2008

The Effect of IS-Auditors' Risk Information on ISManagers' Perceived Risk

Arno Nuijten
Erasmus School of Accounting & Assurance, arno.nuijten@planet.nl

Bert Zwiers
Erasmus School of Accounting & Assurance

Gert van der Pijl
Erasmus School of Accounting & Assurance

21st Bled eConference
eCollaboration:
Overcoming Boundaries through Multi-Channel Interaction
June 15 - 18, 2008; Bled, Slovenia

The Effect of IS-Auditors' Risk Information on IS-Managers' Perceived Risk

Arno Nuijten, Bert Zwiers, Gert van der Pijl

Erasmus School of Accounting & Assurance, The Netherlands
arno.nuijten@planet.nl

Abstract

In their efforts to implement an effective IT-governance framework, many companies have acquired IS-Audit staff to provide executive management with information on IS-risks. For the purpose of effective communication, it would be helpful to understand how IS-Auditors, IS-management and executive management shape their perception of IS-risks, since this forms the basis for their judgement and decision making.

In this study we focus on IS-Managers' Risk Perception. More precise we investigated the relative contribution of Probability-information and Impact-information to the Perceived Risk of 32 IS-managers of a financial institution. We conclude that Impact is the more dominant factor determining their perceived risk. We discuss explanations and consequences of the results.

Keywords: IT-Governance, IS management, Risk perception, Probability, Impact, Risk

Introduction

As a consequence of the increased focus on corporate governance, executive management has become aware of the relevance of an effective internal control and reporting structure on opportunities and risks inherent to the company's IS systems (Steuperaert, 2004). Despite this increased awareness, several authors still consider it a challenge to many companies to implement a proper control framework on IS risks and incorporate IT governance in Corporate Governance (McCollum, 2006) (Khan, 2006). Several authors stress the contribution of internal audit staff (Hadden et al., 2003). (Gramling & Hermanson, 2006), (D'Silva & Ridley, 2007) to the corporate governance framework and IT governance framework more specifically.

Auditing of IS-risks has been subject of expertise of dedicated professionals, since the introduction of Information Systems (IS) in companies late sixties and seventies. These pioneer EDP-Auditors mainly focussed on the impact of "Electronic Data Processing" on risks and control of manual business processes, often in batch-oriented mainframe environments, see for example the early work (Frielink, 1961). In the 80's and 90's, further penetration of Information Systems in business processes took place, as well as developments in Information Technology (on-line, client-server, web-based). The number of IS-auditors grew and the profession matured. Techniques and professional standards for executing IS-audits were developed. The worldwide Information System Audit and Control Association (ISACA) played an important role in these developments. Since the introduction of examination and qualification for IS-Auditors in 1978, the number of qualified IS-

Auditors reached a level of 13.000 in the period 1978-2001 and increased towards 55.000 in the year 2007 worldwide[1]. With the foundation of the IT-Governance Institute in 1998, and the introduction of CobiT (release 3 in 2000 and release 4 in 2005) as a framework for IT-Governance, the focus of IS-Auditors has expanded from (technically) proper execution of IS-audits towards providing executive management with valuable information on IS-risks.

This allows more and more companies to use dedicated IS-Audit staff to provide executive management with information on IS-risks. IS-Auditor's reporting on IS-risks should be embedded within the company's general reporting framework, often identifying Low, Medium and High risks, thus allowing executive management to prioritise the implementation of control measures to mitigate financial risks, operational risks and IS-risks. This requires a common set of risk definitions and risk-severity levels to be shared amongst auditors, IS-management and executive management to enable communication on risks.

Simply assuming that such common risk-framework ensures that executive management makes rational decisions on IS-risks would, however, ignore insight obtained from practice and theory. Today's practice shows that executive management still faces difficulties in considering and weighting IS-risks as comprehensive part of their decision making (Kirkley, 2007). From our own consulting experience at several financial institutions, we have seen that executive management often solicits the opinion of his/her IS-managers, when IS-auditors report on IS-risks. The executive manager considers them both to be experts on control and risks related to IS. Both should support the executive manager to make balanced decisions on IS-risks. However, the IS-auditors and IS-managers don't always share the perception of the level of risk associated with findings the IS-auditor has reported. This could disturb the prioritization of IS-risks in risk-reporting, budget assignment and the planning of solutions to mitigate the IS-risks. One could doubt the effectiveness of the internal audit staff to embed IS-risks in the corporate governance framework, when a relatively large amount of reported IS-risks remain unsolved too long. Therefore, from practical perspective, we find it relevant for internal auditors to understand their own biases and the IS-managers' biases with respect to IS-risks.

In this study we focus on the question how IS-managers shape perception of IS-risk, based upon IS-risks that are reported by IS-auditors. In a separate parallel study (Nuijten et al, 2007) we focused on how IS-auditors shape their perception of IS-risks.

