The International Journal of Digital Accounting Research
Vol. 14, 2014, pp. 1-35
ISSN: 2340-5058

# Cousins Separated by a Common Language: Perceptions of Information Technology Risk

**James L. Worrell**. University of Alabama at Birmingham. USA worrellj@uab.edu

**Ashley A. Bush**. Florida State University. USA.

**Paul M. Di Gangi**. University of Alabama at Birmingham. USA.

**Abstract.** The authors employ a seeded, ranking type Delphi to answer the following research question: how do each of the major stakeholder groups within organizations (representing both strategic and operational levels) conceptualize the risks associated with IT in operations? Using three expert panels drawn from Big 4 IT audit groups and Fortune 1000 business/IT managers, we identify the IT risks most salient to these groups, explore areas of convergence/divergence among them, and offer theoretical and practical implications from this research.

**Keywords:** Information Technology Risk, stakeholder groups, Delphi method.

## 1. INTRODUCTION

One has only to check the news headlines to appreciate the pervasiveness of business reliance on information technology (IT) and to grasp the variety of risks associated with its strategic use in the competitive marketplace. Numerous tales of disaster and significant corporate loss have repeatedly demonstrated the potential risks an organization faces when its operations and support processes rely on its IT infrastructure without taking necessary safeguards. For instance, an audit of the Department of Taxation for the State of Hawaii placed numerous employees on administrative leave due to internal security breaches of its tax database (Isotov, 2011). In 2012, a computer glitch in a newly-installed trading system at Knight Capital Group cost the firm $440 million when it erroneously triggered

*Submitted April 2013*
*Accepted January 2014*

DOI: 10.4192/1577-8517-v14_1

rapid-fire buys and sells of over 100 stocks (Popper, 2012). More recently, weaknesses in the point-of-sale systems at U.S-based retailer Target allowed hackers to gain access to customer credit and debit card information during the 2013 holiday shopping season (Harris *et al.*, 2014).

These failures, and countless others, illustrate the need for various organizational stakeholder groups to identify, understand and effectively manage the risks associated with IT operations. We define this risk (termed 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. While the need to properly identify IT risks is self-evident, this task is neither simple nor straightforward. Since IT risk impacts both technology and underlying business processes, they must be considered simultaneously. As a result of the Sarbanes Oxley Act of 2002 and associated Public Company Accounting Oversight Board (PCAOB) Auditing Standards, all publicly traded companies are required to assess their internal control structure, much of which is embedded within IT.

Furthermore, the impact of IT risk on business processes requires both business professionals (those who leverage the power of information systems to execute business processes and achieve business objectives) and IT professionals (those who develop and support IT at the operational level) to develop a shared vision of what IT risks actually threaten the organization's success and ability to support its business operations. Developing this shared vision necessitates that organizational stakeholders and decision makers agree on those IT risks 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 (Bassellier and Benbasat, 2004; Bassellier *et al.*, 2001; Keil *et al.*, 2002; Schmidt *et al.*, 2001).

IT solutions deployed in the production environment (hereafter referred to as 'IT in operations') and supporting day-to-day business activities can represent significant risks to achieving strategic, operational, reporting and compliance objectives. Given the complex and situated nature of identifying and prioritized IT risks in operations, as well as the various stakeholders involved in this task, there have been numerous calls for research on how stakeholder perceptions influence identification and assessment of IT risks (Abu-Musa, 2006; Hermanson *et al.*, 2000; Hunton *et al.*, 2004; Wilkin and Chenhall, 2010). We hope our study adds to this conversation, and is motivated by the following research questions: *How do each of the major stakeholder groups within organizations (representing both strategic and operational levels) conceptualize the risks associated with IT in operations*? *What are the factors that explain similarities and differences in their perceptions?*

This manuscript will proceed as follows. First, we review the relevant literature on the risks associated with IT in operations. Next, we present our rationale for employing a seeded, ranking-type Delphi study to address the research questions. The design and execution of the Delphi study are then explained, as well as the selection and composition of our three expert panels representing three distinct stakeholder groups (IT management, business management, and IT auditors).Our results suggest that each group holds a distinct perspective on IT risk, with wide disagreement between these groups as to which IT risk factors are most important and should therefore receive the most attention. We conclude our paper by discussing the theoretical and practical implications of this exploratory study.

## 2. BACKGROUND

As IT has become increasingly vital to efficient and effective operations, as well as accurate and timely reporting, the audit and governance community has responded with a variety of guidance and governance frameworks. Each of these frameworks addresses the need to identify the business risk associated with the deployment of IT. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management-Integrated Framework (ERM) tasks the firm's management with identifying events that threaten the organization's ability to achieve its objectives, specifically citing identification of risks that relate to technology (COSO, 2004). The IT Governance Institute's COBIT 5.0 similarly prescribes the identification of IT risk factors that may adversely affect the organization and should therefore be subject to controls that reduce the impact and likelihood of these risks to an acceptable level, and singles out business management as the most important stakeholder with respect to IT and its associated risks (ITGI, 2012). Finally, The Institute of Internal Auditors' GAIT-R views IT risk as a component of the organization's overall business risk, a component that must be accounted for when considering governance- and risk management-related issues (IIA, 2008).

Given the critical role that IT plays in financial reporting, it is not surprising that auditing standards have emerged to provide guidance on addressing IT risk in the context of the financial statement audit. SAS 109 tasks the auditor with performing a risk assessment of the entity, control environment, and its system of internal controls (Auditing Standards Board, 2006). AS5 requires the auditors of publicly traded companies to assess the adequacy of internal controls over financial reporting (Public Company Accounting Oversight Board, 2007). SAS 94 directs the auditor to gain an understanding of how IT impacts the system of internal controls (Auditing Standards Board, 2001). Since controls related to financial reporting are often embedded within the organization's IT (such as enterprise resource planning systems), identifying risks associated with IT takes on a prominent role in the audit planning process as well.

While identifying IT risk is critical in today's business environment, the definition, composition and importance of IT risk is a long running debate, with limited resolution (Sherer and Alter, 2004; Wilkin and Chenhall, 2010). Painting with a broad brush, the literature on IT risk falls into two dominant camps: (1) threats to IT in operations as they relate to the reliability of financial reporting and internal control over financial reporting, and (2) threats to the security of IT resources (i.e., the confidentiality, integrity and availability of information systems). Each perspective sheds light on the nature of IT risk and how it threatens the achievement of organizational objectives.

### 2.1 Reliability of financial reporting

Accounting researchers have turned their focus to better understanding how identification and assessment of IT risk influences the planning and execution of audit services, and ultimately the veracity of financial reporting. The emergence of e-business partnerships and outsourcing/co-sourcing arrangements, combined with the ubiquitous nature of computerized accounting systems, have increased the attention given to IT risk (Abu-Musa, 2006; Sutton and Hampton, 2003). IT risk investigated in the accounting information systems (AIS)literature include business interruption (Abu-Musa, 2006; Hermanson *et al.*, 2000; Hunton *et al.*, 2004), process interdependency (Hermanson *et al.*, 2000; Hunton *et al.*, 2004), logical security over networks and applications (Ettredge and Richardson, 2003;

Hermanson *et al.*, 2000; Hunton *et al.*, 2004), and data integrity (Abu-Musa, 2006; Mock *et al.*, 2008; Wright and Wright, 2002).

For the most part, the focus of recent IT risk research in the accounting domain has been a result of the Sarbanes Oxley Act and resulting guidance that places an emphasis on assessing internal control over financial reporting (ICoFR). As organizations have moved their accounting and financial reporting functions to advanced business information systems, auditors are forced to assess control risk and reliance on controls as part of planning and executing the audit (Abu-Musa, 2006; Hunton *et al.*, 2004). Since much of ICoFR is embedded in information systems, threats to these have far-reaching consequences that must be assessed and managed. Organizations with weak IT-related controls (i.e., those that fail to adequately manage IT risk related to financial reporting) report more misstatements of their financial reports than do those with more robust IT-related controls (Klamm and Watson, 2009).

