4-2008

Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships

Steve G. Sutton
University of Central Florida

Clark Hampton
University of Central Florida

Deepak Khazanchi
University of Nebraska at Omaha, khazanchi@unomaha.edu

Vicky Arnold
University of Central Florida

Journal of the Association for Information Systems
JAIS

Special Issue

Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships *

Steve G. Sutton
College of Business Administration
University of Central Florida/
Faculty of Economics & Commerce
University of Melbourne
Steve.Sutton@bus.ucf.edu

Deepak Khazanchi
College of Information Science & Technology
University of Nebraska at Omaha
khazanchi@unomaha.edu

Clark Hampton
College of Business Administration
University of Central Florida
Clark.Hampton@bus.ucf.edu

Vicky Arnold
College of Business Administration
University of Central Florida
Faculty of Economics & Commerce
University of Melbourne
Vicky.Arnold@bus.ucf.edu

Abstract

The focus of this study is to identify the critical risk factors that can be used to assess the impact of B2B e-commerce on overall enterprise risk. We apply the Khazanchi and Sutton (2001) framework for B2B e-commerce assurance as the organizing conceptual model for the study. The framework focuses on three primary risk components: (1) technical risks, (2) application-user risks, and (3) business risks. To identify a critical set of B2B risk factors, structured focus groups applying a nominal group technique were conducted with three internal constituency groups (corporate groups consisting of IS security, internal IT audit, and e-commerce development managers) and two external constituency groups (e-commerce consultants and external IT auditors). Tests of consistency between the groups confirm strong agreement on the identified critical B2B risk factors. Tests were also conducted on participant groups' perceived relative importance of the critical B2B risk factors. The only substantial inconsistencies were between the internal constituency groups and the e-commerce consultants' group for the business risk factors. This would appear to indicate that the priorities of internal groups might be different from the e-commerce consultants who appear more focused on management support of projects than on active involvement of trading partner staff with systems integration. Subsequent testing of the three-component B2B risk assurance model with a follow-up questionnaire suggests that the identified risk factors support the model, including theorized interrelationships among the three risk components.

Keywords: *Electronic commerce, e-business, business-to-business, interorganizational systems, extended enterprise systems, business partners, systems assurance, enterprise risk management.*

* Sal March, T.S. Raghu, and Ajay Vinze were the accepting guest editors. This paper was submitted on January 31, 2007 and went through two revisions.

Volume 9, Issue 3/4, pp. 151-174, Special Issue 2008

1. Introduction

There is accumulating evidence that the benefits of B2B e-commerce relationships are predominantly produced by enhanced collaboration (Lee et al., 2003) engendered by the benefits accrued from widespread internal integration of B2B (Iacouvou et al., 1995). Despite all the perceived benefits of forging integrated business relationships, for many organizations there is still some trepidation about entering into these relationships (Iacovou et al., 1995). This trepidation can come from costs, but more frequently is a result of perceived enterprise risks. Kumar and van Dissel (1996) summarize these risks as the costs associated with exposure to being exploited in the relationship. These risks include transaction-specific capital (i.e., investment by one party that has little or no value outside of the business relationship), information asymmetries (i.e., problems in monitoring performance that lead to a risk of shirking by a business partner), and loss of resource control (i.e., resources that are transferred in a relationship that cannot be returned or controlled in the event of the relationship's termination).