From theoretical perspective we know that it is not 'objective' risk but 'perceived risk' that drives an actor's judgment or decision making on risks (Fischhoff et al., 1981). This is confirmed across many studies on various practical areas, i.e. management control and auditing (Helliar et al., 2002), aircraft pilot decision making (Hunter, 2002), car driving behaviour (Ranney, 1994; Ulleberg & Rundmo, 2003), insurance decisions (Shanteau, 1992), project management decisions (Keil et al., 2000) and a variety of decisions (and behaviour) imposing risk to people's health (Schwartz & Griffin, 1986; Gregory et al., 1996). Substantive research on human processing of risk information delivered descriptive theories, such as Prospect Theory (Tversky & Kahneman, 1982), and uncovered a list of information processing biases (Plous, 1993) that explained "irrational" decisions due to biased risk perceptions. These descriptive theories and biases have been tested in many laboratory experiments, for example in the domain of financial auditing (Ashton & Ashton, 1995) (Bonner, 1999)

It would be too easy to simply apply these theories and biases in the area of reporting and decision making on IS-risks. General Theories, such as prospect theory, are still criticised (Nwogugu, 2006) on their restrictions (laboratory settings may oversimplify complexity of real decision making) and unclarities, (i.e. what timeframe to consider, risk-types, reference points for losses vs gains). They

[1] The development in the number of qualified IS-Auditors was found on www.isaca.org. It should be noted that qualified IS-Auditors not exclusively operate in the role of internal IS-Auditor, but can also be found in the role of external IS-auditor, IS-consultant, IS-security expert or in senior (IS-) management positions. IS-Auditors, by nature, are most easily found in organisations where IS are dominant, such as financial institutions and governments.

are also criticised (Forlani, 2002) on assumed domain characteristics, that not necessarily apply to our specific domain of IS-risks.

We have chosen to focus on an element of risk perception that has proven to vary across domains and actors: the relative dominance of probability or impact in risk perception. This could help us understand differences and analogies with other domains. We want to examine the process of shaping risk perceptions in a realistic setting concerning the way in which IS-auditors report risks to executive management. There for we chose to study a situation in which a qualitative framework is used for risk reporting.

In the next paragraphs we will discuss our research questions and describe considerations and choices on the research strategy we followed in this study. After that we present our empirical results and draw some conclusions.

Research Questions

Within this study we are interested in the question how IS Managers shape Risk Perception within a qualitative risk framework that is representative for the way internal audit departments report risks in practice. Especially we are interested in the contribution of Probability-information and Impact-information to IS-managers' Perceived Risk.

Several studies in other domains show Probability of loss as more dominant while other studies show Impact as the more dominant factor in shaping risk perception and/or decision making. Research with regard to loss-insurance (Shanteau, 1992) (Kunreuther & Pauly, 2004), shows that "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." Criminology research shows that the best deterrent to crime is not so much the severity of punishment as the (perceived) likelihood of being caught (Lochner, 2007). Studies of gambling behaviour show that focus on the likelihood of losing can lead to irrational behaviour, in which subjects prefer an unfavourable gamble to accepting a sure loss (Hershey & Schoemaker, 1980). On the other hand, a review of managerial perspectives on risk-taking (March & Shapira, 1987) suggest that the magnitude of potential loss is the more salient than probability in the minds of managers. More specific, the experiment of risk-perception regarding Information System projects (Keil et al., 2000) showed magnitude of loss as having the main effect on perceived risk.

Given the diversity of outcomes in experimental research in other domains, we defined the following research questions:

1. Do Probability and Impact contribute equally to IS-'Managers' Perceived Risk within a given qualitative (LMH) risk framework?
2. What relation is found between given Probability and Impact information and IS managers' Perceived Risk within a given qualitative (LMH) risk framework?

To assure that this research question sufficiently contributes to insight in risk-perception biases of IS-managers related to reporting IS-risks to executive management in practice, we should focus our study on a broadly used framework for reporting risks. We found that a qualitative reporting framework, using a Low-Medium-High (LMH) scale is common to many internal audit departments in reporting risk levels to executive management[2] ans IS-management. Therefore we focused our research question on this qualitative LMH-risk framework.

[2] As part of a study to Audit Management Systems in 2006 we discussed reporting-requirements with 30+ internal audit departments and suppliers of Audit Management Systems (TeamMate, AutoAudit, Galileo, PAWS, Auditor Assistant and others). We assessed that 3-level risk ratings in audit-reporting to executive management, are widely used amongst organisations and found that most audit departments also express probability and impact on a 3 level (LMH) qualitative scale. This was consistent with our own consulting experiences at several internal audit departments. At global level, we also found the 3-level LMH scale to be used across many organisations that shared their practices on conferences and on the internet, such as following quote from Canadian Government "Policy shows that the enterprise level reporting of risk will normally be done with a matrix that shows three levels of likelihood and three levels of impact", "The

Research Strategy

In choosing an appropriate research strategy (McGrath, 1981) we faced following dilemmas in balancing *precision of measurement*, *generality over actors* and *context realism* of our study. In order to serve the objective of this study: better understand IS-managers' shaping of perceived risk in practice, the study should apply to "realistic" circumstances and be close to their operational practice. We considered following the research strategy of a field study (not obtrusive) or field experiment (obtrusive) in which IS-managers would be observed in their operational practice. Especially an ethnographic study could be worth full in obtaining a holistic view on how IS-managers operate in practice. These fieldwork approaches would have provided maximum *context realism* and approached real-life complexity, but would have allowed less controlled (contrived) settings for studying the specific variables we were interested in from our research question.