## 2.2 Threats to IT resources.

The second literature stream casts IT risk in terms of breaches that negatively impact physical and/or logical resources (Rainer *et al.*, 1991; Sherer and Alter, 2004; Straub and Welke, 1998). These threats can be broadly categorized as relating to the interruption, interception, modification or fabrication of information resources (Yeh and Chang, 2007). Sources of these threats may be either internal or external to the organization and originate from human or nonhuman actors (Goodhue and Straub, 1991; Loch *et al.*, 1992; Straub and Welke, 1998). Threats to information resources include damage to physical resources (Loch *et al.*, 1992; Rainer *et al.*, 1991; Straub and Welke, 1998), malware and viruses (Loch *et al.*, 1992), unauthorized access (Loch *et al.*, 1992; Rainer *et al.*, 1991; Straub and Welke, 1998), and inadvertent damage by authorized users (Loch *et al.*, 1992; Rainer *et al.*, 1991; Straub and Welke, 1998).

Early works in this vein attempted to identify the nature of IT risk in information security terms. For example, Goodhue and Straub (1991) viewed the security and safeguarding of IT resources as a function of the risk inherent in the organization’s external environment, the extent of control activities placed into operation, and individual characteristics of managers. Straub and Welke (1998) extended this view by defining systems risk as the likelihood that IT resources are inadequately protected against damage or loss resulting from natural and manmade threats, and proposed a model to deter security breaches. Loch and colleagues (1992) contributed to the dialogue on IT risk by suggesting that threats may come from human and non-human sources, and may be deliberate or accidental in nature. Ranier and colleagues (1991) noted the subjective nature of assessing the impact and likelihood of IT risk, and suggested that managers may not act to reduce these risks because of the subjective nature of their assessment.

As research into the threats to information resources matured, scholars began to take a more critical view of these foundational works. Early theory-driven works were criticized because basic assumptions under which the theories hold true were ignored (Dhillon and Backhouse, 2001; Sharma and Dhillon, 2009). For example, classical probability theory (CPT) is the most commonly used theoretical lens through which to examine IT risk. One of CPT's primary assumptions is that historical events can be used to predict future outcomes. Because IT and its associated risk are relatively new phenomena that are continually adapting and emerging, limited historical data exist from which to predict future outcomes (Dhillon and Backhouse, 2001). In addition to these shortcomings, scholars have been criticized for failing to account for the temporal nature of IT risk as well as the non-financial impacts of IT disruptions (Raghupathi, 2007; Suh, 2003; Yeh and Chang, 2007).

### 2.3 Synthesis of the two literatures

Although there are distinct differences between the two literatures, both streams converge on several key points. Both recognize that IT is embedded in most facets of modern business, and this high degree of integration represents a source of risk. Both recognize that these threats to the organization's IT may have negative consequences for decision making, executing transactions, and reporting on the ongoing operations of the firm. Both acknowledge that the identification and assessment of IT risk is largely subjective and affected by perceptual differences among various stakeholders. Finally, both suggest that focusing on a single stakeholder's view of IT risk may yield suboptimal results.

Identifying and assessing IT risk is viewed as a subjective exercise by many scholars; therefore, understanding the perceptions of those identifying and assessing the impact and likelihood of IT risk is critical. Even among trained professionals, these perceptions are often at odds. For example, IT auditors often assess IT risk at higher levels than do their financial auditor counterparts, and auditors in general identify IT risk factors with greater frequency than do their counterparts in the organization's IT function (Abu-Musa, 2006; Hunton *et al.*, 2004).

One of the limitations of prior research on IT risk is that it often focuses on the perceptions of a specific stakeholder, such as project managers (Schmidt *et al.*, 2001), IT security specialists (Karabacak and Sogukpinar, 2005; Webb, 2000), business managers, IT executives (Dickson *et al.*, 1984; Niederman and Brancheu, 1991), assurance professionals (Hunton *et al.*, 2004), Board members (Parent and Reich, 2009) or the nebulous "user." Focusing on a single perspective can be problematic, as different stakeholders often have differing perspectives with respect to risk and expectations (Hermanson *et al.*, 2000; Keil *et al.*, 2002). Since management may view assessments of IT risk as subjective, they may be hesitant to make decisions based on the results of the risk assessment process (Rainer *et al.*, 1991). Although understanding the discrete IT risk factors that impact the organization's decisions and control mechanisms is crucial, equally important is grasping how various stakeholders prioritize their efforts and resources to mitigate these threats (Hermanson *et al.*, 2000).

One way in which various risk management frameworks can inform the academic community is their emphasis on multiple perspectives in identifying and managing IT risk. ERM, COBIT, and GAIT-R are consistent in the notion that management, not the IT function, is ultimately accountable for managing IT risk. While the IT function does play a role in identifying and managing IT risk, it does not bear exclusive responsibility and accountability. And while business management and IT management have a role to play in managing IT risk, audit and assurance professionals are tasked with assessing the effectiveness of management's risk identification, assessment and remediation efforts. In essence, all three stakeholders must work in unison through cooperation and collaboration for effective risk management to occur. Thus, a pressing need among both scholars and practitioners is to understand the similarities and differences of how each stakeholder group perceives IT risk.

## 3. RESEARCH DESIGN AND METHOD

We employed a Delphi study to ascertain similarities and differences in perceptions of IT risk factors among three distinct groups commonly involved in IT risk management: IT auditors, business management, and IT management responsible for the operation and maintenance of IT. These three stakeholder groups were chosen because they are traditionally involved in event identification and risk assessment efforts. Therefore, their perceptions (and where these perceptions converge and diverge) are of interest. The Delphi method has been used extensively in accounting, auditing and information systems research over the past quarter century (e.g., Baldwin-Morgan, 1993; Baldwin and Trinkle, 2011; Brancheau *et al.*, 1996; Brancheau and Wetherbe, 1987; Cotter, 1998; Dickson *et al.*, 1984; Greenstein and Hamilton, 1997; Holsapple and Joshi, 2001; Keil *et al.*, 2002; Mursu *et al.*, 2003; Ramamoorti *et al.*, 1999; Schmidt *et al.*, 2001), and is appropriate for exploratory studies involving complex multi-disciplinary problem sets (Meredith et al, 1989; Neely, 1993; Akkermans *et al.*, 1999, 2003). Itconsists of a series of structured, iterative group decision processes with the aim of reaching consensus among a panel of experts on a given decision task or issue (Linstone and Turoff, 2002). This method is appropriate when addressing research questions where no definitive answer exists, when leveraging divergent opinions regarding a problem or issue, and when experts are geographically and/or temporally dispersed (Linstone and Turoff, 2002; Schmidt, 1997).

The panel of experts remains unknown to one another, thereby avoiding any interaction of personalities that might serve to bias the panel's ability to reach consensus (Saren and Browlie, 1983). The Delphi method has been shown to provide more accurate decisions than other group decision process techniques, such as focus groups or nominal group technique (Rowe and Wright, 1999; Daniel and White, 2005). It has been used extensively in research whose aim is to identify factors and refine frameworks (see Bonson *et al.*, 2009; De Haes and Van Grembergen, 2009; Doke and Swanson, 1995; Fomin *et al.*, 2008; Greenstein and Hamilton, 1997; Iden and Langeland, 2010; Kasi *et al.*, 2008; Keil *et al.*, 2002, and Liu *et al.*, 2010).

For the present study, we chose a seeded, ranking-type Delphi survey, designed to gather the opinions of our expert panels and reach consensus on the importance of IT risk factors through a series of controlled iterative feedback exercises. Figure 1 provides an overview of the seeded Delphi method used in this study. The following subsections explain the choice and composition of the three expert panels, the selection of the IT risk factors used for our seed, and the execution of the study.

