Het effect van risico-informatie op de risico-perceptie van IT-auditors

Arno Nuijten, Bert Zwiers en Gert van der Pijl

SAMENVATTING Het inschatten van risico's vormt een centraal element in de meeste benaderingen van 'corporate governance' en de daarmee samenhangende 'IT-governance'. In dit artikel doen we verslag van een onderzoek naar de wijze waarop IT-auditors risico's inschatten. Het blijkt dat de schatting van het risico veel sterker wordt beïnvloed door de verwachte omvang van de schade bij het acuut worden van een bedreiging dan door de kans dat een bedreiging zich daadwerkelijk realiseert. Ook blijkt dat de veel gehanteerde formule waarin risico wordt gehanteerd als het product van de kans van het optreden van een schade en de verwachte omvang daarvan een minder goede verklaring van risico-inschattingen geeft dan een additieve formule.

RELEVANTIE VOOR DE PRAKTIJK Gezien de centrale rol van risico-inschatting in het formuleren van maatregelen ter beheersing van organisaties is het van groot belang dat de bij een risico-inschatting betrokken partijen goed inzicht hebben in elkaars risicopercepties. Dit artikel geeft inzicht in de risicoperceptie van IT-auditors.

Drs. Ing. A.L.P. Nuijten is werkzaam als zelfstandig auditor en consultant op het gebied van beheersing van IT en bedrijfsprocessen. Tevens is hij docent en onderzoeker bij Erasmus School of Accounting and Assurance.
Drs. B. Zwiers is IT Audit Manager Global Markets en Global Clients bij ABN Amro bank in Londen.
Prof. Dr. G.J. van der Pijl is Program Director van de post-doctorale opleiding EDP-auditing van de Erasmus Universiteit en Director of research van Eurac bv. Hij is tevens eind-redacteur van "de EDP-auditor".

1 Inleiding

De toegenomen focus op 'corporate governance' heeft het management bewust gemaakt van het belang van een effectieve interne controle en rapportagestructuur betreffende kansen en bedreigingen op het gebied van informatietechnologie (IT) (Steuperaert, 2004). Niettemin valt het voor veel bedrijven nog niet mee een goed raamwerk voor IT-risico's te implementeren en 'IT-governance' goed in te passen in 'corporate governance (McCollum, 2006; Khan, 2006). Verschillende auteurs benadrukken de belangrijke rol die interne auditafdelingen in deze kunnen vervullen (Hadden et al., 2003; Gramling en Hermanson, 2006; D'Silva en Ridley, 2007). Binnen die interne auditafdelingen spelen IT-auditingspecialisten steeds vaker een rol. Steeds vaker ook worden daarbij de activiteiten van accountants, operational auditors en IT-auditors samengebracht in een geïntegreerde auditaanpak (Mollema en Van der Pijl, 2005). Daarbij past men de planning van de verschillende audits op elkaar aan, steunt op elkaars werkzaamheden en rapporteert gezamenlijk aan het management.

De wijze waarop IT-auditors rapporteren over IT-risico's moet passen in het algemene rapportageraamwerk van de organisatie. Dit vereist dat auditors vanuit de verschillende disciplines en algemeen management een gemeenschappelijke set van risicodefinities en van risiconiveaus hanteren.
In dit artikel doen we verslag van een onderzoek waarin we ons afvroegen hoe de risicoperceptie van IT-auditors tot stand komt. Paragraaf 2 gaat kort in op eerder uitgevoerd onderzoek. In paragraaf 3 geven we een nadere uitwerking van de onderzoeksvraag. Vervolgens bespreken we in paragraaf 4 de onderzoeksopzet en presenteren we in paragraaf 5 de onderzoeksresultaten. In paragraaf 6 worden ten slotte de conclusies getrokken en geven we enige bespiegelingen.