We also considered applying a survey amongst a large number of IS-managers. This research strategy would have maximised *generality over actors,* however we assumed that both *precision of measurement* and *context realism* would be harmed too much when IS-managers would be asked to step aside and consider their own "biases" from a distance. This self-report would insufficiently uncover risk shaping biases "in action", which was key in our research objective.

We also considered following the research strategy of a laboratory experiment which would have maximised *precision of measurement* of our study. We considered a within-group and between-group (test-group and control-group) experimental setting with random assignment of treatments to respondents. This would have maximised controlled settings for measuring independent (treatment) and dependent variables (effect). It would have allowed assessing causal relations between treatment and effect. The downside however was that we would loose too much *context realism* to the IS-managers. Next to that, our research objective was to gain insight in the relative dominance of Probability and Impact information on Perceived Risk and not to assess a causal relationship (by means of falsification) between treatment (risk-information) and effect (risk-perception). A laboratory experiment was less suitable to answer for our research question.

We decided Experimental Simulation (McGrath, 1981) best served the purpose of this study, with created (contrived) settings in the form of cases, in which probability and impact information was given and perceived risk was measured from IS-managers of a large financial institution. In choosing this research strategy we balanced *precision of measurement* and *context realism* of our study. In this way we also assured that respondents are used to IS-auditors reporting to IS-management and executive management within a qualitative (LMH) risk framework in a complex IS-environment.
Throughout the next paragraphs we will explain the way we implemented the principles of this research strategy in the design and execution of this study and how we managed validity-issues.

Research Design and Execution

According to Libby (Libby, 1981) many variables play a role in processing of risk information. Within the design and execution of this study we had to take account of these variables, to prevent them from disturbing validity of this study. Therefore these variables (we preferred the term "attributes") are labelled in figure 1 that describes the conceptual constructs and relations that were analysed and the way they were made operational to manipulate and measure them in the empirical part of this study.

---

plotting of each risk according to these two attributes provides management with a risk rating (Red, Yellow, Green)".
Although we found the 3-level scales to be common, it should be mentioned that the levels are presented in various forms "low-medium-high", "green-yellow-red", "1-2-3" across formats of management reporting. We should also mention that a minor part of internal audit departments considered to improve granularity of probability and impact levels to a 5-level scale, while retaining to the LMH-scale for the resulting reported risk levels.

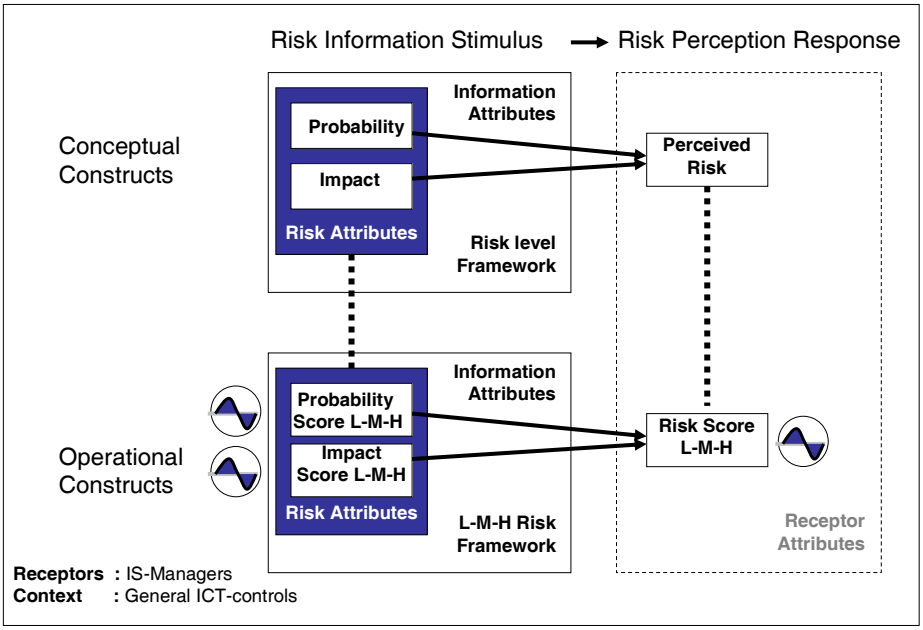

Figure 1: *Research Design*

Figure 1 shows first how we deal with the stimulus-response design for this study. We provide someone (the receptor) with information on risks (stimulus) and measure perceived risk (response). At a conceptual level we are interested in the effect of treating the *risk attributes* Probability and Impact (independent variables)[3]. This has been made operational through providing cases with a given level of Probability and Impact. We measure respondents' Perceived Risk on a Low-Medium-High scale. Below we consider *information attributes* (the way we present and provide information on risk-attributes) in their influence on respondent's perceived risk. We also consider *receptor attributes,* respondents' characteristics that might influence respondents' perceived risk levels as measured.

Treatment of Probability and Impact

The respondents were provided with a number of cases. These cases were prepared to make them familiar to IS-managers, since they cover subjects that are addressed in regular IS-Audits. These subjects (such as IS-backup's, IS-capacity planning, IS-helpdesk, IS-change management) will be recognized by IS-managers worldwide. They are basic elements in IS-management responsibilities and education according to standards as ITIL and with respect to IS-risks. CobiT[4]The cases reflect these so called "general" IS-controls thus making them not restricted to any particular Information System or organisation. So the cases not only apply to financial institutions but to all organisation where Information Systems are in place and provide any level of business value and risk.