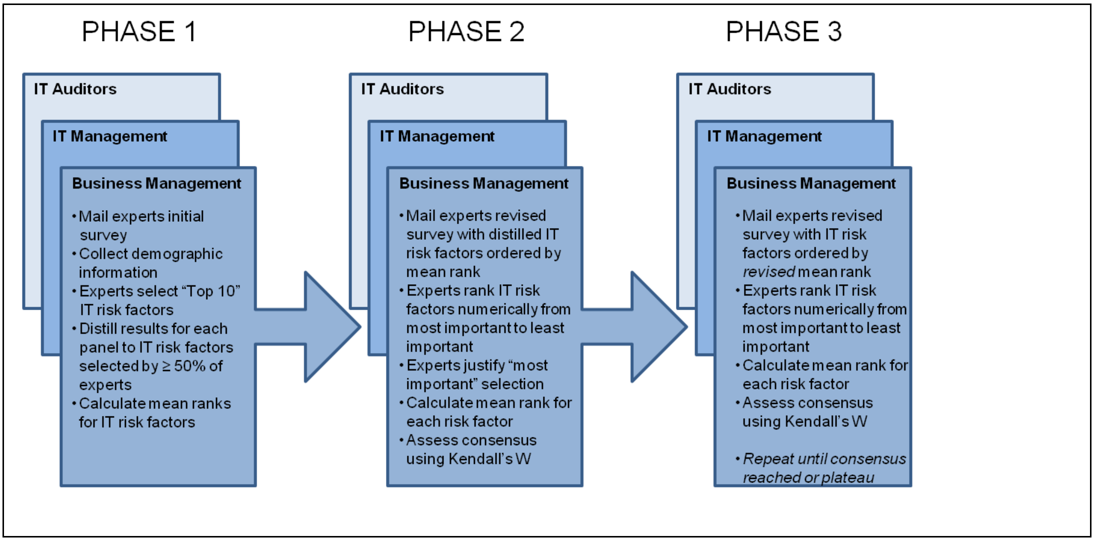
PHASE 1
IT Auditors
IT Management
Business Management
• Mail experts initial survey
• Collect demographic information
• Experts select "Top 10" IT risk factors
• Distill results for each panel to IT risk factors selected by ≥ 50% of experts
• Calculate mean ranks for IT risk factors
PHASE 2
IT Auditors
IT Management
Business Management
• Mail experts revised survey with distilled IT risk factors ordered by mean rank
• Experts rank IT risk factors numerically from most important to least important
• Experts justify "most important" selection
• Calculate mean rank for each risk factor
• Assess consensus using Kendall's W
PHASE 3
IT Auditors
IT Management
Business Management
• Mail experts revised survey with IT risk factors ordered by *revised* mean rank
• Experts rank IT risk factors numerically from most important to least important
• Calculate mean rank for each risk factor
• Assess consensus using Kendall's W
• *Repeat until consensus reached or plateau*

Figure 1. Seeded Delphi Method

### 3.1 Expert Panel Selection and Composition

Expert panel selection and composition is critical to the success of the Delphi method, and to the reliability of its results. In Delphi studies, the selection of "appropriate experts" is essential to the success of the study in terms of external validity. Studies must explicitly define the criteria used to assess expertise, whether it is academic credentials indicating sufficient training beyond that of a layperson (B.S., MBA, Ph.D., etc.), years of experience, or specific expertise areas denoted by professional license or credential (e.g., CPA, CISA, CISSP, etc.) (Adler & Ziglio, 1996).

In this study, our primary interest was in examining IT professionals, IT audit professionals, and business management professionals requiring narrow experience in terms of both academic, professional, and work experience history to ensure appropriate expertise is used. Each panel was representative of its industry in terms of traditional training and work experience indicating knowledge above and beyond the traditional layperson. As noted by Adler and Ziglio (1996, p14),

> *It should be noted that the definition of 'experts' varies according to the context and field of interest in which the Delphi method is going to be applied. Being an expert entails the acquisition of experience, special skill in or knowledge of a particular subject. Experts selected for participation in a Delphi process do not necessarily need*

*to have standard academic qualifications such as First Class Honours degrees and Ph.Ds.*

Three expert panels were created with experts selected based on their expertise and years of industry experience (see Tables 1 and 2 for demographics). Expert panel sizes were chosen to be sufficiently large to provide a variety of perspectives, and yet sufficiently small to manage information and provide timely feedback. Guidance varies on an "ideal" panel size. Extant literature suggests a panel of 10 to 18 experts is acceptable, with panel sizes as small as 4 being sufficient under ideal conditions (Boje and Murnighan, 1982; Brockhoff, 2002; Dalkey and Helmer, 1963; Delbecq *et al.*, 1975; Paliwoda, 1983). Studies have suggested that there is no consistent relationship between panel size and effectiveness in decision making (Brockhoff, 2002; Boje and Murnighan, 1982). While we tried to keep the panels roughly the same size, analysis of panel feedback is not affected by unequal panel size (Schmidt, 1997).

The IT auditors expert panel was composed of 16 experts representing 7 unique organizations 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 held at least one professional certification (CPA, CIA, CISA, or CISSP) and ranged from senior associate to partner. Furthermore, more than half (56%) of panel members earned a graduate degree which aligns with the extensive educational requirements associated with the auditing field. The majority (88%) of the IT auditors expert panel were employed by large organizations (IT expenditures of more than $100 million) within the professional services industry. Panel members averaged 7.7 years of experience in their field, with 4.7 years at their current organization. All panelists were residents of and worked primarily in the United States.

The business management expert panel was composed of 14 experts representing 8 unique organizations, with seven employed as managers in Fortune 1000 companies, and 79% working for large, publicly traded companies. Half of the expert panel worked within the financial services industry. On average, panel members had 14.5 years of experience in their field with 4.4 years working for their existing organization. This indicates the panel consisted of experts at the middle- to upper- level of management which aligns with our target panel. These experts represented a variety of business units within their respective organizations, including marketing, strategic planning, financial reporting, operations, and human resources. Our goal in assembling the business management expert panel with varied management focus was to more clearly represent a typical management team that considers issues at the managerial rather than field-specific level. All panelists were residents of and worked primarily in the United States.

The IT management expert panel was composed of 11 experts representing 6 unique organizations, nine of whom were employed by Fortune 1000 companies. In general, the IT management expert panel exhibited similar characteristics to the business management panel. A majority (73%) worked within the financial services industry and possessed on average 16.5 years of work experience with 6.1 years in their current organization. Similarly, experts were drawn from a variety of IT backgrounds, including network engineering, computer operations, disaster recovery/business continuity, enterprise technical architecture, IT product management, and application development. As with the business management panel, we assembled this panel to possess a holistic view of IT within an organizational context. All panelists were residents of and worked primarily in the United States.

Participation in the expert panels was entirely voluntary. The experts within and across panels remained unknown to each other, and were geographically dispersed. At the completion of the study, panelists received a $5 coffee house gift card and an executive summary of the study’s findings. As part of the solicitation process, panelists were informed of the necessity to devote adequate time and effort to the issue under investigation, as well as the need to complete all rounds in a timely manner. Throughout the course of the study, all but one panelist for each expert panel completed all rounds of the Delphi process.

| | **IT Auditors (n=16)** | **Business Management (n=14)** | **IT Management (n=11)** |
|---|---|---|---|
| **Educational Level** | | | |
| Associate | - | - | 27% |
| Bachelors | 44% | 57% | 64% |
| Masters | 56% | 43% | 9% |
| **Years in Field** | | | |
| Mean | 7.69 | 14.5 | 16.45 |
| St. Dev. | 2.73 | 7.29 | 7.19 |
| **Tenure in Organization** | | | |
| Mean | 4.67 | 4.43 | 6.09 |
| St. Dev. | 2.75 | 2.82 | 4.21 |

Table 1. Individual Demographics

| | **IT Auditors (n=16)** | **Business Management (n=14)** | **IT Management (n=11)** |
|---|---|---|---|
| **Ownership model** | | | |
| Publicly Traded | 13% | 79% | 82% |
| Privately Held | 88% | 7% | 9% |
| Government | - | 7% | - |
| Not for Profit | - | 7% | 9% |
| **Industry** | | | |
| Financial Services | 6% | 50% | 73% |
| Manufacturing | - | 21% | - |
| Professional Services | 94% | 7% | 9% |
| Healthcare | | 7% | 9% |
| Information Services | - | 7% | 9% |
| Transportation | - | 7% | - |
| **Number of Employees** | | | |
| Less than 5,000 | 6% | 36% | 9% |
| 5,000 - 9,999 | - | 57% | 73% |
| 10,000 - 99,999 | 6% | 7% | 18% |
| More than 100,000 | 88% | - | - |
| **Annual Revenues** | | | |
| Less than $1 billion | 6% | 14% | 9% |
| $1 billion - $4.9 billion | - | 43% | 73% |
| $5 billion - $9.9 billion | 6% | 14% | - |
| More than $10 billion | 88% | 29% | 18% |
| **IT Expenditures** | | | |
| Less than $50 million | 6% | 57% | 18% |
| $50 million - $99.9 million | - | 43% | 82% |
| More than $100 million | 94% | - | - |

Table 2. Organizational Demographics

Overall, each expert panel adequately represents the specific targets intended by the researchers (Linstone and Turoff, 2002). Based on the demographic data, each panel possessed the unique characteristics, titles, and requisite work responsibilities to suggest the panelists would accurately represent the three stakeholder groups of interest (Brockhoff, 2002; Delbecq *et al.*, 1975). Having assessed the composition of each expert panel as suitable for our purposes, we proceeded to the next stage of the Delphi process which presented an initial list of IT risk factors to the expert panels for selection and elimination.