These risks primarily center on loss of investment, which can have negative financial ramifications for an organization, but in most cases are not likely to cripple an organization. Yet, in an era where the focus has been on enhancing core business processes, outsourcing activities that other organizations can do better at lower cost, and developing integrated value chains, breakdowns in relationships may have far greater ramifications than simply financial losses and/or inefficiencies (Sutton and Hampton, 2003). For instance, in a just-in-time environment where a vendor is responsible for managing the materials and parts inventory, a vendor's failure to deliver parts for a prolonged period of time could lead to extended shutdowns of manufacturing processes. These interruptions could put the manufacturing company at risk due to the inability to produce goods, inability to meet obligations downstream in the supply chain, loss of other business partners' trust, and decline in general reputation. Such risks could jeopardize an organization's long-term standing. The Sarbanes-Oxley Act has brought these IT and e-commerce risks to the forefront as companies struggle to address Section 404 requirements related to reporting on internal controls. Organizations are slowly coming to the realization that requirements under Sarbanes-Oxley extend internal controls within the audit context from direct controls over financial activities to a broader enterprise risk management frame that includes strategic, operational, reputational, regulatory, and information risks (Katz, 2003; Banham, 2003). As the risk side of the equation increases as a component of assessing potential and existing B2B relationships, methods of risk mitigation become of greater interest. Various models of assurance services for assessing the IT risk of an organization have begun to evolve. Within the automotive industry, Harbinger provides reports that highlight B2B capability and the degree of integration with underlying business processes of various small- and medium-sized enterprises (SMEs) supplying major auto manufacturers. The reports help automobile manufacturers identify potential suppliers that can operate in their just-in-time manufacturing environments and more effectively monitor business risk from partner relationships (Yost, 1999). Research suggests that assurance over IT systems is valued by firm stakeholders, including organizational management (Boritz and Hunton, 2002) and financial analysts evaluating firms (Hunton et al., 2000).

The wide variety of concerns in B2B integration led Massetti and Zmud (1996) to this conclusion: "What seems absent is a rich, tactical understanding that links strategic expectations regarding [B2B] with operational plans for potential implementation." The focus of Massetti and Zmud's study was on deriving factors for assessing the benefits from B2B linkage. As interorganizational systems have become more tightly coupled, a focus on the opposite side of the equation (i.e., associated business risks) seems particularly critical. While prior research has addressed a variety of general risk factors in extended-enterprise systems linkages (e.g., Papazoglou et al., 2000; Unal, 2000; McIvor et al., 2003; Hempel and Kwong, 2001; Westland, 2002; Kumar and van Dissel, 1996), a focused effort on identifying specific risk factors within various general categories can aid managers in risk management and inform future extended-enterprise systems development and innovation.

Extant IT governance frameworks (e.g., COBIT, ITIL, ISO/IEC 17799) do not specifically provide any

guidance for assessing or addressing B2B (inter-organizational) concerns and risks associated with extended enterprise linkages (IT Governance Institute and the Office of Government Commerce, 2005). In fact, ITIL, published by the UK government, provides guidance on best practices for IT service management; COBIT, published by the IT Governance Institute (ITGI) is positioned as a high-level governance and control framework; and ISO/IEC 17799, published by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), provides a framework for information security management (IT Governance Institute and the Office of Government Commerce, 2005). The latter can be used as a "basis for developing security standards and management practices within an organization to improve reliability on information security in inter-organizational relationships" (IT Governance Institute and the Office of Government Commerce, 2005, p. 16). All the guidelines relating to this goal are tied to assessing IT-related risks (e.g., system crashes and security breaches), project risk (e.g., failure, waste), and business risk from internal circumstances rather than the cascading impact of external (B2B) linkages.

The purpose of this research is two-fold. The first is to explore and identify the critical risk factors involved in B2B e-commerce driven extended-enterprise systems that can potentially escalate an organization's overall enterprise risk. The second is to explore the interrelationships among the various B2B e-commerce risk components so as to understand how various components influence each other and affect overall risk.

