PERCEPTIONS OF INFORMATION TECHNOLOGY RISK: A DELPHI STUDY

James L. Worrell
Florida State University
College of Business
Tallahassee, FL 32306-1110
jworrell@fsu.edu

Ashley A. Bush
Florida State University
College of Business
Tallahassee, FL 32306-1110
abush@fsu.edu

Abstract

Reliance on IT has complicated risk management efforts by introducing IT risk, defined as the risk that an organization's information systems will not adequately support achieving business objectives, sufficiently safeguard information resources, or deliver accurate and complete information to users. There are multiple stakeholders involved in the effort to manage IT risk, however it is not clear how these different stakeholder groups perceive this risk. We conducted a Delphi study consisting of three expert panels from "Big 4" public accounting firms and Fortune 1000 companies to investigate perceptual differences among three key stakeholder groups: IT audit and security experts, business users of IT, and IT professionals. Our results suggest that these stakeholder groups not only lack consensus on important IT-related risk factors within their groups but also across groups. This research highlights the importance of accounting for multiple perspectives in risk management activities.

Keywords
Information technology risk, risk, Delphi method, perceptions

Introduction

As organizations navigate the uncertain waters of the market and their environment, one necessary task stakeholders must undertake is risk identification. The infusion of information technology (IT) into business processes has increased both the complexity and the necessity of this task by introducing a new dimension of business risk, IT risk. We define IT risk as the risk that an organization's information systems will not adequately support the organization in achieving its business objectives, sufficiently safeguard its information resources, or deliver accurate and complete information to its users.

Identifying IT risk within business processes is a necessary first step in any comprehensive risk management strategy. By identifying technology-related risks that threaten achieving business objectives, organizations are better equipped to determine what actions, if any, to take to reduce these risks to an acceptable level. Since IT is embedded in the business processes used to execute business strategy and meet business objectives, it follows that any risk which impairs achieving these objectives warrants attention.

Identification of IT risk, however, is not easy. Since IT risk impacts both technology and underlying business processes, they must be considered in concert. In the current, post-Enron business environment, this task has taken on greater significance. As a result of the Sarbanes Oxley Act of 2002, all publicly traded companies are required to assess their internal control structure, much of which relies on IT. In evaluating the impact of IT risk on technology and business processes, both business professionals (those who use the information systems to execute business processes and achieve business objectives) and IT professionals (those who develop and support information systems) must share in a common vision of what technology-related risks actually threaten the organization's success. Additionally, internal and external auditors often contribute to this debate. In other words, organizational stakeholders and decision makers must agree on those IT risk factors that threaten achievement of business objectives and execution of business strategies. Complicating this task is both anecdotal evidence and empirical research that suggests disconnects between IT professionals and business professionals with regards to decision making, sense making and risk identification (Li 1997; Keil et al. 2002).

To address this gap in our understanding, we conducted a Delphi study to answer the following research question: *How do different stakeholder groups within organizations conceptualize IT risk?* First, we review prior research on risk in the information systems (IS) literature. Next, we explain the Delphi method used in this study and present our findings. Finally, we discuss potential explanations for our results, and conclude with implications for research and practice.

Information Technology Risk

The definition, composition and importance of technology-related risks in the IS literature is a long running debate, with limited resolution (Alter and Sherer 2004; Sherer and Alter 2004). This lack of resolution is not surprising, as researchers in the risk management literature have had difficulty objectively measuring technology risk and other associated operational risks (Crouhy et al. 2001).

To better understand how IS researchers conceptualize and operationalize risk, Sherer and Alter (Alter and Sherer 2004; Sherer and Alter 2004) authored a pair of articles that attempted to untangle nearly twenty years of research on IT risk. Based on their review of articles published in top-tier IS journals since 1986, they observed that prior research lacks a consistent conceptualization of IT risk, as well as an organizing framework that is readily applicable by organizational decision makers.

With the possible exception of IT project risk, which has been heavily researched (see Anderson and Narasimhan 1979; Zmud 1980; Schmidt, Lyytinen et al. 2001; Keil et al. 2002), one common complaint is that risk factors tend to be offered for management consideration without any organizing logic or framework (Sherer and Alter 2004). However, an equally important observation about prior research is that, with few exceptions, it often focuses on risk from the perception of a specific stakeholder, such as a project manager (Schmidt et al. 2001), business manager (Sherer and Alter 2004), IT executive (Dickson et al. 1984; Niederman and Brancheu 1991) or the nebulous "user."

