International Standard on Auditing 315 Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, te vinden op www.ifac.org.
- Klijnsmit, P., M. Sodekamp en Ph. Wallage, (2003), Bedrijfsrisico van de accountant en het Audit Risk Model, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 77, nr. 5, mei, pp. 190-195.
- Knechel, W.R., (2001), *Auditing*, 2nd edition, South Western College Publishing Thomson Learning Cincinnati.
- Mollega, K.Y., (1991), *Zichtbaarheid van informatiekwaliteit*, Samsom Bedrijfsinformatie, Alphen a/d Rijn (academisch proefschrift).
- Mollega, K.Y., (2003), Auditrisico, meer dan ooit en issue! (1), in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 77, nr. 12, december, pp. 551-556.
- NivRA, (2003) *Richtlijnen voor de Accountantscontrole*, Kon. NIVRA Amsterdam.
- Public Oversight Board, (2000), *Panel on Audit Effectiveness – Report and Recommendations*, www.pobauditpanel.org/download.html.
- Root S.J., (1998), *Beyond COSO*, John Wiley & Sons, New York.
- Tabaksblat, M., (2003), *Commissie corporate governance. De Nederlandse corporate governance code. Beginselen van goede corporate governance en best practice bepalingen*. Juli 2003, www.commissiecorporate-governance.nl.
- U.S. Congress, Sarbanes Oxley Act of 2002; <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>.