## 3.2 IT Risk Factors Seed

Consistent with prior studies that have employed a seeded Delphi method (Greenstein and Hamilton, 1997; Keil *et al.*, 2002; 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 *starting point* for our list, and then augmented this list with IT risk factors from the broader management information systems and accounting information systems literatures. Sherer and Alter's (2004) list was chosen as the starting point for deriving our IT risk factors for two main reasons. First, their list was compiled based on articles that focused on risk published in leading IS research outlets, and therefore represented an organized cross-section of the IT risk literature. Second, and perhaps more importantly, Sherer and Alter (2004) differentiated between risks associated with implementing new technologies (i.e., project risk) and risks associated with operations. We elected to scope risks associated with IT projects out of our study because we were keenly interested in IT risks related to those systems currently deployed in the production environment and supporting business activities. From our perspective, IT projects represented IT initiatives that were still in a developmental phase, and therefore not supporting current business activities.

After initially identifying 27 risk factors specific to IT in operations, we developed definitions for these based on the underlying research 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 a group of experts consisting of both academics and practitioners with expertise in the area of IT risk. The experts 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 their feedback, several IT risk factors were either dropped or combined with others, and definitions were refined, resulting in the final list of 22 IT risk factors submitted to the three expert panels for evaluation.

### 3.3 Data Collection and Analysis Method

After assembling the three expert panels, each panelist was emailed a link to a web-based survey 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 to ensuring the confidentiality, integrity and availability of information systems, 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. This additional step was taken to ensure that all relevant IT risk factors were afforded the opportunity to be represented. Given the fragmented nature of the IT risk literature, as well as the constantly changing nature of IT, we felt this additional step was crucial to obtain a thorough and up-to-date list of IT risk factors. Although 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.

After receiving each panel's selection of "most important" IT risk factors, a reduced list was created (see Table 3 for the reduced list by expert panel) by carrying forward any IT risk factor from the previous step that received a simple majority (50% or more selections within the specific expert panel) (Schmidt, 1997). Each panelist was then presented with the reduced list (specific to their expert panel) ordered based on the percentage of their expert panel that selected the IT risk factor as one of their most important so they could be ranked in terms of importance. Panelists were asked to rank these IT 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 in order to gain insight into each panelists ranking rationale for researchers as well as to provide context and explanation to other panelists (Boje and Murnighan, 1982). This allows the panelist to consider the opinion of other members without directly influencing his or her ranking decision. This one-way, non-interactive approach used in the Delphi method reduces the likelihood of group biases from influencing each panelist, maintains the conceptual purpose of the technique to establish consensus among a panel of independent experts, and has been shown to increase the accuracy and quality of assessments by the expert panels (Best, 1974).

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 for their panel ordered by their mean ranks based on the previous round results, and included feedback indicating the degree of consensus among their expert panel relative to the risk factor rankings. Each round displayed the current rankings from the prior round, but did not display prior individual round rankings so as to reduce an anchor/adjustment bias from the panelists. Each round was conducted over a two week period with a reminder sent five days before each deadline. This process was repeated until consensus reached a plateau (Linstone and Turoff, 2002; Schmidt, 1997). Data collection lasted approximately seven weeks.

## 4. RESULTS

Results for each expert panel are summarized in Table 3. Seventeen members of the IT auditors' expert panel initially responded to the study, resulting in sixteen usable responses[1]. The eight IT risk factors identified by this expert panel are almost evenly split among those that suggest weaknesses in IT governance (*R8-Lack of organizational alignment between business and IT, R7-Lack of IS participation in business initiatives*), those that suggest weaknesses in management of IT processes and resources (*R3-Information quality, R17-Resource insufficiency, R22-Weak change management*), and those that suggest weaknesses in technology security and configuration (*R6-Interdependencies between systems, R19-Technical complexity, R20-Unauthorized information access*)[2]. Kendall's W for this phase was 0.30, which indicates weak agreement in the rankings among the panelists (Schmidt, 1997). We conducted follow-up rounds to improve the degree of consensus among this panel. Subsequent rounds

[1] Initial panel sizes were as follows: IT auditors' panel (17), business management panel (15) and IT management panel (12). For the IT auditors' expert panel, one expert and associated responses were dropped due to the respondent incorrectly completing the initial survey. For the remaining two expert panels, one expert and associated responses were dropped from each panel due to attrition.

[2] We elected to use the dimensions from the IT Control Framework presented in The IIA's Global Technology Audit Guide-Information Technology Controls (IIA, 2005) guidance as a basis for categorizing IT risks. This framework suggests IT risks and controls fall into three categories: Governance, Management, and Technical.

resulted in Kendall's W of 0.37 and 0.39 suggesting moderate agreement in the rankings among the panelists, after which the Delphi was discontinued for this expert panel. Based on feedback from the panelists, we determined that we had reached a plateau of consensus and that further rounds would not result in a greater degree of consensus.

Fifteen business management experts initially responded to the study, with fourteen usable for analysis. The nine IT risk factors identified by this expert panel were mostly related to weaknesses in technology security and configuration (*R1-Difficulty integrating software from vendors and subcontractors, R6-Interdependencies between systems, R15-Problematic interfaces between systems, R18-Software errors/bugs, R19-Technical complexity*), some consideration for weaknesses in management of IT processes and resources (*R3-Information quality, R17-Resource insufficiency, R22-Weak change management*), and only one risk factor associated with IT governance (*R8-Lack of organizational alignment between business and IT*). Kendall's W for this phase was 0.30, which indicates weak agreement in the rankings among the expert panel. Based on this result, a subsequent round was conducted, resulting in a significant drop-off in agreement (Kendall's W = 0.23). In accordance with Schmidt's (1997) guidance, we deemed we had reached a plateau of consensus in the initial round. Twelve IT management experts initially responded to the study, with eleven usable for analysis. Similar to the business management expert panel, the ten IT risk factors identified by this expert panel were mostly related to weaknesses in technology security and configuration (*R1-Difficulty integrating software from vendors and subcontractors,R6-Interdependencies between systems, R11-Malicious software,R15-Problematic interfaces between systems, R18-Software errors/bugs, R19-Technical complexity,R20-Unauthorized information access*), followed by those related to weaknesses in IT governance (*R8-Lack of organizational alignment between business and IT, R7-Lack of IS participation in business initiatives*) and management of IT processes and resources (*R21-Unauthorized physical access to hardware and processing environment*). Kendall's W for this phase was 0.37 which suggests moderate agreement in the rankings, prompting us to conduct a subsequent round in an effort to achieve a greater degree of consensus among the expert panel. However, as with the business management expert panel, the subsequent round resulted in significantly lower agreement among the panelists (Kendall's W = 0.22), and we determined that subsequent rounds would be counterproductive.