Phase I of the study directly targets the identification of the critical risk factors in B2B relationships. The paper uses the Khazanchi and Sutton (2001) model for B2B e-commerce assurance as the conceptual lens for viewing specific categories of risk. We use a methodology designed to elicit the expertise of key participants in B2B core processes (Abernethy et al., 2005). Initially, we conduct three structured focus groups with information systems security officers, internal IT auditors, and e-commerce developers from three large corporations that heavily use B2B e-commerce across the value chain in order to identify the critical risks associated with these relationships and to determine whether a consensus exists across organizations as to what risk factors are critical. We conduct two additional focus groups with an e-commerce consulting firm and an external audit firm in order to explore whether differences exist between corporate teams and external professionals. The results from all five structured focus groups provide a consensus set of 49 critical risk factors across three risk dimensions: (1) technical risk, (2) application-user risk, and (3) business risk. In Phase II of the study, the 49 risk factors identified in Phase I are used to develop a risk assessment instrument. The risk assessment instrument is integrated into a questionnaire that was distributed through the Institute of Internal Auditors Research Foundation (IIARF) to members of the Institute with specific focus on soliciting participation from internal auditors, e-commerce consultants, and IS security staff for purposes of assessing the risk of a trading partner. The survey responses are used to validate the risk measures across the three risk dimensions in the model and to subsequently test the interrelationships between the three risk components.

The remainder of the paper is presented in four parts. First, we present an overview and discussion of the conceptual model for B2B e-commerce assurance. Second, we present and discuss Phase I of the research, which applies the structured focus group methodology to identify critical risk factors in B2B relationships, and the results thereof.. In the third part we present Phase II of the research, where the focus shifts to scale development and validation of the risk factors. Finally, we discuss the implications of the results for e-commerce managers and researchers.

2. Theoretical Model

Khazanchi and Sutton (2001) propose an assurance services model based on three levels of perceived B2B risk (see Figure 1): technical level risks, application-user level risks, and business level risks. The B2B assurance model initially evolved through a grounded theory approach based on an analysis of 90 small and medium sized enterprises engaged in EDI-based B2B relationships. The model was further refined using a combination of surveys, phone interviews and written descriptions from participating organizations. (See Khazanchi and Sutton (2001) for a complete description of the evolution of this model.)

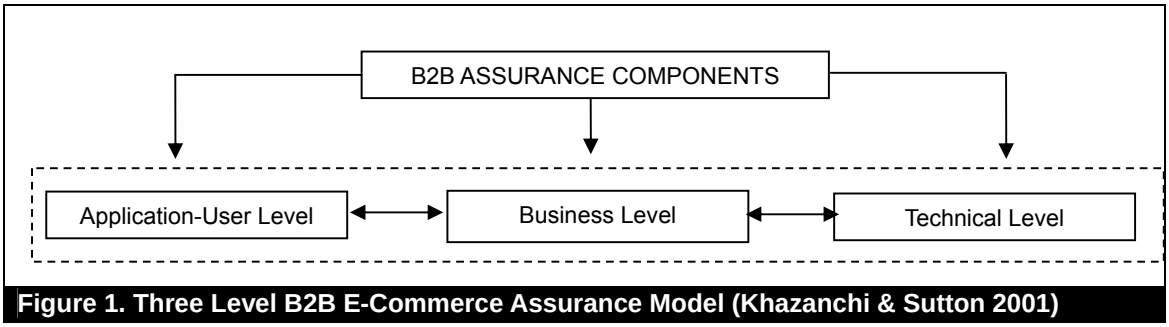

Figure 1. Three Level B2B E-Commerce Assurance Model (Khazanchi & Sutton 2001)

Technical level risks address whether technical B2B elements are in place and integration with external and internal applications is feasible with available financial and technological resources. This includes a variety of technical services such as selecting appropriate internal applications for B2B linkages, integrating multiple trading partners, mapping customer/supplier data for direct use in internal applications, ensuring business transaction processes work and include all electronic transaction sets, and using appropriate B2B intermediaries to support processes (Khazanchi and Sutton, 2001).

The application user-level risks relate to ensuring that decision makers' choices and rationale for B2B implementation are appropriate. Risks in this area focus on understanding potential benefits of B2B linkages, assessing the current business environment and internal processes, obtaining information about B2B options, assessing organizational readiness for adopting B2B, relying on paper-based transactions for internal processes, dealing with the impersonal nature of e-commerce transactions, and assessing the reliability of internal transaction processing. The adequate preparation of an organization's staff for B2B activities should be addressed, as well as related training initiatives.