[3] It should be noted that the independent variables are *information* on Probability and Impact provided to respondents. As a step in mental processing of this information to shape risk perception, the intermediate variables Perceived Probability and Perceived Impact can play a role. These intermediate variables are not measured in our study, since measuring (asking) them might have steered/disturbed the IS-managers' mental processing and might have influenced the results for our particular research question. In this choice we followed studies in other domains, such as (Keil, 2000)

[4]CobiT is a framework for IT-governance and covers the strategic planning of Information Systems, the acquisition and projects to implement new Information Systems and the processes to ensure proper operations of existing Information Systems.

Each case described a finding (internal control weakness) of a fictive IS-audit. The findings were presented to respondents in the following form:

Finding nr 7. Single Point of Failure in the Company Network

Probability = Low
Impact = High

Despite the redundancy of the company's star network infrastructure, there is still a single point of failure in the central location. If the network connection of this location is lost, none of the other locations can communicate with each other. The risk exists that productivity comes to a full standstill when problems arise in the central location.

Figure 2: *Example of presentation of findings*

Within these findings Probability and Impact information (*risk attributes*) was manipulated throughout the complete range Low-Medium-High. All respondents received 9 findings with both Probability and Impact given in random order. We pre-tested and mitigated inconsistencies between "given" probability and impact and the description through feedback from IS-professionals (IS Audit directors, teachers, IS-consultant)[5]. Those professionals involved in pre-testing were not invited as respondents within this study.

Providing respondents with a sequence of 9 findings (*information attribute*) may cause contamination or fatiguing effects in the responses measured. Although a sequence of findings inevitably causes statistical noise in the results, it didn't drive results on the relation between probability, impact and perceived risk into a certain direction (randomization). A time series performed on the sequence of findings showed no significant tendency (increase or decrease) in perceived risk. No structural correlation was found between couples of sequential findings[6].

Within the cases we manipulated "given" probability and impact as attributes of risk. Since the source or "sender" of this information might be relevant to receptor's response (*information attribute*), we provided the additional statement to the findings (cases) that probability and impact were assessed by an (independent) IS-Auditor. This "3rd party" information is used here to make stimulus information operational in a "neutral" way (there is no personal involvement that colours the information's reliability).[7]

Measurement of Perceived Risk

The conceptual construct *Perceived Risk* is defined as "a decision maker's assessment of the risk inherent in a situation" (Sitkin & Pablo, 1992). We asked the respondents to rate the perceived risk related to the individual findings. This ought not be confused with asking respondents for their

[5] In this way we took care on inconsistencies between the text phrases of the individual findings and the given "reported" levels of probability are impact. Nevertheless it cannot be ruled out completely that these texts are of influence on the measurements.

[6] Correlational study for contamination effects showed no significant correlation between subsequent findings, except for two couples. Finding 7 (high impact and low probability) and Finding 8 (medium impact and medium probability) show Pearson correlation of 0,364 with sig (2 tailed) of 0,04. We concluded no structural contamination effects were measured.

[7] A remaining *information attribute* about the source/sender in this study is the fact that respondents know this information is coming from the researchers given to them in a "created" setting. This validity threat might colour their responses compared to their daily operations, however is unavoidable in any research strategy with contrived and created settings (laboratory experiments, experimental simulations).

"worries" as notified by (Sjöberg, 2000c) that would have delivered measurements only poorly related to Perceived Risk (MacGregor, 1991), (Sjöberg, 1998d).

We asked respondents to express the Perceived Risk on the 3-level scale (Low-Medium-High). This way of measurement of Perceived Risk meets meets major requirements on response formats to measure risk perception (Sjöberg, 1994).

We realise that the presentation of Risk-attributes Probability and Impact and measurement of Perceived Risk within this 3-level Risk Framework (*information attribute)* causes "framing" effects on responses (Kahneman & Tversky, 1984) (Slovic, 2001) (Levin et al., 2002). Therefore we limit this study to the given (widely used) risk level framework and cannot claim any measured effects to occur in other frameworks in a similar way.

Respondents

In discussing our research-strategy, we already discussed that we decided to involve IS-managers from an international banking firm to participate in our study. We also discussed why we preferred them over alternatives for reasons of internal and external validity of our study. These IS-managers work on the bank's head-office in Amsterdam/London and perform their tasks globally from regional hubs in Amsterdam/London, Singapore, Sao Paolo and Chicago). They are relatively well educated and experienced (financial institutions are ahead of many other companies with implementing professional IS-Audit and IS-management staff and involve them in risk reporting).

The respondents were invited by email and joined the study on a voluntary basis. The questionnaire with findings was presented and collected electronically. Additional data from the 32 respondents was collected (*receptor attributes* in figure 1) gender, experience, education, function as described in the table below.

Respondents

IS Management experience			Gender		
< 3 years		0%	Male		89%
3-5 years		0%			
5-10 years		37%	Female		11%
10-15 years		26%			
> 15 years		37%			
Totals		100%			100%

***Figure 3**: Respondents' characteristics*

This confirms that the 32 respondents score relatively high on IS-management experience, so it will not be likely that empirical results of our study would be driven by a lack of knowledge or experience of our respondents in the area of IS-risks.