| **IT Risk Factor**(source) | | **IT-A** | **BM** | **IT-** | **Definition** |
|---|---|---|---|---|---|
| **R1** | **Difficulty integrating software from vendors and subcontractors** (Schmidt *et al.*, 2001) | | 5 | 5 | Integration of packages from multiple vendors hampered by incompatibility and lack of cooperation |
| **R2** | **Inability to implement solution in existing technical environment** (Baskerville and Stage, 1996) | | | | Information system to be implemented is incompatible with the existing technical environment |
| **R3** | **Information quality** (Ackoff, 1967) | 3 | 1 | | Failure in management decision-making resulting from irrelevant, incorrect, or insufficient information provided by the information system |
| **R4** | **Information quantity** (Ackoff, 1967) | | | | Failure in management decision making resulting from a lack of or overabundance of information provided by the information system |
| **R5** | **Infrastructure performance shortfalls**(Kemerer and Sosa, 1991) | | | | Performance problems associated with the telecommunications infrastructure, such as reliability or network throughput |
| **R6** | **Interdependencies between systems** (Barki *et al.*, 2001; Gogan *et al.*, 1999) | 4 | 6 | 1 | The need for systems to share data with other applications or systems, either internal or external to the organization |
| **R7** | **Lack of IS participation in business initiatives** (Grover *et al.*, 1995) | 6 | | 7 | Failure to aggressively leverage or engage IT enablers in business initiatives |
| **R8** | **Lack of organizational alignment between business and IT** (Grover *et al.*, 1995; Kemerer and Sosa, 1991; Reich and Benbasat, 2000) | 1 | 4 | 2 | Failure to align the IT infrastructure and applications with business needs |
| **R9** | **Lack of user commitment to technology** (Barki *et al.*, 2001) | | | | Users are unwilling to accept the changes the information system entails, or do not have a positive opinion regarding how the information system can meet their needs |
| **R10** | **Large number of system users/oversubscription** (Kemerer and Sosa, 1991) | | | | Inability of the information system to meet unanticipated demand |

Table 3. IT Risk Factors, Rankings and Associated Definitions

| | | | | | |
|---|---|---|---|---|---|
| **R11** | **Malicious software** (Loch *et al.*, 1992) | | | 6 | Software written to produce an undesirable effect to the system, user, or organization |
| **R12** | **New or unproven technology** (Barki *et al.*, 2001; Schmidt *et al.*, 2001) | | | | "Bleeding edge" technology that has not been previously used successfully in similar applications in other organizations |
| **R13** | **Physical damage to processing environment**(Straub and Welke, 1998) | | | | Firm's information systems are not adequately protected against disasters or other physical threats |
| **R14** | **Poor help desk and user support function** (Smith *et al.*, 2001) | | | | User help desk and regular end-user support functions are insufficient |
| **R15** | **Problematic interfaces between systems** (Barki *et al.*, 2001; Gogan *et al.*, 1999) | | 2 | 4 | Information and data exchanges between systems do not occur completely, accurately, or in a timely manner |
| **R16** | **Reliance on consultants and vendors** (Schmidt *et al.*, 2001) | | | | Consultants or vendors do not deliver, go out of business, or are unclear as to their roles and responsibilities |
| **R17** | **Resource insufficiency** (Grover *et al.*, 1995; Jiang *et al.*, 2002) | 7 | 7 | | Insufficient resources are available to carry out or execute an IS initiative or plan, such as insufficient personnel or budgeting |
| **R18** | **Software errors / bugs** (Loch *et al.*, 1992) | | 3 | 8 | Programming problems typically resulting from oversights of programmers and/or analysts |
| **R19** | **Technical complexity** (Zmud, 1980) | 8 | 9 | 9 | Information system or application is comprised of multiple components that combine to yield a complex system |
| **R20** | **Unauthorized information access** (Loch *et al.*, 1992; Straub and Welke, 1998) | 2 | | 3 | Firm's information or information systems are not adequately secured against unauthorized logical access |
| **R21** | **Unauthorized physical access to hardware and processing environment** (Loch *et al.*, 1992) | | | 10 | Weak, ineffective, or inadequate physical control over access to the processing environment |
| **R22** | **Weak change management** (Boehm and Ross, 1989) | 5 | 8 | | Weak policies and procedures governing changes to applications or technical infrastructure and other information system components |

Table 3. IT Risk Factors, Rankings and Associated Definitions (continuation)

## 5. DISCUSSION

The purpose of this exploratory study was to answer the following research questions: *How do each of the major stakeholder groups within organizations (representing both strategic and operational levels) conceptualize the risks associated with IT in operations*? *What are the factors that explain similarities and differences in their perceptions?* For our study, we focused on the IT risk perceptions of three key stakeholder groups: IT auditors, business management, and IT management. These three stakeholder groups were chosen because of their heavy involvement in organizational risk management processes, which include identifying IT risk exposure and recommending IT risk remediation strategies. Given the sometimes conflicting priorities of these groups, we anticipated that there would be convergence as well as divergence of perceptions among the three groups. The results of the study bore this out, suggesting several topics that warrant discussion. First are the points of convergence between the three expert panels (i.e., the overlap in risk factors identified by all three panels as their "most important"). The second, and perhaps more interesting, topic of discussion is to address the question of why two of the three expert panels failed to reach strong consensus on the rankings of IT risk factors. The final topic of discussion is to review instances where there was overlap in IT risk factors between two expert panels, but not a third.

Of the thirteen IT risk factors identified across the three expert panels, only three were identified as "most important" across all expert panels: *(R8) Lack of organizational alignment between business and IT, (R6) Interdependencies between systems, and (R19) Technical complexity*. Not surprisingly, all groups ranked *(R8) Lack of organizational alignment between business and IT* relatively high. This relatively high ranking across the three expert panels likely is a result of the attention that IT governance has received, as well as past failures in aligning IT initiatives with business needs (Chan and Reich, 2007; Chan *et al.*, 2006; Henderson and Venkatraman, 1999; Piccoli and Ives, 2005). 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, *(R6) Interdependencies between systems* and *(R19) Technical complexity*, 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 *(R6) Interdependencies between systems*, all three expert panels ranked *(R19) Technical complexity* in the bottom third of their listing. 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 development manager at a large health insurer 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.*

A second discussion topic suggested by the results is to explore why these panels were unable to reach strong consensus on the rankings. We can look to two sources for explanations: internal and external contextual factors, and biases in individual decision making.

COBIT's control objectives for Assess and Manage IT Risks (PO9) suggest that those involved in IT risk management establish and evaluate the context within which IT risk occurs. As part of this evaluation process, the internal and external environment should be examined to identify areas of concern. This sentiment is echoed with COSO's ERM in the event identification component.

Both frameworks advocate a cross-functional approach to identification and assessment of IT risks because different viewpoints lead to a richer risk assessment process. It is possible that experts across all three panels were implicitly evaluating the internal and external environments of their organizations, and factoring these considerations into their rankings of IT risk factors. Given the diversity in organizational settings and industries, this represents one potential explanation.

A second and equally supported explanation exists. Confronted 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). People employ heuristics that often lead to suboptimal decision making (Northcraft and Neale, 1987; Tversky and Kahneman, 1981; 1974). For instance, an individual may anchor thier organization’s risk culture, resulting in a narrow definition of risk and how IT either enhances or reduces these risks (Northcraft and Neale, 1987; Tversky and Kahneman, 1974). Furthermore, 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, suggest a plausible explanation as to why the business management and IT management expert panels in particular were unable to achieve a high degree of consensus.

Several panelists shared comments that support this explanation. For example, 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 follow-up conversation, this executive 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. Recall the Manager of Cost Accounting who likened his organization’s systems to “Frankenstein’s monster” and noted that issues “just this month” drove home the importance of interdependencies between systems. 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 management and IT management panelists) who work day in and day out in the same organization tend to focus on issues that challenge their particular organization. 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. While knowledge of a specific organization, its challenges and capabilities may afford a more accurate assessment and deeper understanding of organization-specific IT risks, heavy reliance on this knowledge may blind management to threats resulting from issues and circumstances not yet encountered by their current employer.

Although we could have expected to see weak to moderate consensus in the business management and IT management expert panels (given the diversity of responsibilities within each grouping), we were surprised that the IT auditors expert panel did not achieve a much higher consensus on the IT risk rankings. Based on these experts' qualifications, educational background, and training regimen, there was substantially less variance within this expert panel than the others. All possessed at least one audit or security-related professional certification, had received initial multi-week IT audit training upon joining their respective firms, were either currently employed in or were alumni of "Big 4" IT audit practices, and possessed a working knowledge IT and internal controls.