Business level risks relate to an organization's ability to appropriately reengineer traditional business processes to incorporate an e-commerce driven business. These risks may center around a variety of issues including the appropriateness of e-commerce for an organization, assessment of direct/indirect benefits actually being realized from e-commerce usage, adherence to legal requirements (electronic orders, signatures, trading partner agreements, information privacy laws, etc.), proper monitoring of data and transmission security/auditability, and appropriateness of workflow procedures for achieving efficiency gains. Accordingly, internal control systems should be assessed for viability in assuring continuous monitoring of controls over privacy of data, reliability of systems, and security of electronic transmissions (Khazanchi and Sutton, 2001).

Khazanchi and Sutton (2001, p. 39) emphasize that one of the key complexities of the B2B assurance model is the interrelationships among the three risk components in the model. They further note that additional research is needed in order to understand the nature of the three components as well as the model itself, including the nature of the interrelationships among the three risk components (p. 43). In the following two sections of this paper, we shift focus to discuss a two-phased study designed to identify and understand the key risks embodied within each component and to improve understanding of the interrelationships among the three components.

Phase I: Identifying Critical Risk Factors

The three components of the B2B assurance model provide a basis for assessing risks associated with an organization's B2B e-commerce activities. While the model provides a strong conceptual foundation for examining B2B e-commerce risks, its definition is limited to broad categories of concern that might make assurance over a trading partner's B2B operations desirable (Khazanchi and Sutton, 2001). Before such assurance services can be provided, however, understanding specific underlying factors that drive risk within a given component is critical at this stage in the research.

Derivation of critical risk factors is problematic because the knowledge in complex systems is expert knowledge embedded at core operating levels as opposed to general knowledge known to top

management (Forrester, 1994; Abernethy et al., 2005). Ambrosini and Bowman (2001) note that the tacitness of knowledge is a matter of degrees and, with appropriate prompting, tacit knowledge can be tapped and made available. The knowledge often remains tacit only because nobody has attempted to articulate the knowledge, but articulation of tacit knowledge through inquiry can allow management to understand key organizational risk factors (see also Abernethy et al., 2005). This conversion of tacit expert knowledge into explicit knowledge is imperative as a first step in the design of effective measurement and/or monitoring within complex systems (Sanchez, 2001; Lorino and Tarondeau, 2002; Morecroft et al., 2002; Abernethy et al., 2005). Such a philosophy is based on the belief that the best way to understand and develop the means for effective monitoring of processes is to engage the individuals who regularly perform the process at the core operational levels (Sutton, 1993; Forester, 1994; Lampe and Sutton, 1994; Havelka et al., 1998; Abernethy et al., 2005).

In the case of B2B e-commerce activities, we identify five key constituencies as being in a position to possess tacit knowledge related to risk within B2B e-commerce relationships: three internal constituencies including e-commerce developers, IS security staff, and internal IT auditors; and two external constituencies including e-commerce consultants (who develop, implement, and maintain e-commerce systems) and external auditors (IT audit specialists who assess risk in assurance engagements). We engage participants from these constituencies in structured group processes during the study as a means of extracting their tacit knowledge to derive more explicit knowledge on key risk factors.

The research method used in the first phase of this study blends the use of focus groups with the structured approach of nominal group techniques (Van de Ven and Delbecq, 1975; 1982). An underlying premise of the methodology is that individuals who perform a task can provide valuable insights into the critical factors that drive risk in a process and can cause quality failures (Adam et al., 1986). We adapted the structured focus group process in this study from an application of the approaches used by Sutton (1993), Lampe and Sutton (1994), and Havelka et al. (1998) that blends the free flow of participant discussion from nominal group techniques with the use of structured objectives; it ultimately concludes with a Q-Sorting task that allows participants to define the actual outcomes of the session. Accordingly, we conduct four-step structured focus groups over three to four hour sessions to identify critical risk factors impacting successful e-commerce processes across the three dimensions of technical-level, application user-level, and business-level risks.