2 Eerder onderzoek

Te gemakkelijk gaan we ervan uit dat de gehanteerde risicoraamwerken garant staan voor eenduidige communicatie van IT-risico's die een goede basis vormt voor de besluitvorming van het algemeen management. Operational auditors, accountants en managers blijken vaak nog problemen te hebben met het onderkennen en wegen van IT-risico's bij hun besluitvorming (Kirkley, 2007). De communicatie tussen experts (IT-auditors) en niet-experts (de andere auditors en algemeen management) wordt vaak verstoord door verschillen in kennis en waardering van de relevante risico's (Sjöberg, 1998; Slovic et al., 1982; Slovic, 2001). Niet het 'objectieve risico' maar de risicoperceptie van actoren blijkt vaak de oordeelsvorming en besluitvorming te bepalen (Sjöberg, 1998; Slovic et al., 1982; Slovic, 2001). Deze bevindingen worden bevestigd door tal van studies in een veelheid van toepassingsgebieden, zoals management control en auditing (Helliar et al., 2002), financiële audits (Verkruijsse, 2005), besluitvorming bij piloten (Hunter, 2002), autorijgedrag (Ranney, 1994; Ulleberg en Rundmo, 2003), verzekeringsbeslissingen (Shanteau, 1992), projectmanagementbeslissingen (Keil et al., 2000) en vele oordelen en beslissingen gerelateerd aan gezondheidsvraagstukken (Schwartz en Griffin, 1986; Gregory et al., 1996). Er is uitgebreid onderzoek naar de manier waarop individuen omgaan met risico-informatie. Dit resulteerde in beschrijvende theorieën zoals de 'Prospect Theory' (Tversky en Kahneman, 1982)[1]. Ook leverde het voorbeelden van irrationele beslissingen op die te danken zijn aan vertekende risicopercepties (Plous, 1993). Vooral op het terrein van de accountancy hebben vele laboratoriumexperimenten bijgedragen aan een beter begrip van verstoringen in de verwerking van informatie betreffende financiële risico's door accountants en besluitvormers (Ashton en Ashton, 1995; Bonner, 1999).

Er is vrijwel geen empirisch onderzoek dat inzicht geeft in de wijze waarop de oordeelsvorming van IT-auditors in de praktijk tot stand komt. Uit onze eigen professionele IT-auditervaring bij diverse financiële instellingen blijkt dat bij het management vele verschillende opvattingen over risico's bestaan. Een wederzijds beter begrip van de risicopercepties van IT-auditors en management kan bijdragen aan een betere onderlinge communicatie over IT-risico's en zodoende tot een betere besluitvorming. Als immers auditors en managers een verschillend beeld hebben van de risico's die gepaard gaan met bijvoorbeeld tekortkoming in de beheersing van een organisatie maakt dit een gesprek over te nemen maatregelen moeilijk, zeker als de verschillen in risicobenadering niet expliciet zijn. Hetzelfde geldt uiteraard voor verschillen in opvattingen over risico's tussen andere bij de risico-acceptatie of het nemen van maatregelen betrokken partijen.

Maar het zou te gemakkelijk zijn de algemene theorieën over oordeelsvorming en besluitvorming zomaar toe te passen op IT-auditors. Theorieën zoals de prospecttheorie zijn nog steeds onderhevig aan kritiek (Nwogugu, 2006), zowel wat betreft hun beperkingen (laboratoriumexperimenten geven geen goed beeld van de werkelijkheid) als hun onduidelijkheden. Ook is duidelijk dat veel domeinen waarin het onderzoek zich afspeelde niet vergelijkbaar zijn met het domein van de IT-gerelateerde risico's (Forlani, 2002).

Zelfs met het overnemen van onderzoek dat specifiek betrekking heeft op accountants en managers moeten we voorzichtig zijn. In tabel 1 presenteren we een overzicht van verschillen in informatieverwerking tussen accountants en IT-auditors. Deze verschillen kunnen leiden tot verschillen in de door Libby (1981) onderscheiden risico-informatieverwerkingsfactoren op de niveaus invoer, verwerking en uitvoer.