We also considered whether other respondent's characteristics (*receptor attributes)* could drive the measurements of Perceived Risk. As Sjöberg (Sjöberg, 2000b) puts it: "Perceived Risk is surely not merely a function of probability and harm but many other factors, such as attitudes". And as Keil (Keil et al., 2000) suggests: "if a person has a high risk-taking propensity, he/she might tend to underestimate the risks involved in a situation". Therefore we performed additional testing on Risk Propensity (a person's willingness to take risks). We measured respondents' Risk Propensity

according to (Nicholson et al., 2005) using a five point unidimensional Likert scale. As shown in the tables we found no significant correlation between the respondent's risk propensity and their perceived risk.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
RiskPerception	32	1,44	2,44	1,9097	,24835
RiskPropensity	32	1,17	4,67	2,4896	,66118
Valid N (listwise)	32				

Correlations

		Risk Perception	Risk Propensity
RiskPerception	Pearson Correlation	1	-,155
	Sig. (2-tailed)		,397
	N	32	32
RiskPropensity	Pearson Correlation	-,155	1
	Sig. (2-tailed)	,397	
	N	32	32

Figure 4: *Correlation between Risk Perception and Risk Propensity*

Based upon the definitions, treatments of independent variables and measurements of depend variables and other significant variables, we defined the circumstances for answering the research questions based upon the empirical results.

Empirical Results

We presented all 32 IS-managers with 9 findings (varying probability and impact over low, medium and high), thus resulting 288 observations.

Based upon these data we performed the following statistical analysis to answer the research questions.

1. Do Probability and Impact attributes of Risk contribute equally to the level of Perceived Risk, within given 3-level (L-M-H) Risk Framework?

To answer this question a t-test has been performed in which we tested whether Impact and Probability values can be exchanged without significant effect on Perceived Risk scores [8]. In other words, we tested the hypotheses whether Perceived Risk levels could be mirrored across Probability and Impact within the table below that presents the mean and Standard Deviation of Perceived Risk scores for all findings presented to the respondents.

[8] For the purpose of statistical analysis we translated the L-M-H values of independent variables (Probability and Impact) and the dependent variable (Perceived Risk) to a 1-2-3 numerical scale.

		Probability					
		Low (1)		**Medium (2)**		**High (3)**	
Impact	**Low (1)**	*Finding 5*		*Finding 4*		*Finding 2*	
		Mean:	**1,13**	Mean	**1,31**	Mean	**1,34**
		SD	0,42	SD	0,47	SD	0,55
	Medium (2)	*Finding* 9		*Finding 8*		*Finding 3*	
		Mean	**1,56**	Mean	**1,72**	Mean	**2,03**
		SD	0,72	SD	0,63	SD	0,60
	High (3)	*Finding 7*		*Finding 6*		*Finding 1*	
		Mean	**2,66**	Mean	**2,69**	Mean	**2,75**
		SD	0,55	SD	0,47	SD	0,57

Figure 5: *Perceived Risk scores per finding*

The table below shows the t-test results on paired observations[9] for finding 4 (low, medium) across finding 9 (medium, low), finding 2 (low, high) across finding 7 (high, low) and finding 3 (medium, high) across finding 6 (high, medium), as described in the tables below.

One-Sample Test

	Test Value = 0					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
q4minq9	-1,854	32	,073	-,24242	-,5088	,0240
q2minq7	-8,348	32	,000	-1,27273	-1,5833	-,9622
q3minq6	-4,924	32	,000	-,63636	-,8996	-,3731

Figure 6*: T-test on paired observations*

Testing whether Probability and Impact could be exchanged (mirrored) for all observations, delivered results as presented below.

[9] q4minq9 was calculated for each respondent (score on finding 4 minus score on finding 9) on a scale -2,-1,0,1,2 and was tested on mean = zero

One-Sample Test

	Test Value = 0					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
mirrored	-7,994	98	,000	-,71717	-,8952	-,5391

Figure 7: *T-test for all paired observations*

There fore we conclude that risk attributes Probability and Impact cannot be mirrored (exchanged) with having a zero-effect on Perceived Risk. With a (2-tailed) significance of 0,000 we reject the hypothesis that Probability and Impact would equally contribute to Perceived Risk.

2. What function best estimates the relation between Risk attributes Probability, Impact and the level of Perceived Risk within given risk framework?

We first analysed to what extend a linear relationship between the variables could explain the empirical results as found and what relative weight of Probability and Impact could be found. For Probability and Impact both given, the Linear Regression results in best estimated function[10] *Perceived Risk = 0,719 Impact + 0,130 Probability + 0,212*, with R-square = *0,529*.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,727[a]	,529	,526	,56572

a. Predictors: (Constant), Probability#, Impact#

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	,212	,120		1,762	,079
	Impact#	,719	,041	,716	17,605	,000
	Probability#	,130	,041	,130	3,189	,002

a. Dependent Variable: Risk#

Figure 8: *Results linear regression*

These results suggest that, when a linear relation would be considered, Impact variable weights almost 5 times the Probability variable.

Using the traditional risk function Risk = Probability x Impact as a basis for non-linear regression results in parameter estimations as described in the table for the equation: *risk# = b1 x impact x probability +b2*, with starting values 1 for b1 and b2.