The first step in the structured focus group is an open forum by the group participants to generally discuss their individual roles, the types of applications with which they have been involved, their perspectives on the success of e-commerce ventures, and the impact of e-commerce on their particular organization's business and overall industry. This open discussion acclimates the participants and group leaders (i.e., the researchers) to the terminology used by the diverse set of participants and their general perspectives as they enter into the group discussion. It also allows time to discuss the model for e-commerce and to assure there is consensus on the meaning of the model's components.

The second step in the structured focus group consists of a silent brainstorming session at the individual level. We provide the participants with the specific component of interest (i.e., technical-, application user- or business-level risk) and ask them to identify all factors that they believe have an impact on a successful e-commerce system/process. The participants are instructed to focus on identifying all factors and not to filter out any that might not be particularly critical. The participants list their risk factors on a sheet of paper that includes a heading reminding them of the component of interest in the model at this stage of the process. The silent generation period provides time for adequate reflection, social facilitation (i.e., the tension created by watching others busily working and generating lists of risk factors), avoidance of interruption, avoidance of prematurely focusing on the first ideas generated by the group, sufficient time for search and recall, avoidance of competition, avoidance of status pressures, avoidance of conformity pressures, and avoidance of choosing between ideas prematurely (Delbecq et al., 1982).

The third step is a round-robin recording of the ideas generated. We generate an aggregate list of the

participants' identified risk factors by taking one idea from each person's list in a continuous around-the-room pattern until all participants' lists are exhausted. As each risk factor is read out, one of the group leaders types the factor into a synthesizing document that is projected to the front of the room where all participants can view the composite list of risk factors. As each risk factor is read out, participants share in forming an understandable phrase representing the factor and an agreed upon definition of the factor (which we record off-screen). The benefits of the round-robin approach include the following: equal participation in presentation of risk factor items, depersonalization of ideas as the list gets combined and grows, ability to deal with a large number of ideas, tolerance for conflicting ideas, encouragement of new risk factor generation based on fellow participants' ideas, and provision of a written record and glossary of the risk factors presented (Delbecq et al., 1982).

The fourth step is to evaluate the long list of risk factors and identify a subset of factors that are considered particularly critical to the success of e-commerce processes. Each focus group participant, at the individual level, first sorts the list of risk factors into "critical" and "not critical" factors. This process represents a Q-sorting approach (Kerlinger, 1986). Subsequently, individual participants rank each of the "critical" risks based on importance to the model component being examined. This is an extreme version of the Q-sort, whereby each item is essentially placed into a classification by itself (Sutton, 1993).

The four-step procedure is repeated for each of the three model components (i.e., technical level then application user level and then business level). After completion of the focus group, we aggregate the rankings into a composite list of critical risk factors; and we use this composite list in subsequent analysis. Fundamental to the process is the reliance on group participants to determine a risk factor's relevance to the given risk component, thus controlling the classification of risk factors by component. There is evidence to support the use of this type of method for aggregating individual rankings into a composite group rating when the intent of the research is to generate a true group preference (Huber and Delbecq, 1972; Sutton, 1993). Thus, the output of the structured focus group is a consensus set of critical risk factors for each of the components.

Participants

Completion and validation of the methodology for identifying critical B2B e-commerce risk factors requires the involvement of internal constituency groups involved in development, implementation, and evaluation of corporate B2B systems and external constituencies who facilitate the development and implementation, and/or the audit and assurance of such systems. We selected the three internal constituency groups for participation in an effort to get a diversified set of perspectives, and we chose the two external constituency groups based on the desire for additional external risk factor validation via e-commerce consultants and external IT auditors involved in assessing the impact of IT risk on overall enterprise risk. We describe the participant groups for this study in Table 1.