Genoemde verschillen maken duidelijk dat resultaten van gedragsexperimenten bij accountants niet zonder meer geldig zijn voor het domein IT-auditing en IT-risicobeoordeling en besluitvorming. Onderzoek dat betrekking heeft op de manier waarop algemeen managers IT-risico's inschatten is ons niet bekend. Wel is er onderzoek naar risicogedrag van managers bij IT-projecten (Keil e.a., 2000). Hoewel het object van beoordeling hier ten dele overlapt met dat van IT-auditors zijn er grote verschillen in opleiding, ervaring en vaak ook in karakter waardoor we er niet op voorhand van uit mogen gaan dat risicogedrag van de professies overeenkomt met dat van IT-auditors.
Wij denken dan ook dat onderzoek naar de manier waarop IT-auditors omgaan met IT-risico-informatie nuttig is voor het professionaliseren van IT-auditing-activiteiten, het verbeteren van de communicatie tussen IT-auditors, financial auditors en management op dit gebied. Daarmee kan het een bijdrage leveren aan de verbetering van de (management) besluitvorming rond IT-risico's.
In dit artikel doen we verslag van een onderzoek waarin we ons afvroegen hoe de risicoperceptie van IT-auditors tot stand komt. In paragraaf 3 geven we

Tabel 1 Verschillen tussen verschillende vormen van auditing

Financial Auditing	IS-Auditing
Invoerniveau: • Het object van risicoanalyse (winst en verlies, financiële cijfers) is goed gedefinieerd en begrensd; • Risico-informatie wordt vaak verkregen door middel van gedetailleerde kwantitatieve en kwalitatieve waarnemingen en substantieel testen; • Risico's zijn goed gedefinieerd en uit te drukken in kwantitatieve financiële termen en toleranties; • Algemeen aanvaarde principes en toleranties zijn al langere tijd beschikbaar en zijn relatief stabiel.	**Invoerniveau:** • Object van risicoanalyse (beheersing van IT-risico's) is moeilijker te definiëren en te begrenzen; • Risico-informatie wordt vaak verkregen door gedetailleerde en technische kwalitatieve observatie; • IT-risico's zijn indirect gedefinieerd (schade aan de kwaliteit van informatie) en moeilijker te kwantificeren dan financiële, reputatie- of operationele schade; • Algemeen geaccepteerde principes en toleranties zijn relatief nieuw.
Processing niveau • Lange historie accountantsopleiding; • Jaarlijks terugkerende observaties van identieke objecten, opbouw van ervaring; • Accountants en IT-auditors verschillen mogelijk in karakteristieken als leeftijd, belangstelling, geslacht, risicogedrag; • Wettelijke rol en daardoor jarenlange interacties met management.	**Processing niveau** • Relatief korte historie van IT-auditing-opleidingen; • Geen lange historie van herhaalde observatie op brede range van objecten; • Accountants en IT-auditors verschillen mogelijk in karakteristieken als leeftijd, belangstelling, geslacht, risicogedrag; • Complexiteit van IT-omgeving vereist vaak het opbreken van audittaak in delen die worden gedekt door verschillende experts en audits; • Nauwe en regelmatige samenwerking tussen auditors en management is relatief nieuw.
Outputniveau (oordeel, voorspelling, beslissing) • Kwalitatieve maten voor accuratesse, consistentie, consensus over oordelen en besluitvorming zijn in de tijd uitgekristalliseerd; • Zelfkennis rond oordeels- en besluitvorming gebaseerd op financiële risico-informatie heeft zich in de loop van de tijd ontwikkeld.	**Outputniveau (oordeel, voorspelling, beslissing)** • Kwalitatieve maten voor accuratesse, consistentie, consensus over oordelen en besluitvorming zijn nog in ontwikkeling; • Zelfkennis rond oordeels- en besluitvorming gebaseerd op IT-risico informatie vereist nog verdere studie en feedback vanuit de praktijk.

daartoe eerst een nadere uitwerking van de onderzoeksvraag.

3 De onderzoeksvraag

In het hier beschreven onderzoek gaan we na hoe de risicoperceptie van IT-auditors tot stand komt bij gebruik van een kwalitatieve risicoanalyse (waarbij risico's worden getypeerd als hoog, gemiddeld of laag) zoals die in hun dagelijkse praktijk wordt gebruikt. We zijn vooral geïnteresseerd in de bijdrage van waarschijnlijkheidsinformatie en impactinformatie aan de risicoperceptie van de IT-auditor.