[10] We are only interested in evaluation of major characteristics of the function that best explains the empirical results. We do not intend to assess Perceived Risk as a function of Probability and Impact for intrapolation or extrapolation purposes to predict Perceived Risk in between or outside the levels L-M-H.

These results suggest, that when Perceived Risk would follow the traditional formula Risk=Probability x Impact, only 32,2% of the variance in the measured Perceived Risk would be explained.

Parameter Estimates

Parameter	Estimate	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
b1	,194	,017	,161	,226
b2	1,136	,078	,983	1,288

ANOVA[a]

Source	Sum of Squares	df	Mean Squares
Regression	1112,657	2	556,329
Residual	131,343	286	,459
Uncorrected Total	1244,000	288	
Corrected Total	193,653	287	

Dependent variable: Risk#

a. R squared = 1 - (Residual Sum of Squares) / (Corrected Sum of Squares) = ,322.

Figure 9: *Results non-linear regression*

Open Questions

After they had finalised the electronic cases, we asked respondents in open questions for difficulties they had encountered in assessing the risk level of the cases, criteria they use in assessing risk levels. We also invited them to provide us with other remarks that could be relevant for interpreting their answers. The tables provide an overview of the answers we obtained from the 32 respondents.

An interesting observation is that the Impact related criteria (generic, regulatory, business continuity, reputation, financial, client satisfaction) are mentioned 77 times compared to 16 times Probability related criteria were mentioned. *Other criteria* were not directly related to the probability or impact elements of risk information but were mentioned 32 times to be relevant to the level of risk the IS-managers perceive. We found these criteria are mainly related to management control and decision making on IS-risks (can I manage the situation, take action if needed, have I dealt with it before, what does it mean for the priorities and cost-effectiveness of my IS-department, does it provide opportunities). Given their role of IS-manager, it is not surprising that these management control elements play a role in the respondents' perception of reported IS-risks.

The answers on the open questions support the empirical results that impact information would be more salient than probability information on IS-risks.

Difficulties in assessing risk level of cases	**Instances**
Type of business unknown and therefore exact business impact is unknown as well as possible regulatory impact	5
Lack of detailed circumstances	3

Criteria IS-managers say to use in assessing risk levels	**Instances**
Probability	16
Impact related criteria	
Type of system / Nature of business	15
Impact	14
Impact on continuity of service	14
Reputational Impact	11
Financial Impact	10
Legal and compliance impact	5
Client satisfaction exposure	4
Time characteristics of risk (direct/duration)	4
Other criteria	
Experience with similar risks	11
Mitigating controls/solutions	9
Value at risk/ cost-effectiveness	6
Risk is known and accepted	2
Opportunity for improvements	2
Management priorities	2

Figure 10: *Remarks from Open Questions*

Conclusions and Considerations

Within this study we assessed that IS-managers' risk-perception on general IS-controls is dominated by Impact information over Probability information for a selected group of IS-managers. The IS-managers that participated in this study, work for a global banking firm and are involved in reporting IS-risks to the bank's executive management as part of the corporate governance framework. They are also used to working with IS-auditors who report IS-risks within a LMH qualitative risk framework.

This result is consistent with Keil (Keil et al., 2000) who concluded that impact is more salient than probability in shaping risk perception within the domain of IS-projects. We complement to that study since we found similar results within the domain of general IS-controls with respondents (IS-managers) that report to executive management as part of corporate governance framework. With Keil we also share the conclusion that no significant correlation was found between respondent's risk propensity and perceived risk, although we measured risk propensity differently.[11].

[11] Keil measured Risk Propensity with a Choice Dilemma Questionnaire according to Wallach, where respondents are invited to rate the probability of failure they still find acceptable for preferring a risky option over a safe alternative. Based upon Keil's conclusions we decided not to use the CDQ for our study. We suspected the CDQ measurement might cause an error in assessing whether a correlation could be found between Risk Propensity and Perceived Risk. The reason for this was that Risk Propensity was measured amongst the Probability factor and Perceived Risk was found less sensitive for the probability factor. This measurement could have hidden a correlation between Risk Propensity and Perceived Risk that might have existed. Although we measured Risk propensity differently, we did not find a significant correlation between Risk Propensity and Risk Perception either.

The study also reveals that these IS-managers' Perceived Risk is better explained by a linear relationship with Probability and Impact (53%), than a non-linear relationship based upon the traditional risk formula (risk = probability x impact) which explains 32% of risk perception variance. This suggests Probability information and Impact information contribute independently to IS-managers' perceived risk and could point at human inability of perfectly "connecting" attributes probability and impact of risk-information within our mental information processing.

These results, given the limitations and assumptions of our study, give rise to some considerations from both a theoretical and a practical perspective. First it is interesting to consider why some studies show Probability and other studies show Impact as the most risk-shaping factor and especially why Impact turned out to be most salient within the domain, respondents and set-up of our study.