The five groups (three internal constituents and two external constituents) provide a rich source of data for identifying the critical B2B e-commerce risk factors. Active involvement by all group members yielded a long list of potential factors that should be considered in assessing the business risk evolving from B2B relationships with business partner organizations.

Results

The robustness of the critical risk factors identified is contingent in large part on the degree of consensus among different organizations on the identified risk factors. The validity of the structured focus groups for risk factor identification is predicated on the belief that groups from different organizations will generate similar lists of critical risk factors (Sutton, 1993; Lampe and Sutton, 1994; Havelka et al., 1998).

The first condition necessary for reliance on the identified set of critical factors is the existence of a high level of agreement among different groups in different corporate environments. We use a chi-square test of independence to test consistency in selection of critical factors. Because the chi-square test is designed to compare two groups, we test all pair-wise combinations of the three groups.

Table 1: Participant Groups

Industry	Description	Participants
Insurance Company	A large insurance company that interacts with a variety of service providers, medical entities, and co-insurance partners. HIPPA requirements add to the complexity of operations.	• Director of Internal Audit • First Executive VP of Information Systems • Senior Information Systems Auditor • Information Systems Audit Supervisor • Information Systems Manager in I/S Administration of EDI • Information Systems Manager in I/S Corporate EDI
Food Manufacturer	A large food manufacturer that uses B2B e-commerce applications to interact with all major suppliers and major customers including a number of very large chains such as Wal-Mart.	• Manager Information Safety and Security • Director Internal Audit • Director Web Application Development • Manager IT Audit • Technical Application Lead • Manager E-Mail/Web Support • E-mail/Web Support Lead
Railroad & Transport	A large railroad and transportation company that deals with a large number of customers and ancillary transportation providers. Systems must price and locate capacity upon request.	• Director Information Technologies • Manager Information Systems Auditing • Information Systems Auditor • Information Systems Auditor • Contractor—Lead on Development/Maintenance of the Pricing Exchange (considered most critical B2b application)
E-Commerce Consulting	A regional e-commerce consulting company specializing in the design and implementation of e-commerce systems.	• Lead Project Manager* for Infrastructure Implementation • Lead Project Manager for Database Management • Lead Project Manager for Application Design • Lead Project Manager Marketing Services
External Audit (Big 4)	A Big Four audit firm and consisted primarily of the partners and managers in IT audit of one region in the U.S.	• Partner-in-Charge of Northeast Region IT Audit Services • IT Audit Manager • IT Audit Manager • IT Audit Manager • IT Audit Manager • Associate CIO for Global Firm Operations

Notes: Each lead project manager is the senior person managing that e-commerce consulting function

The chi-square test of independence uses a 2x2 contingency table that focuses on commonalities (items selected/not selected by both groups—cells 1 and 4 in the contingency table) and differences (items selected by only one group—cells 2 and 3 in the contingency table). The null hypothesis underlying a chi-square test of independence is that the two sets of decisions will be independent. Rejection of the null supports the alternative hypothesis that the two groups' decisions are not independent. Results in Table 2 indicate significant agreement between all pair-wise combinations of groups in the selection of critical e-commerce risk factors.

We compare the results of the structured focus groups conducted with e-commerce consultants and external IT auditors individually with the results from the three internal constituency groups. The tests examine agreement by the e-commerce consultant group with the internal constituency groups and by the external IT auditor group with the internal constituency groups. We run tests using all pair-wise combinations of internal constituency companies with each of the external constituencies (e.g., external audit group and e-commerce consultants group) and using an aggregate ranking from all three internal constituency groups. Results for chi-square tests displayed in Table 2 indicate significant agreement by both the consulting group and the external IT audit group with internal constituency groups.