Focusing on a single perspective can be problematic. Numerous researchers have demonstrated that different stakeholders have differing perspectives with respect to risk and expectations (Keil et al. 2002). Although understanding the discrete IT risk factors that impact the organization's decisions and control mechanisms is crucial, equally important is grasping the magnitude and salience of specific risk factors, and understanding how various stakeholders prioritize their efforts and resources to mitigate these threats. Our efforts are aimed at broadening our knowledge of IT risk in operations by identifying those risk factors that organizational stakeholders view as most critical to success in meeting current business objectives, securing information resources, and providing timely and accurate information to decision makers.

Method and Data Collection

In line with past studies whose focus was to determine perceptions among various stakeholder groups, we employed a seeded Delphi study to ascertain similarities and differences in perceptions of IT risk factors among three groups: IT audit and security professionals, business users of IT resources, and IT managers responsible for the operations and maintenance of information systems. The Delphi method is comprised of a series of structured, iterative groups decision processes with the aim of reaching consensus among a panel of experts on a given decision task or issue (Keil et al. 2002).

While some Delphi studies in prior IS research utilized the expert panel to first identify a list of factors or issues (Dickson et al. 1984; Schmidt et al. 2001), we provided our panelists with a preliminary list of IT risk factors, or "seed," from which our three expert panels could begin their efforts. We utilized Sherer and Alter's (2004) comprehensive list of IT risk factors as a basis for our list for two main reasons. First, their list was compiled based on articles published in leading IS research outlets that focused on risk. Second and perhaps more importantly, Sherer and Alter differentiated between risks associated with implementing new technologies (i.e., project risk) and risks associated with operations. As we were primarily concerned with IT risk factors associated with "IT in operations," we focused on those IT-related risk factors that threaten an organization's information systems once they have been implemented and are available for use.

After initially identifying 27 risk factors specific to IT in operations, we developed definitions for these based on the underlying research article from which the risk factor was first derived. To assess face validity, we pilot tested these definitions by providing a list of the risk factors and a separate list of definitions to three people with expertise in the area of IT-related risk. They were asked to match the risk factors with definitions and to provide feedback on both the wording of the risk factors and associated definitions. Based on this feedback, several risk factors were either dropped completely or combined with others, and definitions were refined, resulting in the final list of 22 IT risk factors submitted to the Delphi expert panels for evaluation (see Table 3).

In Phase One, three panels were created with panelists selected based on their expertise and years of experience in both industry and their respective organizations (see Tables 1 and 2 for demographics). Panel sizes were chosen to be sufficiently large and diverse to provide a variety of perspectives, and yet sufficiently small to manage information and provide timely feedback. The IT Audit/Security panel was initially comprised of 19 experts, all of whom currently work for or were previously employed by "Big 4" public accounting firms in their respective IT assurance and risk management practices. All experts on this panel held at least one professional certification (CPA, CIA, CISA, or CISSP) and ranged from senior associate to partner. Two panelists were dropped after the first phase due to non-response. The Business Professionals panel was initially comprised of 18 professionals, with eight being employed as managers in Fortune 1000 companies, and all but three working for large, publicly traded companies. The experts on this panel represented a variety of business units within their respective organizations, including marketing, risk management and planning, financial reporting, operations, and human resources. Three of the initial panelists were dropped after the first phase due to non-response. The IT Professionals panel was initially composed of 14 professionals, ten of whom were employed by Fortune 1000 companies. Experts were drawn from a wide range of IT disciplines, including network engineering, disaster recovery, enterprise technical architecture, IT product management and application development. Two panelists were dropped after the initial phase due to non-response.

Table 1. Individual Demographics

	IT Audit/Security (n=17)	Business Professional (n=15)	IT Professional (n=12)
Educational Level			
Associate	-	-	25%
Bachelors	47%	53%	67%
Masters	53%	47%	8%
Years in Field			
Mean	7.94	15.33	17.13
St. Dev.	2.79	8.16	8.16
Tenure in Organization			
Mean	4.21	3.97	6.75
St. Dev.	2.26	3.10	5.94

After assembling the three expert panels, each panelist was emailed a link to a web-based survey instrument containing a randomized list of the 22 IT risk factors and was asked to identify the ten IT risk factors they viewed as most important, based on the definition of IT risk as *the risk that an organization's information systems will not adequately support the organization in achieving its business objectives, sufficiently safeguard its information resources, or deliver accurate and complete information to its users.* Panelists were asked to identify any additional IT risk factors not included in the initial seeded list. While several offered additional risk factors, these were determined to either overlap with existing factors or were more closely associated with project risk factors, which were outside the current study's scope.