Although our study shows results that are consistent with Keils study on IS-projects (Keil et al., 2000), the results seem to be inconsistent with Forlani's (Forlani, 2002) experiment of manager's new-business high-risk decision making and especially the effect of perceived control in risk-taking behaviour across domains. Within that experiment he tests and concludes that the probability element of risk is dominant in managers' risk taking behaviour within a domain where managers perceive a high level of outcome control and the impact element of risk is dominant when managers perceive a low level of outcome control. We did not measure the level of perceived outcome control IS-managers associated with the risk-information we provided in the cases within our study. However, the suggestion that perceived control could be a relevant intermediate variable in shaping the perception of IS-risks is consistent with a recent study in the domain of IS-projects specifically (Stephen Du et al., 2007). We could expect that people who are not sitting in the driver-seat perceive control lower than the people who are in the driver seat and holding the steering-wheel, as literally found in a car-driving behaviour study (Horswill & McKenna, 1999). IS management is in charge to make decisions and take actions to mitigate, reduce or accept IS-risks. The open questions uncovered that criteria as *experience with the risk, mitigating controls/alternatives, setting priorities, opportunity for improvements, cost-effectiveness* play a role in the risk perception of the IS-managers that were involved in our study .These criteria could easily be associated with the IS-managers sitting the driver seat in making decisions, considerations and take actions as part of management responsibility. Forlani's study suggests that IS managers' risk perception should merely be driven by the Probability-factor, when Perceived Outcome control is high. Further analysing the assumptions of Forlani's study and our study may provide additional insight in explaining our results.

Forlani's experiment was focused on managers' risk taking behaviour in high-risk product developments. Within Forlani's study, Perceived Control was manipulated across low and high levels and the consequences of a manager's decision (successful or not successful introduction of a new product) are clearly expressed in winning and losing (thus covering both the GAIN and LOSS domain according to Prospect Theory (Kahneman & Tversky, 1979). In our study we measured risk-perception but we did not focus on the IS-managers' decision or action to accept or mitigate the risk. Furthermore the IS-risks in our domain of study (deficiencies in general IS-controls) focus on the LOSS-domain and hardly refer to risk-perception in the GAIN-domain. The following explanations could be found for our results compared to Forlani's:

- Forlani's experiment measures risk taking behaviour of managers. If we assume IS-general controls to be a domain where experienced IS-managers perceive a high level of control over outcomes, then dominance of probability in managers' risk taking behaviour would be expected. This not necessarily contradicts dominance of impact in managers' perceived risk (as we measured). In other words: the IS-managers of our study not necessarily take decisions and actions on reducing/mitigating IS-risks on the axis of impact. Despite dominance of impact in their risk perception they may prefer taking probability-reducing actions over impact-reducing actions;
- Forlani mentions that Perceived Control not always plays a significant role in risk perception and in determining the relative dominance of probability or impact. For example, when all alternatives in a decisionmaker's consideration have a low probability of loss, then magnitude of risk becomes the dominant element of risk. In that case (March

& Shapira, 1987) there is hardly any leverage of perceived control in the risk shaping function. Perceived control in that domain of low-probabilities is low and irrelevant for risk taking decisions. In other words: the IS-managers would perceive a very low level of output control when a decision/action would reduce probability of loss from 0,0001% to 0,00001% (10 times) and risk taking would then be dominated by impact of loss. In a domain where a decision/action would reduce probability of loss from 50% to 5% (10 times) managers' perceived outcome control would be much higher (decision really makes a difference) and probability would be dominant in risk taking decisions. The results of our study could point at the IS-managers considering the domain of general IS-controls to be associated with (very) low probability of loss compared to other risks (losses and gains) they deal with. According to Forlani's model, this would imply that impact of loss would be dominant in IS-managers' risk taking behaviour on general IS-controls. It is interesting that these domain characteristics, according to Forlani's model, would also imply that IS-managers would tend to risk-seeking behaviour in the domain of general IS-controls and tend not to take decisions, actions or investments to decrease a risk that they already consider to be (very) low compared to other risks.

With our study we made a first step in understanding risk-perception of IS-management when IS-auditors provide them with information on IS-risks in the domain of general IS-controls. The results, limitations and assumptions of our study also raised several questions and options for further research, such as:

- Similar studies (IS-managers' perceived risk in the IS-domain of general IS-controls) with different choices in research strategy (f.e. ethnographic study), research design, measurement scales (f.e. 5-level scale for probability and impact information combined with LMH-scale for perceived risk could be considered). . This would be fruitful in order to improve validity on the relation between Risk Information and Perceived Risk;
- Similar studies on perception of IS-risks outside the domain of general IS-controls. This could give insight in IS-managers' risk perception and decision making related to strategic advantages, acquisition of ERP-systems, IS-outsourcing, where impact (not only losses but also gains), probabilities and perceived outcome control may differ from the domain of general IS-controls. This could, for example, help in better understanding IS-management biases in setting priorities and allocating resources to reported IS-audit findings on general IS-controls compared to other options;
- Similar studies with other respondents. Next to IS-managers and IS-auditors (from this or other organisations) it could be interesting to study executive management's biases on IS-risks reported by IS-auditors. We hope that insight in risk perception and decision making biases on IS-risks amongst these actors, will help to improve communication and decision making on IS-risks.

References

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

Bonner, S. E. (1999). Judgment and Decision-making Research in Accounting. — Accounting Horizons, Vol 13, No 4, pp 385-398.

D'Silva, K. & Ridley, J. (2007). Internal Auditing's international contribution to governance. — International Journal of Business Governance and Ethics, Vol 3, No 2, p 113.

Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. L. & Keeney, R. L. (1981). Acceptable Risk. — Cambridge University Press, Cambridge.

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.