Sommige studies in andere domeinen concluderen dat de kans op verlies de dominantere factor is, terwijl andere studies de grootte van de schade als dominante factor aanwijzen. Onderzoek op het gebied van verliesverzekering (Shanteau, 1992; Kunreuther en Pauly, 2004) toont aan dat "It is not the magnitude of a potential loss that inspires people to buy insurance voluntarily – it is the probability a loss is likely to occur." Criminologisch onderzoek wijst uit dat de (gepercipieerde) kans om gepakt te worden een grotere afschrikwekkende werking heeft dan de zwaarte van de straf (Lochner, 2007). Studies naar gokgedrag laten zien dat fixatie op de kans op verlies kan leiden tot irrationeel gedrag waarbij mensen de voorkeur geven aan een ongunstige gok boven een zeker verlies (Hershey en Schoemaker, 1980). Anderzijds suggereert een overzicht van risicogedrag van managers (March en Shapira, 1987) dat de grootte van de potentiële schade in de hoofden van managers een grotere rol speelt dan de kans op schade. Ook bij een experiment aangaande risicoperceptie bij IT-projecten (Keil et al., 2000) bleek de grootte van het verlies de meeste invloed te hebben op het gepercipieerde risico. Ons is geen onderzoek bekend waarbij wordt gekeken naar de dominantie van kansen of bedreigingen bij enig type auditors.

De verschillen in resultaten van experimenteel onderzoek in andere domeinen overziend definiëren wij als researchvragen:

1 Dragen kans en schade evenveel bij aan het door IT-auditors gepercipieerde risico?
2 Welke relatie bestaat er tussen kans en schade en het door IT-auditors gepercipieerde risico als zij een bekende kwalitatieve (Laag, Gemiddeld, Hoog, verder LGH) risico-analysemethode gebruiken?

4 Onderzoeksontwerp

Om te komen tot de beantwoording van de onderzoeksvragen hebben we een experiment opgezet waarbij we casussen hebben voorgelegd aan een aantal IT-auditors, allen werkzaam bij de IT-auditafdeling van een grote internationale organisatie actief in de financiële sector[2].
Ieder van de casussen bevat een korte situatiebeschrijving betreffende een tekortkoming in de beheersing van IT en een waardering van die situatie in termen van kans en schade (zie voorbeeld in figuur 1). Er deden 44 deelnemers aan het experiment mee. Ieder van hen kreeg 9 casussen voorgelegd waarin alle mogelijke combinaties LGH voor zowel kans als bedreiging telkens een maal voorkwamen. De casussen behandelen zwaktes in de interne controle op het gebied van "general IT controls'. Een voorbeeld is gegeven in onderstaand kader.

Casus nr 7. Single Point of Failure in het bedrijfsnetwerk
Kans = laag **Schade = Hoog**

Ondanks de redundantie in het (computer)netwerk van het bedrijf is er nog altijd een 'single point of failure' op de centrale locatie. Als de netwerkverbinding van deze locatie uitvalt, kunnen de andere locaties niet meer met elkaar communiceren. De kans bestaat dat de productie volledig stil komt te liggen in geval van een probleem op de centrale locatie.

Ter beoordeling van helderheid en realiteitsgehalte van de casussen voor de gegeven waardering van kans en schade zijn ze voorgelegd aan een aantal deskundigen zowel uit de hoek van het management als uit de hoek van IT-auditing. Daarbij bleek de kwaliteit van de casussen als goed te worden ervaren.
De samenstelling van de groep van respondenten is weergegeven in tabel 2. De tabel laat zien dat het om een relatief ervaren groep gaat en dat het in meerderheid gecertificeerde auditors betreft. De man/vrouwverhouding blijkt niet significant af te wijken van hetgeen gebruikelijk is in de beroepsgroep[3].

De deelnemers werd per e-mail gevraagd om op vrijwillige basis aan het experiment deel te nemen. Hen werd gevraagd hun risicoperceptie van iedere casus weer te geven op een driepuntsschaal (LGH). Ondanks het pleidooi dat Sjöberg (1994) houdt voor een 5-7 puntsschaal kozen we hiervoor omdat dit aansluit bij de praktijk in de werksituatie van de deelnemers.