Table 2. Organizational Demographics

	IT Audit/Security (n=17)	Business Professional (n=15)	IT Professional (n=12)
Ownership model			
Publicly Traded	12%	80%	83%
Privately Held	82%	7%	8%
Government	-	7%	-
Not for Profit	6%	7%	8%
Industry			
Financial Services	6%	53%	75%
Manufacturing	-	20%	-
Professional Services	88%	7%	8%
Healthcare	6%	7%	8%
Information Services	-	7%	8%
Transportation	-	7%	-
Number of Employees			
Less than 5,000	6%	33%	8%
5,000 - 9,999	6%	60%	75%
10,000 - 99,999	6%	7%	17%
More than 100,000	82%	-	-
2004 Annual Revenues			
Less than $1 billion	6%	13%	8%
$1 billion - $4.9 billion	6%	47%	67%
$5 billion - $9.9 billion	6%	13%	-
More than $10 billion	82%	27%	17%
2004 IT Expenditures			
Less than $50 million	12%	53%	17%
$50 million - $99.9 million	-	40%	67%
More than $100 million	88%	-	-

Table 3. IT Risk Factors, Rankings and Associated Definitions

Risk Item		IT AS	B	IT	Definition
R8	**Lack of organizational alignment between business and IT**	1	6	2	Failure to align the IT infrastructure and applications with business needs
R20	**Unauthorized information access**	2		3	Firm's information or information systems are not adequately secured against unauthorized logical access
R3	**Information quality**	3	1		Failure in management decision-making resulting from irrelevant, incorrect, or insufficient information provided by the information system
R6	**Interdependencies between systems**	4	4	1	The need for systems to share data with other applications or systems, either internal or external to the organization
R22	**Weak change management**	5	8		Weak policies and procedures governing changes to applications or technical infrastructure and other information system components
R7	**Lack of IS participation in business initiatives**	6		7	Failure to aggressively leverage or engage IT enablers in business initiatives
R17	**Resource insufficiency**	7	7		Insufficient resources are available to carry out or execute an IS initiative or plan, such as insufficient personnel or budgeting
R19	**Technical complexity**	8	9	9	Information system or application is comprised of multiple components that combine to yield a complex system
R15	**Problematic interfaces between systems**		2	4	Information and data exchanges between systems do not occur completely, accurately, or in a timely manner
R1	**Difficulty integrating software from vendors and subcontractors**		5	5	Integration of packages from multiple vendors hampered by incompatibility and lack of cooperation
R11	**Malicious software**			6	Software written to produce an undesirable effect to the system, user, or organization
R18	**Software errors / bugs**		3	8	Programming problems typically resulting from oversights of programmers and/or analysts
R21	**Unauthorized physical access to hardware and processing environment**			10	Weak, ineffective, or inadequate physical control over access to the processing environment

Phase Two involved presenting each panel with a reduced list of risk factors so they could be ranked in terms of importance. This reduced list (see Table 3 for the reduced list by panel) was determined by carrying forward any risk factor from the previous phase that received a simple majority (50% or more selections within the specific panel) (Schmidt 1997) and ordered based on the percentage of their panel that selected the risk factor as one of their Top Ten (Keil et al. 2002). Panelists were asked to rank these risk factors from most important to least important based on their expert judgment. Additionally, they were asked to provide a short justification for selecting their top-ranked risk factor.

At the end of this round, the mean ranks for each risk factor were calculated, as well as Kendall's Coefficient of Concordance (W) to determine the degree of consensus among each expert panel (Schmidt 1997). Subsequent rounds presented the panelists with the risk factors ordered by their mean ranks, and feedback indicating the degree of consensus among their panel relative to the risk factor rankings.

Results

Phase Two results for each panel are summarized in Table 3. Seventeen members of the IT Audit/Security panel responded to the study, resulting in sixteen usable responses. Of the eight IT risk factors identified by this panel, four are strategy-related (*R8-Lack of organizational alignment between business and IT, R7-Lack of IS participation in business initiatives, R3-Information quality, R17-Resource sufficiency*), two are technical-related (*R6-Interdependencies between systems, R19-Technical complexity*), and the remaining two are security-related (*R20-Unauthorized information access*) and process-related (*R22-Weak change management*). Kendall's W for this phase was 0.301, which indicates weak agreement in the rankings among the panelists (Schmidt 1997). Based on this assessment, we conducted follow-up rounds to improve the degree of consensus among this panel. Subsequent rounds resulted in Kendall's W of 0.371 and 0.393, after which the Delphi was discontinued for this panel. Based on feedback from some of the panelists, we determined that we had reached a plateau in terms of consensus and that further rounds would not result in a greater degree of consensus.