These factors would suggest that a common mindset is created for how professionals approach organizational issues and how they prioritize the relative importance of these issues, regardless of specific circumstance or organizational factors (Walsh, 1988). However, the results did not bear this out. After following up with several experts on this panel, the most likely explanation for moderate consensus in the IT risk rankings has to do with firm-mandated specializations in industry and technology. Many of the experts in our IT auditor panel were highly attuned to IT risk factors specific to platforms and industries, often to the exclusion of others. In essence, they are susceptible to the same biases found in the IT management and business management expert panels.

Finally, we were interested in exploring those instances where two expert panels shared ranking commonalities which were dissimilar to the remaining expert panel. While an in-depth exploration of the motivations and perceptions of expert panel members is beyond the scope of the Delphi method, a comparison of the commonalities among the expert panels indicates the potential for power dynamics and shared interests as a factor in the ranking process. Research suggests that politics within organizations affect organizational units as they vie for influence in how finite resources are distributed (Ferris *et al.*, 1989; Mintzberg, 1985; 1983).The purpose of the Delphi method is to create a rank-ordered listing of issues. Such a list might be used by executive management teams for making budgetary decisions to ensure an organization is maximizing the value of its resources while minimizing its exposure. Consequently, it is likely that the expert panels would share commonalities in their ranking of specific issues based upon shared interests. For instance, the role of IS participation in business initiatives would be vitally important to any technology-oriented organizational unit. Interestingly, both the IT auditors and IT management expert panels cited *(R7 )Lack of IS participation in business initiatives* as a potential risk while the business management expert panel did not indicate this risk being of primary importance. This sentiment was alluded to by a Senior Manager of Consumer Banking and Lending at a Fortune 500 financial services firm:

> *My rank in importance focused on the human element of IT Management. Information quality, insufficient resources and the alignment between IT and management are more political and volatile in the company than 'weak change management', which is a process that can be analyzed and controlled.*

IT auditors and IT management shared common rankings for several items which business management left unranked. Given the technology-oriented focus of the IT auditors and IT management expert panels, members of these expert panels maintain a sense of allegiance to their respective problem domains (e.g., IT). Both IT auditors and IT management expert panels also ranked *(R20) Unauthorized physical access to hardware and processing environment* as vitally important to an organization’s risk concerns; however business management panelists did not include this risk. Both IT auditors and IT management ranked *(R8) Lack of organizational alignment between business and IT* as vitally important, while business management panelists ranked it considerably lower. It appears that framing of organizational issues from their referent discipline may still influence their selection and assessment of IT risk factors.

Similarly, convergence exists between the IT auditors and business management expert panels as well as the IT management and business management expert panels. The IT auditors and business management expert panels viewed the quality, usefulness and control of information as highly important. Both expert panels ranked *(R3) Information quality, (R17) Resource insufficiency,* and *(R22) Weak change management* as vital concerns, while the IT management expert panel did not include these in their rankings. The IT auditors and business management expert panels possessed a shared vision of information as a strategic resource which requires it to be protected through control mechanisms and of sufficient quality to ensure effective decisions are made.

As can be seen from the results of this study, each expert panel expressed distinct opinions on the importance of certain IT risk factors over others. Each expert panel demonstrated the challenges facing organizations when it comes to effectively managing their risk portfolio in concert with organizational dynamics and individual proclivities. As expected, commonalities exist across the expert panels indicating that while some IT risk factors rise above the tides of selective perceptions from individual stakeholder groups, we cannot but question how prior experiences, politics, and idiosyncrasies in decision making influence the ability to identify and evaluate IT risk.

## 6. CONCLUSION AND IMPLICATIONS

Nobel Laureate George Bernard Shaw has been famously quoted as observing that “England and America are two countries separated by a common language.” The results of this study suggest that Shaw’s observation about cousins being separated by a common language holds true today as it relates to IT risk *in operations*: business, IT and audit professionals are all concerned with managing IT risk, but each approaches the task from different perspectives. Specifically, we demonstrate that stakeholders from business, IT and audit communities often have difficulty in both identifying those risk factors 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 risk is situational***, and that managers who consistently work in the same organization or industry often find it difficult to look beyond the daily challenges their organization faces. This bias may present a significant challenge to effective risk management efforts. While it is has been several decades since the early work on biases was first established, it appears that ***biases***

***and selective perception remain a significant hurdle*** for management and audit professionals must still strive to overcome.

As with all research, our study is not without its limitations. First, the purpose of this study was to broaden our existing views of IT risk and serve as an initial discussion point for both researchers and practitioners. The Delphi method is a valuable method to initiate this discussion and allows panel members to reflect on the perceived importance of each IT risk factor in both an independent and collective manner. Furthermore, this study included three separate expert panels to obtain a cross-functional view of how IT risk is perceived within organizations today. As a direct result of treating each panel as a distinct entity, a limitation to the current study is the reliance on researcher observation and interpretation to synthesize the results. Future research that conducts similar Delphi studies should consider incorporating an integration point at the end of the study to give panel members an opportunity to reflect and comment on the results of each expert panel (e.g., Sutton *et al.*, 2008). Second, interpretation of the expert panel results was based largely on the use of strategic thinking (i.e., experts would act in the best interest of the organization as a whole). While some explanation was provided concerning non-strategic rationales based on power and politic influences commonly seen in organizations, the potential for alternative assessments of the ranking differences is warranted. Future research should consider developing surveys and other assessment techniques to capture alternative perspectives that may influence a panel member's ranking decisions. Lastly, the lack of information concerning motivations prevents this study from exploring the role of power dynamics that may influence the risk rankings and provide further explanation of the commonalities between two and not a third expert panel. Future research is needed to determine whether organizational politics factors influence organizational units to ensure specific risks are deemed important.

This study has implications for researchers and practitioners. To our knowledge, it is one of the first studies to examine how the three primary stakeholder groups involved in organizational risk management view IT risk. 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. Moreover, researchers should not discount the influence of organizational politics and power dynamics in the identification, evaluation and remediation of risks. Therefore, any effort to develop a theoretical framework for IT risk should include risk factors that are salient to a variety of organizational stakeholders, and account for non-strategic influences on decision making and prioritization. Finally, our results suggest that IT auditors, including those in public accounting, often are susceptible to the same biases we found in experts employed in their client base.

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 particular organization may face. Additionally, those tasked with identifying IT risk factors within organizations must learn to balance their past experiences so as not to be blinded to un-encountered, but equally threatening, risks. Perhaps most importantly for 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.

## 7. REFERENCES

ABU-MUSA A. (2006): “Perceived security threats of computerized accounting information systems in the Egyptian banking industry”, *Journal of Information Systems*, vol. 20:187-203. http://dx.doi.org/10.2308/jis.2006.20.1.187

ACKOFF, R. (1967): “Management misinformation systems”, *Management Science*, vol.14:147-156. http://dx.doi.org/10.1287/mnsc.14.4.B147

AKKERMANS, H.; BOGERD, P.; VOS, B. (1999): “Virtuous and vicious cycles on the road towards international supply chain management”, *International Journal of Operations & Production Management*, vol.19:565-581. http://dx.doi.org/10.1108/01443579910260883

AKKERMANS, H. A.; BOGERD, P.; YÜCESAN, E.; & VAN WASSENHOVE, L. N. (2003): “The impact of ERP on supply chain management: Exploratory findings from a European Delphi study", *European Journal of Operational Research* 146:284. http://dx.doi.org/10.1016/S0377-2217(02)00550-7

ADLER, M.; ZIGLIO, E. (1996): "*Gazing into the oracle: The Delphi method and its application to social policy and public health". London: Jessica Kingsley Publishing.*

AUDITING STANDARDS BOARD (2001): "The effect of information technology on the auditor's consideration of internal control in a financial statement audit". *Statement on Auditing Standards*, n. 94. New York, NY: AICPA.

AUDITING STANDARDS BOARD (2006): "Understanding the entity and its environment and assessing the risk of material misstatements", *Statement on Auditing Standards,* n. 109. New York, NY: AICPA.

BALDWIN-MORGAN A. (1993): "The impact of expert system audit tools on auditing firms in the year 2001: A Delphi investigation", *Journal of Information Systems*, vol. 7:16-34.