5 Resultaten

De eerste resultaten van het onderzoek zijn te vinden in figuur 1. In totaal werden 9x44=396 cases aan de deelnemers voorgelegd. Daarvan werden er 108 geclassificeerd als 'laag' risico, 151 als 'middel' risico en 137 als 'hoog' risico. In figuur 1 is te zien dat in elk van deze drie groepen de invloed van de schade op de risico-inschatting groter is dan die van de waarschijnlijkheid. Veranderingen in schade blijken immers tot aanzienlijk grotere wijzigen in de risico-inschatting te leiden dan veranderingen in de kans op het optreden van die schade. Geen van de casussen met grote impact wordt als laag risico gekwalificeerd. Slechts twee maal wordt een casus met een lage impact gekwalificeerd als een hoog risico.

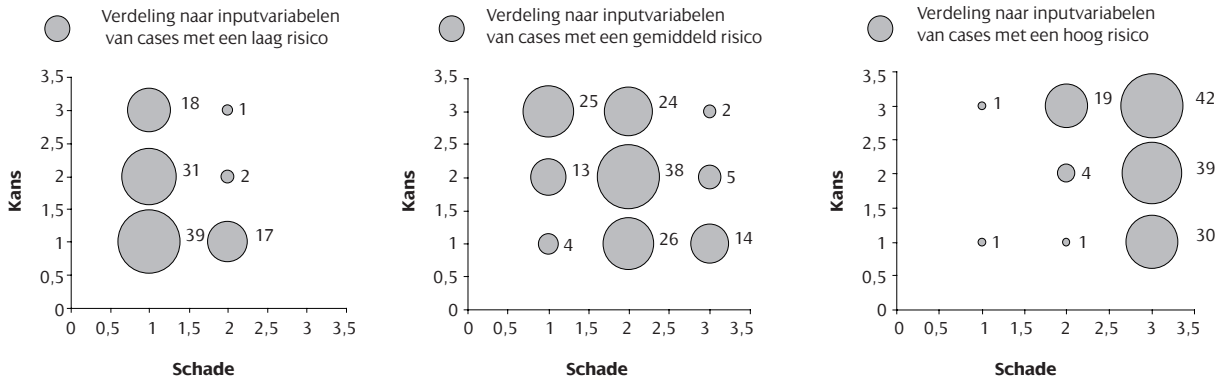
Met behulp van de in figuur 1 weergegeven data konden we onze onderzoeksvragen beantwoorden.

Tabel 2 Samenstelling respons

IT-Auditing ervaring			Geslacht			IT-Auditing opleiding		
< 3 jaar	1	2%	Man	39	89%	Gecertificeerd IT-auditor* (CISA, NOREA)	36	82%
3-5 jaar	11	25%				(nog) niet gecertificeerd		
5-10 jaar	22	50%	Vrouw	5	11%			
10-15 jaar	10	23%						
> 15 jaar	0	0%					8	18%
Totaal	44	100%		44	100%		44	100%

* Naast de over de hele wereld erkende CISA-titel hadden verschillende respondenten ook landspecifieke postinitiële opleidingen gevolgd en waren ingeschreven in het register voor EDP-auditors.

Figuur 1 Weergave van de verdeling van effect en kansfactoren voor casussen met laag, gemiddeld en hoog risico.
Een 1 staat voor 'laag' en een 3 voor 'hoog'.



Dragen kans en schade evenveel bij aan het door IT-auditors gepercipieerde risico?

Een statistische t-test op gepaarde waarnemingen toont aan dat het in figuur 1 weergegeven patroon van risicopercepties dusdanig afwijkt van het patroon dat verwacht kan worden bij een even grote invloed van schade en kans op optreden dat de schade een grotere invloed heeft dan kans. Schade en kans dragen dus niet evenveel bij aan het gepercipieerde risico.

Welke relatie bestaat er tussen kans en schade en het door IT-auditors gepercipieerde risico als zij een bekende kwalitatieve (LGH) risicoanalyse-methode gebruiken?

In de praktijk hanteren we als formule voor het berekenen van schades meestal:

R(isico) = K(ans) x S(chade)

Op basis van onze gegevens testten we eerst door middel van de regressie-analyse de wat algemenere formule:

$R = a_1K \times S + a_2$

Dit gaf als resultaat de formule:

R = 0,227K x S + 1,166

Deze formule verklaarde echter niet meer dan 48 procent van de variatie in de uitkomsten (gecorrigeerde R^2 = 0,485). De geldigheid van de klassieke risicoformule is daarmee dus duidelijk niet aangetoond. Vervolgens testten we de alternatieve formule, waarbij we uitgaan van een additief in plaats van een multiplicatief verband tussen R, K en S:

$R = b_1K + b_2S + b_3$

Met als resultaat:

R = 0,255K + 0,746S + 0,073

In dit geval wordt 67,4 procent van de spreiding van de uitkomsten door de formule verklaard, dat is dus aanzienlijk beter. Ook hier zien we de dominantie van de schadefactor terug. We concluderen dat de relatie tussen kans en schade en het gepercipieerde risico het best wordt weergegeven door de additieve methode.