Fourteen Business Professionals responded to the study, with all usable for analysis. Of the nine IT risk factors identified by this panel, three are strategy-related (*R8-Lack of organizational alignment between business and IT, R3-Information quality, R17-Resource sufficiency*), five are technical-related (*R6-Interdependencies between systems, R19-Technical complexity , R15-Problematic interfaces between systems, R18-Software errors/bugs, R1-Difficulty integrating software from vendors and subcontractors*), and the remaining are process-related (*R22-Weak change management*). Kendall's W for this phase was 0.301, which indicates a low degree of consensus among the panel. Based on this result, a subsequent round was conducted, resulting in a significant drop-off in agreement (Kendall's W = 0.226). In accordance with Schmidt's (1997) guidance, we deemed we had reached a plateau of consensus in the initial round.

Eleven IT Professionals responded to the study, with all usable for analysis. Of the ten IT risk factors identified by this panel, two are strategy-related (*R8-Lack of organizational alignment between business and IT, R7-Lack of IS participation in business initiatives*), five are technical-related (*R6-Interdependencies between systems, R15-Problematic interfaces between systems, R18-Software errors/bugs, R19-Technical complexity, R1-Difficulty integrating software from vendors and subcontractors*), and the remaining three are security-related (*R20-Unauthorized information access, R11-Malicious software, R21-Unauthorized physical access to hardware and processing environment*). Kendall's W for this phase was 0.369, prompting us to conduct a subsequent round in an effort to achieve a greater degree of consensus among the panel. However, as with the Business Professionals panel, the subsequent round resulted in significantly lower agreement among the panelists (Kendall's W = 0.224), and we determined that subsequent rounds would be counterproductive.

Discussion

Our results suggest two items that warrant discussion. The first is points of agreement between the three panels, i.e., what risk factors did all three panels identify among their "most important". The second, and perhaps more interesting, is to address the question of why two of the three expert panels could not reach an acceptable level of consensus.

Of the thirteen IT risk factors identified across the three panels in Phase Two, only three factors were identified by all three panels as "most important": *lack of organizational alignment between business and IT (R8), interdependencies between systems (R6), and technical complexity (R19)*. Not surprisingly, all groups ranked *lack of organizational alignment between business and IT (R8)* relatively high, first for the IT Audit/Security panel, fourth for the Business Professionals panel, and second for the IT Professionals panel. This relatively high ranking across the three panels likely is a result of both attention that strategic alignment between IT and business has received in the academic and practitioner literature, as well as past failures in aligning IT initiatives with business needs. As a Director of Human Resources at a large government agency noted:

> Not having IT "at the table" as management decisions are made leads to misalignment of business needs and IT. On the front end, this results in IT not being able to provide the advice and support needed to make a decision or select a product. In production, this greatly limits IT's ability to create or procure the needed programs and/or supply the necessary data in an efficient, effective way.

This sentiment was echoed by the Vice President-Enterprise Architecture at a Fortune 1000 company:

> Alignment of IT investment and business priorities must exist for optimum use of IT. We must avoid irrelevant investments, and focus on that which is most important to the success strategy for the business. Without formal traceability of strategies, tactics and priorities, we cannot be assured of good alignment, and most likely will have wasted effort and lost opportunity.

The last two risk factors, *interdependence between systems (R6)* and *technical complexity (R19)*, are indicative of the overarching risks associated with complex systems in today's business environment. While there was a lack of consensus on the relative importance of *interdependence between systems* (sixth for the IT Audit/Security panel, second for the Business Professionals panel, and first for the IT Professionals panel), all three panels ranked *technical complexity (R19)* in the bottom third of their listing.

Overall, these two risk factors reflect the experts' concerns that system complexity, both in terms of underlying technology as well as data integration, might compromise their organization's ability to extract relevant information or maintain these systems long-term. As an application developer at a large insurance company noted:

> Complex cross-platform systems … have to efficiently and accurately produce the desired results. In particular, it is often difficult to find the human resources with knowledge across the systems to implement/maintain these…

This sentiment was echoed by the Manager of Cost Accounting for a multinational beverage bottler:

> In our particular case, we have numerous systems cobbled together and resembling something like Frankenstein's monster. Because much of the data flow is one-way, and shortcuts have been taken in some of the interfaces, error recovery can be excruciating, as it was for us just this month.