BALDWIN A.; TRINKLE B. (2011): "The impact of XBRL: A Delphi investigation", *The International Journal of Digital Accounting Research*, vol. 11:1-24. http://dx.doi.org/10.4192/1577-8517-v11_1

BARKI H.; RIVARD S.; TALBOT J. (2001): "An integrative contingency model of software project risk management", *Journal of Management Information Systems,* vol.17:37-69.

BASKERVILLE R.; STAGE J. (1996): "Controlling prototype development through risk analysis", *MIS Quarterly*, vol. 20:481-504. http://dx.doi.org/10.2307/249565

BASSELLIER G.; BENBASAT I. (2004): "Business competence of information technology professionals: Conceptual development and influence on IT-business partnerships", *MIS Quarterly,* vol. 28:673-694.

BASSELLIER G.; REICH B.; BENBASAT I. (2001): "Information technology competence of business managers: A definition and research model", *Journal of Management Information Systems*, vol. 17:159-182.

BEST R. (1974): "An experiment in Delphi estimation in marketing decision making", *Journal of Marketing Research*, vol.11:448-452. http://dx.doi.org/10.23

07/3151295

BOEHM B.; ROSS R. (1989): “Theory-W software project management: Principles and examples”, *IEEE Transactions on Software Engineering,* vol. 15:902-917. http://dx.doi.org/10.1109/32.29489

BOJE D.; MURNIGHAN J. (1982): “Group confidence pressures in iterative decisions”, *Management Science* vol. 28:1187-1196. http://dx.doi.org/10.1287/mnsc.28.10.1187

BONSON, E.; CORTIJO, V.; EXCOBAR, T. (2009): “A Delphi investigation to explain the voluntary adoption of XBRL”, *The International Journal of Digital Accounting Research*, vol. 9:193-205. http://dx.doi.org/10.4192/1577-8517-v9_7

BRANCHEAU J.; JANZ B.; WETHERBE J. (1996): “Key issues in information systems management: 1994-1995 SIM Delphi results”, *MIS Quarterly*, vol. 20:225-242. http://dx.doi.org/10.2307/249479

BRANCHEAU J.C.; WETHERBE J.C. (1987): “Key issues in information systems management”, *MIS Quarterly,* vol. 11:22. http://dx.doi.org/10.2307/248822

BROCKHOFF K. (2002): “*The performance of forecasting groups in computer dialogue and face-to-face discussion*”. In Turoff M.; Linstone H.; Eds. *The Delphi Method: Techniques and Applications*: Addison-Wesley Publishing Co.: 285-311.

CHAN Y.; REICH B. (2007): “IT alignment: what have we learned”, *Journal of Information Technology*, vol. 22:297-315. http://dx.doi.org/10.1057/palgrave.jit.2000109

CHAN Y.; SABHERWAL R.; THATCHER J. (2006): “Antecedents and outcomes of strategic IS alignment: an empirical investigation”, *IEEE Transactions on Engineering Management*, vol. 53:27-48. http://dx.doi.org/10.1109/TEM.2005.861804

COSO (2004): “*Enterprise risk management-Integrated framework*”. Jersey City, NJ: American Institute of Certified Public Accountants.

COTTER J. (1998): “Utilisation and restrictiveness of covenants in Australian private debt contracts”, *Accounting & Finance,* vol. 38:181-196. http://dx.doi.org/10.1111/1467-629X.00009

DALKEY N.; HELMER O. (1963): "An experimental application of the Delphi method to the use of experts", *Management Science,* vol. 9:458-467. http://dx.doi.org/10.1287/mnsc.9.3.458

DANIEL, E.; WHITE, A. (2005): "The future of inter-organisational system linkages: Findings of an international Delphi study", *European Journal of Information Systems*, vol. 14:188-203. http://dx.doi.org/10.1057/palgrave.ejis.3000529

DEARBORN D.; SIMON H. (1958): "Selective perception: A note on the departmental identification of executives", *Sociometry,* vol. 21:140-144. http://dx.doi.org/10.2307/2785898

DEHAES, S.; VANGREMBERGEN, W. (2009): "An exploratory study into IT governance implementations and its impact on business/IT alignment", *Information Systems Management*, vol. 26:123-137. http://dx.doi.org/10.1080/10580530902794786

DELBECQ A.; VENA.V.D.; GUSTAFSON D. (1975): "*Group techniques for program planning: A guide to nominal group and Delphi processes"*. Glenview: Scott, Foresman and Company.

DHILLON G.; BACKHOUSE J. (2001): "Current directions in IS security research: Towards socio-organizational perspectives", *Information Systems Journal*, vol. 11:127-153.

DICKSON G.W.; LEITHESER R.L.; WETHERBE J.C.; NECHIS M. (1984): "Key Information systems issues for the 1980's", *MIS Quarterly,* vol. 8:135.

DOKE, E. R.; SWANSON, N. E. (1995): "Decision variables for selecting prototyping in information systems development: A Delphi study of MIS managers, *Information & Management*, vol. 29:173-182.

ETTREDGE M.; RICHARDSON V. (2003): "Information transfer among Internet firms: The case of hacker attacks", *Journal of Information Systems*, vol. 17:71-82.

FERRIS G.R.; RUSS G.; FANDT P.M. (1989): "*Politics in organizations*". In: Giacalone R.A.; Rosenfeld P.; eds. *Impression management in the organization*. Hillsdale, NJ: Lawrence Erlbaum: 143-170.

GOGAN J.; FEDOROWICZ J.; RAO A. (1999): “Assessing risks in two projects: A strategic opportunity and a necessary evil”, *Communications of the Association for Information Systems*, vol. 1:2-34.

FOMIN, V.; PEDERSEN, M. K.; & DEVRIES, H. (2008): “Open standards and government policy: Results of a Delphi study”, *Communications of AIS*, vol. 22:459-484.

GOODHUE D.; STRAUB D. (1991): “Security concerns of system users: A study of perceptions of the adequacy of security measures”, *Information & Management*, vol. 20:13-27. http://dx.doi.org/10.1016/0378-7206(91)90024-V

GREENSTEIN M.M.; HAMILTON D. (1997): “Critical factors to consider in the development of an audit client engagement decision expert support system: A Delphi study of big six practicing auditors”, *Intelligent Systems in Accounting, Finance and Management*, vol. 6:215-234.

GROVER V.; JEONG S.; KETTINGER W.; TENG J. (1995): “The implementation of business process reengineering”, *Journal of Management Information Systems*, vol.12:109-144.

HARRIS, E.; PERLROTH, N.; POPPER, N.; STOUT, S. (2014): “*A sneaky path into Target customers' wallets*”. Retrieved 1/20/2014, from http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-custome-wallets.html

HENDERSON J.; VENKATRAMAN N. (1999): “Strategic alignment: Leveraging information technology for transforming organizations”, *IBM Systems Journal*, vol. 38:472-484. http://dx.doi.org/10.1147/SJ.1999.5387096

HERMANSON D.; HILL M.; IVANCEVICH D. (2000): “Information technology-related activities of internal auditors”, *Journal of Information Systems*, vol. 14:39-53. http://dx.doi.org/10.2308/jis.2000.14.s-1.61

HOLSAPPLE C.; JOSHI K. (2001): “Organizational knowledge resources”, *Decision Support Systems*, vol. 31:39-50.

HUNTON J.; WRIGHT A.; WRIGHT S. (2004): “Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems?”, *Journal of Information Systems*, vol. 18:7-28.

IDEN, J.; LANGELAND, L. (2010): "Setting the stage for a successful ITIL adoption: A Delphi study of IT experts in the Norwegian armed forces", *Information Systems Management*, vol. 27:103-112. http://dx.doi.org/10.1080/10580531003708378

IIA.GAIT for business and IT risk. Altamonte Springs, FL: The Institute of Internal Auditors, 2008.

IIA. (2005): "*Global Technology Audit Guide - Information Technology Controls*". Altamonte Springs, FL: The Institute of Internal Auditors.

ISOTOC, S. (2011): Department of Taxation security audit leads to investigation. Retrieved 7/5/2012 from http://mauinow.com/2011/12/15/department-of-taxation-security-audit-leads-to-investigation/

ITGI.COBIT 5.0. Rolling Meadows, IL: IT Governance Institute, 2012.