6 Conclusie en nabeschouwing

In dit onderzoek stelden we vast dat de risicoperceptie betreffende 'general IT-controls' van de IT-auditors die aan het experiment deelnamen in sterke mate wordt bepaald door informatie over de schade die als gevolg van incidenten kan optreden. Deze bevindingen stemmen overeen met die van Keil et al. (2000) gebaseerd op eerder onderzoek naar risicopercepties bij IT-projecten.
Het onderzoek laat ook zien dat de risicoperceptie van de onderzochte groep beter wordt verklaard door een lineaire relatie met kans en schade dan door de gebruikelijke multiplicatieve formule. Dit suggereert dat kans en schade-informatie onafhankelijk van elkaar de risicoperceptie beïnvloeden. Dit zou erop kunnen wijzen dat het voor de mentale verwerkingsprocessen van mensen moeilijk is om kans en schade-informatie op een juiste manier met elkaar in verband te brengen.

Het zou interessant zijn om na te gaan waarom in sommige studies kans en in andere studies schade als voornaamste invloed op de risicoperceptie wordt gevonden. Een mogelijke verklaring wordt gegeven in Forlani's (2002) experiment waarin hij kijkt naar het risicogedrag van managers in de context van nieuwe activiteiten met een hoog risico. Daarin concludeert hij dat het kanselement dominant is in situaties waar managers het gevoel hebben dat ze veel grip hebben op de uitkomst van een activiteit en dat schade de dominante factor is als zij het gevoel hebben weinig invloed op de uitkomst te hebben. Vertalen we dat naar ons experiment dan zouden we kunnen veronderstellen dat IT-auditors minder het gevoel hebben dat zij 'in control' zijn dan algemeen managers of IT-managers. In dat geval zouden auditors meer uitgaan van schades en managers meer van kansen. Dit zou een oorzaak kunnen zijn van gebrekkige communicatie tussen IT-auditors en (IT-)management. Daarbij dienen we wel te bedenken dat in het geval van een accountantsverklaring over het jaarverslag of van een 'in control'-verklaring betreffende andere bedrijfsprocessen van operational auditors er nog een schakel zit tussen de IT-auditor en het algemeen management. In dat geval rapporteren IT-auditors namelijk aan de accountant die op zijn beurt rapporteert aan het management. Ook in de schakels tussen IT-auditor en accountant en tussen accountant en management kunnen zich verschillen in risicoperceptie voordoen.

Een andere verklaring voor de dominantie van schade in ons onderzoek zou gelegen kunnen zijn in het feit dat schade gemakkelijker is te conceptualiseren dan kans. Een studie betreffende ongelukken met elektriciteit laat zien dat in dat geval een nieuwe variabele een belangrijke rol gaat spelen, namelijk 'mentale simulatie'. Dit zou vele 'irrationaliteiten' in menselijke informatieverwerking kunnen verklaren. De ervaring van een persoon zou kunnen helpen bij het visualiseren van kansen of schades en daardoor ook kans of schade de dominante factor maken bij risicoperceptie. Als iemand bijvoorbeeld vaak snelheidscontroles, flitspalen of politie tegenkomt, zou het kunnen zijn dat het gemakkelijker is om de kans van het betrapt worden op een snelheidsovertreding concreet te maken dan de boete die daarvan het gevolg kan zijn. Eigen waarneming van ernstige ongelukken als gevolg van snelheidsovertreding zouden er echter toe kunnen leiden dat schade een dominante rol speelt in de risicoperceptie. Zo zou in het geval van de IT-auditor zijn kennis van en professionele aandacht voor 'wat er fout kan gaan' ertoe kunnen leiden dat hij gemakkelijker wordt beïnvloed door informatie over schade dan door informatie betreffende kansen. Als we deze redenering volgen, zou de dominantie van impactinformatie niet noodzakelijkerwijs ook hoeven te gelden voor het management.