Although it is enlightening to investigate where the three panels agreed, perhaps the most interesting question suggested by the results is why the Business Professionals and IT Professionals panels were not able to reach a meaningful consensus on their ranking, while the IT Audit/Security panel was. One potential explanation is biases in individual decision making, while heterogeneity within the Business Professionals and IT Professionals panels might provide additional insight.

Research suggests that, faced with a decision or risk proposition, managers and executives gravitate towards issues that are salient to their respective departments, often to the exclusion of other issues (Dearborn and Simon 1958). In addition to this bias based on selective perception, others propose that individuals employ heuristics to aid decision making (Tversky and Kahneman 1974), and that while these heuristics are credited with simplifying the decision making process, the biases inherent in these heuristics are fairly robust and lead to suboptimal decision making (Tversky and Kahneman 1974; Tversky and Kahneman 1981; Northcraft and Neale 1987). Selective perception and the availability heuristic, in which decision makers assess the probability of an event occurring based on their ability to recall a similar event from prior experiences, may be especially informative as to why two panels were unable to achieve consensus.

Over the course of the study, several panelists shared comments that support this explanation. For example, after the second round in Phase Two, the Senior Vice President-Marketing of a Fortune 1000 financial services firm commented:

> I'm sorry to be dim-witted, but I don't understand the point of trying to reach consensus for your study. I don't remember precisely how I voted the first time, but I wouldn't change my opinion based on what other people wrote in a survey response.

In a phone conversation with this executive, he further commented that his views were shaped more by issues encountered in his organization, and that the experiences of other panel experts weighed less heavily on him than did issues currently at hand. Similarly, an IT manager at a global professional services firm noted that he was "sticking to his guns on his initial rankings from the prior round" and was not "moved" by the experiences and feedback provided by other panelists. As with the marketing executive, this IT manager was more heavily influenced by issues closer to home than by those faced in other organizations. Finally, recall the Manager of Cost Accounting for a multinational beverage bottler who likened his organization's systems to "Frankenstein's monster" and noted that issues "just this month" drove home how important interdependencies between systems was to him and his organization. For this manager, his "most important" risk factor remained constant throughout rounds, regardless of peer feedback.

Taken collectively, these recollections and comments lend support to the notion that, in many instances, experts (such as our Business Professionals and IT Professionals panelists) who work day in and day out in the same organization (i.e., not consultants) tend to focus on issues that their particular organization faces. Many times, these individuals were either unwilling or unable to see past issues they grappled with on a daily basis to understand and attend to other risk factors. The members of the Business Professionals and IT Professionals panels were employed in the same organization for many years (Table 1), and it is reasonable to expect that their perceptions were shaped by their experiences and the culture within their respective organizations.

A second possible explanation for why the Business Professionals and IT Professionals panels were unable to reach consensus might be the heterogeneity of each panel. While many research efforts view stakeholders as either "IT resources" or "users," we intentionally constructed our Business Professionals and IT Professionals panels in such a way as to obtain a "cross-section" of the IT and business user community. For example, our Business Professionals panel was comprised of managers from business controllership, finance and accounting, strategic planning, sales and marketing, and human resources. By constructing our panel this way, we felt our panel would be able to bring a "real world" view to bear on the Delphi task, which in all likelihood resulted in our panel introducing "real world" conflict in terms of conflicting business goals and information needs.

Similarly, our IT Professionals panel was represented by resources employed in network engineering, network administration, business continuity and disaster recovery, enterprise change management, enterprise technical architecture, technology product management, and other functions within large IT departments. As with the Business Professionals panel, conflicting goals and experiences of those experts employed in different areas within their IT department likely resulted in firm stances on risk factor rankings.