JIANG J.; KLEIN G.; ELLIS T. (2002): "A measure of software development risk", *Project Management Journal*, vol. 33:30-41.

KARABACAK B.; SOGUKPINAR I. (2005): "ISRAM: Information security risk analysis method". *Computers & Security*, vol. 24:147-159.

KASI, V.; KEIL, M.; MATHIASSEN, L.;PEDERSEN, K. (2008): "The post mortem paradox: A Delphi study of IT specialist perceptions", *European Journal of Information Systems*, vol. 17:62-78. http://dx.doi.org/10.1057/palgrave.ejis.3000727

KEIL M.; TIWANA A.; BUSH A.A. (2002): "Reconciling user and project manager perceptions of IT project risk: A Delphi study", *Information Systems Journal*, vol.12:103-119.

KEMERER C.; SOSA G. (1991): "Systems development risks in strategic information systems", *Information and Software Technology*, vol. 33:212-223.

KLAMM B.; WATSON M. (2009): "SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology", *Journal of Information Systems*, vol. 23:1-23.

LINSTONE H.A.; TUROFF M. (2002): "*The Delphi method: Techniques and applications*", Addison-Wesley Publishing Co.

LIU, S.; ZHANG, J.; KEIL, M.; CHEN, T. (2010): "Comparing senior executive and project manager perceptions of IT project risk: A Chinese Delphi study, *Information Systems Journal*, vol. 20:319-355. http://dx.doi.org/10.1111/j.1365-2575.2009.00333.x

LOCH K.; CARR H.; WARKENTIN M. (1992): "Threats to information systems: Today's reality, yesterday's understanding", *MIS Quarterly*, vol. 16:275-285.

MEREDITH, J.; RATURI, A.; AMOAKO-GYAMPAH, K.; KAPLAN, K.(1989): "Alternative research paradigms in operations", *Journal of Operations Management*, vol. 8:297-327. http://dx.doi.org/10.1016/0272-6963(89)90033-8

MINTZBERG H. (1985): "The organization as political arena", *Journal of Management Studies*, vol. 22:133-154. http://dx.doi.org/10.1111/j.1467-6486.1985.tb00069.x

MINTZBERG H. (1983): "*Power in and around organizations"*. Englewood Cliffs, NJ: Prentice-Hall.

MOCK T.; SUN L.; SRIVASTAVA R.; VASARHELYI M. (2008): "An evidential reasoning approach to Sarbanes-Oxley mandated internal control risk assessment", *International Journal of Accounting Information Systems*, vol. 10:65-78. http://dx.doi.org/10.1016/j.accinf.2008.10.003

MURSU A.; LYYTINEN K.; SORIYAN H.; KORPELA M. (2003): "Identifying software project risks in Nigeria: An international comparative study". *European Journal of Information Systems*, vol. 12:182-200.

NEELY, A. (1993): "Production / operations management: Research process and content during the 1980s", *International Journal of Operations & Production Management*, vol.13:5-18. http://dx.doi.org/10.1108/01443579310023963

NIEDERMAN F.; BRANCHEU J.C. (1991): "Information systems management issues for the 1990s, *MIS Quarterly*, vol.15:475. http://dx.doi.org/10.2307/249452

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

PALIWODA S. (1983): "Predicting the future using Delphi", *Management Decision*, vol. 21:31-38. http://dx.doi.org/10.1108/eb001309

PARENT M.; REICH B. (2009): “Governing information technology risk”, *California Management Review,* vol. 51:134-152. http://dx.doi.org/10.2307/41166497

PICCOLI G.; IVES B. (2005): “IT-dependent strategic initiatives and sustained competitive advantage: A review and synthesis of the literature”, *MIS Quarterly,* vol. 29:747-776.

POPPER, N. (2012): “*Knight Capital says trading glitch cost it $440 million*”. Retrieved 12/15/2013, from http://dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (2007): “An audit of internal control over financial reporting that is integrated with an audit of financial statements”, *Auditing Standard* No. 5.

RAGHUPATHI W. Corporate governance of IT: A framework for development. *Communications of the ACM* 2007;50:94-99.

RAINER R.; SNYDER C.; CARR H. (1991): “Risk analysis for information technology”, *Journal of Management Information Systems,* vol. 8:129-147.

RAMAMOORTI S.; BAILEY A.; TRAVER R. (1999): “Risk assessment in internal auditing: A neural network approach”, *International Journal of Intelligent Systems in Accounting, Finance and Management*, vol. 8:159-173.

REICH B.H.; BENBASAT I. (2000): “Factors that influence the social dimension of alignment between business and information technology objectives”, *MIS Quarterly*, vol. 24:81. http://dx.doi.org/10.2307/3250980

ROWE, G.; WRIGHT, G. (1999): “The Delphi technique as a forecasting tool: Issues and analysis”, *International Journal of Forecasting* vol. 15:353-375.

SAREN M.; BROWLIE D. (1983): “*A review of technology forecasting techniques and their application”*. Yorkshire: MCB University Press Limited, 1983.

SCHMIDT R. (1997): “Managing Delphi surveys using nonparametric statistical techniques”, *Decision Sciences,* vol. 28:763-774.

SCHMIDT R.; LYYTINEN K.; KEIL M.; CULE P. (2001): “Identifying software project risks: An international Delphi study”, *Journal of Management Information Systems,* vol.17:5-36.

SHARMA S.; DHILLON G. (2009): “IS risk analysis: a chaos theoretic perspective”, *Issues in Information Systems*, vol. 10:552-560.

SHERER S.; ALTER S. (2004): “Information system risks and risk factors: Are they mostly about information systems?”, *Communications of the AIS*, vol.14:29-64.

SMITH H.; MCKEEN J.; STAPLES D. (2001): “Risk management in information systems: Problems and pitfalls”, *Communications of the Association for Information Systems*, vol. 7:1-29.

STRAUB D.; WELKE R. (1998): “Coping With Systems Risk: Security Planning Models for Management Decision Making”, *MIS Quarterly,* vol. 22:441-469.

SUH B.H.(2003): “The IS risk analysis based on a business model”, *Information & Management,* vol.41:149-158.http://dx.doi.org/10.1016/S0378-7206(03)00044-2

SUTTON S.; HAMPTON C. (2003): “Risk assessment in an extended enterprise environment: redefining the audit model”, *International Journal of Accounting Information Systems*, vol. 4:57-73.

SUTTON S.; KAZANCHI D.; HAMPTON C.; ARNOLD V. (2008): “Risk analysis in extended enterprise environments: Identification of critical factors in B2B e-commerce relationships”, *Journal of the Association for Information Systems,* vol.9:151-174.

TVERSKY A.; KAHNEMAN D. (1981): “The framing of decisions and the psychology of choice”, *Science* vol. 211:453-458.

TVERSKY A.; KAHNEMAN, D. (1974): “Judgment under uncertainty: Heuristics and biases”, *Science* vol.185:1124-1131.

WALSH J. (1988): “Selectivity and selective perception: An investigation of managers' belief structures and information processing”, *Academy of Management Journal*, vol. 31:873-896. http://dx.doi.org/10.2307/256343

WEBB S. (2000): “Crimes and misdemeanors: How to protect corporate information in the Internet age”, *Computers & Security*, vol. 19:128-132.

WILKIN C.; CHENHALL R. (2010): “A review of IT governance: A taxonomy to inform accounting information systems”, *Journal of Information Systems*, vol. 24:107-146. http://dx.doi.org/10.2308/jis.2010.24.2.107

WRIGHT, S.; WRIGHT, A. (2002): “Information System Assurance for Enterprise Resource Planning Systems: Unique Risk Considerations”, *Journal of Information Systems*, vol. 6:99. http://dx.doi.org/10.2308/jis.2002.16.s-1.99

YEH Q.; CHANG A. (2007): “Threats and countermeasures for information system security: A cross-industry study”, *Information & Management*, vol. 44:480-491. http://dx.doi.org/10.1016/j.im.2007.05.003

ZMUD. (1980): “Management of large software development efforts”, *MIS Quarterly*, vol. 4:45-55. http://dx.doi.org/10.2307/249336