Een beter begrip van de risicoperceptie van IT-auditors, operational auditors, accountants en management kan helpen om de communicatie tussen al deze partijen, en daarmee de effectiviteit van het auditen, te verbeteren. Op zijn beurt zou dit kunnen leiden tot een betere besluitvorming door het (IT-)management. We realiseren ons dat ons onderzoek slechts een klein deel van het gehele onderzoeksgebied bestrijkt. Veel onderzoek is nog nodig. Daarbij denken we in het bijzonder aan:

- Vergelijkbare studies, maar met variaties in onderzoeksstrategie, onderzoeksontwerp en meetschalen. Dit zou de validiteit van de bevindingen over de relatie tussen risico-informatie en gepercipieerd risico kunnen vergroten.
- Vergelijkbare studies met andere respondenten (algemeen management, IT- management, operational auditors, accountants). Dit zou meer zicht kunnen geven op verschillen in de totstandkoming van risicopercepties die de communicatie tussen de diverse groepen kunnen verstoren. Zeker daar waar gestreefd wordt naar vormen van integrated auditing en van het onderling steunen op auditresultaten lijkt dit zeer relevant.
- Vergelijkbare studies gericht op risicoperceptie bij andere soorten IT-controls en op business controls (bijvoorbeeld in het kader van een ERM-risicobenadering of de inrichting van IT-processen zoals beschreven in COBIT).
- Onderzoek naar (verschillen in) risicogeneigdheid van de verschillende typen auditors en (IT-)management.

Zoals al in de inleiding gezegd, denken wij dat nog veel onderzoek naar het omgaan met risico's van alle bij de beheersing van IT betrokkenen nodig is voordat we met enig vertrouwen kunnen rekenen op de goede inpassing van IT-risico's in de vele op risico-analyse en riscobeheersing gestoelde beheersraamwerken. ■

Literatuur

Ashton, R.H. en A.H. Ashton (1995), *Judgment and decision-making research in accounting and auditing*, Cambridge: Cambridge University Press.

Bonner, S.E. (1999), Judgment and decision-making research in accounting, *Accounting Horizons*, vol. 13, pp. 385-398.

D'Silva, K. en J. Ridley (2007), Internal auditing's international contribution to governance, *International Journal of Business Governance and Ethics*, vol. 3, no. 2, pp. 113-126.

Forlani, D. (2002), Risk and rationality: The influence of decision domain and perceived outcome control on the manager's high-risk decisions, *Journal of Behavioral Decision Making*, vol. 15, pp. 125-140.

Gramling, A.A. en D.R. Hermanson (2006), What role is your internal audit function playing in corporate governance?, *Internal Auditing*, vol. 21, no. 6, pp. 37-39.

Gregory, R., P. Slovic, en J. Flynn (1996), Risk perceptions, stigma, and health policy, *Health & Place*, vol. 2, pp. 213-220.

Hadden, L.B., F. Todd DeZoort, en D.R. Hermanson (2003), IT risk oversight: The roles of audit committees, internal auditors and external auditors, *Internal Auditing*, vol. 18, no. 6, pp. 28-30.

Helliar, C., A.A. Lonie, D.M. Power, en C.D. Sinclair (2002), Managerial attitudes to risk: a comparison of Scottish chartered accountants to U.K. managers, *Journal of International Accounting, Auditing & Taxation*, vol. 11, pp. 165-190.

Hershey, J.C. en P.J.H. Schoemaker (1980), Risk taking and problem context in the domain of losses: An expected-utility analysis, *Journal of Risk and Insurance*, vol. 47, pp. 111-132.

Hunter, D.R. (2002), *Risk perception and risk tolerance in aircraft pilots*, Washington: US Department of Transportation-Federal Aviation Administration.

Keil, M., L. Wallace, D. Turk, G. Dixon-Randall, en U. Nulden (2000), An investigation of risk perception and risk propensity on the decision to continue a software development project, *The Journal of Systems and Software*, vol. 53, pp. 145-157.

Khan, K. (2006), How IT governance is changing, *The Journal of Corporate Accounting and Finance*, vol. 17, no. 5, pp. 21-25.