While the Business Professionals and IT Professionals panels were unable to reach an acceptable level of consensus, the same was not true of the IT Audit/Security panel, which increased its degree of consensus in each subsequent round, and ultimately bordered on a moderate degree of consensus. The most obvious explanation for this is the group's relative homogeneity. Based on these experts' qualifications, educational background, and training regimen, there was significantly less variance within this panel than the others. For example, all experts possessed at least one audit or security-related professional certification, requiring understanding a specific common body of knowledge. All had received initial multi-week IT audit training upon joining their respective firms. Lastly, as all were either currently employed in "Big 4" public accounting firms or were "Big 4" alumni working as internal auditors in publicly traded firms, all possessed a working knowledge of the Sarbanes Oxley Act of 2002 and its focus on IT and internal controls, and all were required to comply with continuing professional education requirements to maintain their professional certifications. Taken collectively, these common experiences and requirements create a mindset that is more similar across this expert panel than the others.

Perhaps a more subtle explanation of why the IT Audit/Security panel was able to reach some degree of consensus stems from the nature of their work and engagement rotations. Excepting the two panelists who were employed in an internal audit capacity, all members of this panel managed an active client portfolio. In essence, rotating from client to client in a consultative role allowed these experts to bring a multitude of experiences and perspectives to bear, *without* being overly influenced by experiences and issues encountered in a single client. This broader world view is also reflected in the wide range of risk factors selected as their "most important," spanning strategy, technical, security and process concerns.

Conclusion and Implications

Our study highlights the difficulties associated with identifying technology-related risks in operations. Specifically, we demonstrate that stakeholders from business, IT and audit communities often have difficulty in both identifying those risks that merit attention, as well as assessing their relative importance. Furthermore, when IT risk factors *are* identified, there is often minimal agreement between the three stakeholder groups. Our results suggest that IT risks are highly situated, and that managers who consistently work in the same organization often find it difficult to look beyond the daily challenges their organization faces.

This study has implications for researchers and practitioners. For researchers, our study demonstrates the need to account for multiple perspectives when conceptualizing and operationalizing technology-related risk factors, especially when endeavoring to determine their relative importance and magnitude. Therefore, any effort to develop a theoretical framework for IT risk should include risk factors that are salient to a variety of organizational stakeholders. For practitioners, our results suggest that truly effective risk management strategies must incorporate multiple world views from within as well as outside the organization to completely identify those IT risks that a specific organization may face. Perhaps most importantly for external auditors and risk consultants, our findings suggest that decision makers within organizations tend to focus on issues and risks which remain fresh in their memory. As the old military adage goes, generals and politicians are often too busy fighting the ghosts of the last war, to react and respond to the current one.

References

Alter, S. and S. Sherer (2004). "A general, but readily adaptable model of information system risk." Communications of the AIS **14**: 1-28.

Anderson, J. and R. Narasimhan (1979). "Assessing project implementation risk: A methodological approach." Management Science **25**(6): 512-522.

Crouhy, M., D. Galai, and R. Mark. (2001). Risk Management. New York, McGraw-Hill.

Dearborn, D. and H. Simon (1958). "Selective perception: A note on the departmental identification of executives." Sociometry **21**(2): 140-144.

Dickson, G. W., R. L. Leitheser, J. Wetherbe, and M. Nechis. (1984). "Key information systems issues for the 1980's." MIS Quarterly **8**(3): 135-159.

Keil, M., A. Tiwana, and A. Bush. (2002). "Reconciling user and project manager perceptions of IT project risk: A delphi study." Information Systems Journal **12**: 103-119.

Li, E. (1997). "Perceived importance of information systems success factors: A meta analysis of group differences." Information & Management **32**(1): 15-28.

Niederman, F. and J. C. Brancheu (1991). "Information systems management issues for the 1990s." MIS Quarterly **15**(4): 475.

Northcraft, G. and M. Neale (1987). "Experts, amateurs and real estate: An anchoring-and-adjustment perspective on property pricing decisions." Organizational Behavior and Human Decision Processes **39**: 84-97.

Schmidt, R. (1997). "Managing delphi surveys using nonparametric statistical techniques." Decision Sciences **28**(3): 763-774.

Schmidt, R., K. Lyytinen, M. Keil, and P. Cule. (2001). "Identifying software project risks: An international delphi study." Journal of Management Information Systems **17**(4): 5-36.

Sherer, S. and S. Alter (2004). "Information system risks and risk factors: Are they mostly about information systems?" Communications of the AIS **14**: 29-64.

Tversky, A. and D. Kahneman (1974). "Judgment under uncertainty: heuristics and biases." Science **185**(4157): 1124-1131.

Tversky, A. and D. Kahneman (1981). "The framing of decisions and the psychology of choice." Science **211**(4481): 453-458.

Zmud (1980). "Management of large software development efforts." MIS Quarterly **4**(2): 45-55.