Frielink, A. B. (1961). Auditing Automatic Data Processing. — Elsevier.

Gramling, A. A. & Hermanson, D. R. (2006). What Role is your Internal Audit Function playing in Corporate Governance. — Internal Auditing, Vol 21, No 6, pp 37-40.

Greening, L. (1997). Risk Perception following exposure to a job-related electrocution accident: The mediating role of perceived control. — Acta Psychologica, Vol 95, pp 267-277.

Gregory, R., Slovic, P. & Flynn, J. (1996). Risk perceptions, stigma, and health policy. — Health & Place, Vol 2, No 4, pp 213-220.

Hadden, L. B., Todd-DeZoort, F. & Hermanson, D. R. (2003). IT Risk Oversight: The roles of Audit Committees, internal auditors and external auditors. — Internal Auditing, Vol 18, No 6, p 28.

Helliar, C., Lonie, A. A., Power, D. M. & Sinclair, C. D. (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.

Hersey, J. C. & Schoemaker, P. J. H. (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.

Horswill, M. S. & McKenna, F. P. (1999). The Effect of Perceived Control on Risk Taking. — Journal of Applied Social Psychology, Vol 29, No 2, pp 377-391.

Hunter, D. R. (2002). Risk Perception and Risk Tolerance in Aircraft pilots;. — In. US Department of Transportation-Federal Aviation Administration, Washington.

Kahneman, D. & Tversky, A. (1979). Prospect Theory: An analysis of decion under risk. — Econometrica, vol 47, pp 263-291.

Kahneman, D. & Tversky, A. (1984). Choices, values and frames. — American Psychologist, Vol 39, pp 341-350.

Keil, M., Wallace, L., Turk, D., Dixon-Randall, G. & Nulden, U. (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 & Finance, Vol 17, No 5, p 21.

Kirkley, J. (2007). Why the CFO should talk to the CIO. — Financial Executive Vol 23, No 2, pp 20-22.

Kunreuther, H. & Pauly, M. (2004). Neglecting Disaster: Why Don't People Insure Against Large Losses? — The Journal of Risk and Uncertainty, Vol 28, No 1, pp 5-21.

Levin, I. P., Gaeth, G. J., Schreiber, J. & Lauriola, M. (2002). A new look at framing effects: Distribution of effect sizes, individual differences, and independence of types of effects. — Organisational Behavior and Human Decision Processes, Vol 88, pp 411-429.

Libby, R. (1981). Accounting and Human Information Processing: Theory and Applications. — NJ: Prentice-Hall, Englewood Cliffs.

Lochner, L. (2007). Individual Perceptions of the Criminal Justice System. — The American Economic Review, Vol 97, No 1, p 8.

MacGregor, D. (1991). Worry of technical activities and life concerns. — Risk Analysis, Vol 11, pp 315-324.

March, J. G. & Shapira, Z. (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 49-54.

McGrath, J. E. (1981). Dillematics- The study of Research Choices and Dilemmas. — American Behavioral Scientist, Vol 25, No 2, pp 179-210.

Nicholson, N., Soane, E., Fenton-O'Creevy, M. & Willman, P. (2005). Personality and domain-specific risk taking. — Journal of Risk Research, Vol 8, No 2, pp 157-176.

Nuijten, A., Zwiers, B. Pijl van der, G. (2007), The effect of Risk Information on IS-auditors' Perceived Risk, 1st European Risk Conference, Muenster-Germany, Sept 5-7.

Nwogugu, M. (2006). A Further Critique Of Cumulative-Prospect-Theory and Related Approaches. — Applied Mathematics & Computation.

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

Ranney, T. (1994). Models of driving behaviour: A review of their evolution. — Accident analysis and prevention, Vol 26, No 6, pp 733-750.

Schwartz, S. & Griffin, T. (1986). Medical Thinking: The psychology of medical judgment and decision making. — Springer-Verlag, London.

Shanteau, J. (1992). Decision Making Under Risk: Applications to Insurance Purchasing. — In: Advances in consumer research (J. F. Sherry & B. Sternthal, eds). Association for Consumer Research, Chicago.

Sitkin, S. B. & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. — Academy of Management Review, Vol 17, No 1, pp 9-38.

Sjöberg, L. (1994). Perceived Risk vs Demand for Risk Reduction. — In. Centre for Risk Research, Stockholm School of Economics, Stockholm.

Sjöberg, L (1998d). Worry and risk perception. — Risk Analysis, Vol 18, pp 85-93.

Sjöberg, L (2000b). Factors in risk perception. — Risk Analysis, Vol 20, pp 1-11.

Sjöberg, L (2000c). The methodology of Risk Perception Research. — Quality and Quantity, Vol 34, pp 407-418.

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

Stephen Du, Keil, M, Mathiassen, L., Shen, Y. & Tiwana, A. (2007). Attention-shaping tools, expertise, and perceived control in IT project risk assessment. — Decision Support Systems, Vol 43, pp 269-283.

Steuperaert, D. (2004). IT Governance global status report. — Information Systems Control Journal 5, 24.

Tversky, A. & Kahneman, D. (1982). The Framing of Decisions and the Psychology of Choice. — In: Question Framing and Response Consistency (R. M. Hogarth, ed). Jossey-Bass Inc. Publishers, San Francisco.

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