Kirkley, J. (2007), Why the CFO should talk to the CIO, *Financial Executive*, vol. 23, no. 2, pp. 20-22.

Kunreuther, H. en M. Pauly (2004), Neglecting disaster: Why don't people insure against large losses?, *The Journal of Risk and Uncertainty*, vol. 28, pp. 5-21.

Libby, R. (1981), *Accounting and human information processing: theory and applications*, Prentice-Hall: Englewood Cliffs, N.J.

Lochner, L. (2007), Individual perceptions of the criminal justice system, *The American Economic Review*, vol. 97, no. 1, pp. 444-460.

March, J.G. en Z. Shapira (1987), Managerial perspectives on risk and risk taking, *Management Science*, vol. 33, no. 11, pp. 1404-1418.

McCollum, T. (2006), Bridging the Great Divide, *The Internal Auditor*, vol. 63, no. 1, pp. 49-53.

Mollema, K., en G. van der Pijl (2005), Tussen strategie en verandering, Informatie, jrg.47, nr.1, pp. 17-31.

Nuijten, A.L.P., B. Zwiers en G.J. van der Pijl (2007), The effect of risk information on IS-auditor's perceived risk, 1st European Risk Conference, Munster, September 2007.

Nwogugu, M. (2006), A further critique of cumulative-prospect-theory and related approaches, *Applied Mathematics & Computation*, vol 179, no. 2, pp. 451-465.

Plous, S. (1993), *The psychology of judgment and decision making*, New York: McGraw-Hill.

Ranney, T. (1994), Models of driving behaviour: A review of their evolution, *Accident Analysis and Prevention*, vol. 26, pp. 733-750.

Schwartz, S. en T. Griffin (1986), *Medical thinking: The psychology of medical judgment and decision making*, London: Springer-Verlag.

Shanteau, J. (1992), Decision making under risk: Applications to insurance purchasing, in: J.F. Sherry en B. Sternthal, eds., *Advances in Consumer Research*, Chicago: Association for Consumer Research.

Sjöberg, L. (1994), *Perceived risk vs demand for risk reduction*, Rhizikon: Risk Research Report no. 18, Centre for Risk Research, Stockholm School of Economics, Stockholm.

Sjöberg, L. (1998), Risk perception: experts and the public, *European Psychologist*, vol. 3, pp. 1-13.

Sjöberg, L. (2000), Factors in risk perception, *Risk Analysis*, vol. 20, no. 1, pp. 1-11.

Slovic, P. (2001), The risk game, *Journal of Hazardous Materials*, vol. 86, pp. 17-24.

Slovic, P., B. Fischhoff en S. Lichtenstein (1982), Facts versus fears: understanding perceived risks, in: D. Kahneman, P. Slovic en A. Tversky, eds., Judgment under uncertainty: heuristics and biases, (Cambridge: Cambridge University Press.

Steuperaert, D. (2004), IT governance global status report, *Information Systems Control Journal*, vol. 5, pp. 24-27.

Tversky, A. en D. Kahneman (1982), The framing of decisions and the psychology of choice, in: R.M. Hogarth (ed.), Question framing and response consistency, San Francisco: Jossey-Bass Inc. Publishers.

Ulleberg, P. en T. Rundmo (2003), Personality, attitudes and risk perception as predictors of risky driving behaviour among young drivers, *Safety Science*, vol. 41, pp. 427-443.

Verkruijsse, H. (2005), *Beoordeling van processen*, Maastricht.

Noten

1 In deze theorie constateren zij op basis van een hele reeks van experimenten dat de oordelen van mensen systematisch afweken van de beschikbare normatieve modellen.

2 Geïnteresseerden in een meer gedetailleerde beschrijving van onderzoeksstrategie en onderzoeksontwerp verwijzen wij naar: Nuijten, Zwiers en Van der Pijl (2007); zie: www.nottingham.ac.uk/business/rmgic/RiskGovernance&Audit_Nuijten_Zwiers_van-der-pijl.pdf.

3 Een systematische steekproef van 180 personen uit de gehele populatie van Register EDP-Auditors in Nederland (medio 2007) leverde 21 vrouwen (11,7%) en 159 mannen (88,3%) als resultaat.