Table 2: Results of Chi-Square Test of Independence for Critical Factor Selection

Internal Constituency (Corporate) Groups	**Chi-Square**	**p-value**	**Contingency Table***	
Organization 1 vs. Organization 2	31.622	<.001	17	5
			14	38
Organization 1 vs. Organization 3	12.119	.007	18	4
			15	22
Organization 2 vs. Organization 3	11.943	.008	22	10
			11	27
External Constituency Groups				
Organization 1 vs. External Audit Group	7.548	.056	9	15
			14	24
Organization 2 vs. External Audit Group	7.116	.068	14	10
			21	24
Organization 3 vs. External Audit Group	6.695	.082	14	10
			12	23
Internal Constituency Groups in Aggregate vs. External Audit Group	48.083	<.001	19	7
			17	53
Organization 1 vs. E-Commerce Consultant Group	6.368	.095	13	13
			9	22
Organization 2 vs. E-Commerce Consultant Group	13.609	.003	18	8
			14	29
Organization 3 vs. E-Commerce Consultant Group	5.231	.156	18	8
			16	10
Internal Constituency Groups in Aggregate vs. E-commerce Consultant Group	44.567	<.001	18	9
			18	52

Notes: *The Chi-square test for independence uses a 2x2 contingency table where the top-left quadrant is "both identify as critical," the bottom right is "both identify as non-critical" and the other two quadrants are where one organization selected a factor as critical but the other didn't (i.e., "disagree on criticalness of factor"). If the chi-square is significant, independence between the groups is rejected. This rejection signifies agreement between the two groups if the "agree" quadrants are larger and disagreement between the two groups if the "disagree" quadrants are larger.

While agreement on the selection of factors captures one dimension of consistency between the groups, a second dimension should also be considered—the relative ranking placed on each identified factor. We use a Spearman's rank correlation test. Because the groups ranked each of the

Table 3: Results of Spearman Rank Correlation Tests for Internal Constituency Groups		
Technical Level	**Spearman's rho**	**p-value**
Organization 1 vs. Organization 2	.601	<.001
Organization 1 vs. Organization 3	.716	<.001
Organization 2 vs. Organization 3	.431	.003
Application-User Level		
Organization 1 vs. Organization 2	.293	.033
Organization 1 vs. Organization 3	.426	.003
Organization 2 vs. Organization 3	.443	.002
Business Level		
Organization 1 vs. Organization 2	.588	<.001
Organization 1 vs. Organization 3	.562	<.001
Organization 2 vs. Organization 3	.681	<.001

Table 4: Results of Spearman Rank Correlation Tests for External Constituencies		
Panel A: Comparisons with E-Commerce Consultants		
Technical Level	**Spearman's rho**	**p-value**
Organization 1 vs. E-Commerce Consultants	.327	.020
Organization 2 vs. E-Commerce Consultants	.405	.005
Organization 3 vs. E-Commerce Consultants	.340	.016
Internal Constituency Groups vs. E-commerce Consultants	.333	.018
Application-User Level		
Organization 1 vs. E-Commerce Consultants	.630	<.001
Organization 2 vs. E-Commerce Consultants	.645	<.001
Organization 3 vs. E-Commerce Consultants	.770	<.001
Internal Constituency Groups vs. E-commerce Consultants	.717	<.001
Business Level		
Organization 1 vs. E-Commerce Consultants	.085	.322
Organization 2 vs. E-Commerce Consultants	.123	.251
Organization 3 vs. E-Commerce Consultants	.108	.279
Internal Constituency Groups vs. E-commerce Consultants	.169	.177
Panel B: Comparisons with External Audit Firm		
Technical Level	**Spearman's rho**	**p-value**
Organization 1 vs. External IT Auditors	.252	.058
Organization 2 vs. External IT Auditors	.341	.016
Organization 3 vs. External IT Auditors	.229	.077
Internal Constituency Groups vs. External IT Auditors	.324	.021
Application-User Level		
Organization 1 vs. External IT Auditors	.170	.146
Organization 2 vs. External IT Auditors	.361	.011
Organization 3 vs. External IT Auditors	.382	.007
Internal Constituency Groups vs. External IT Auditors	.250	.060
Business Level		
Organization 1 vs. External IT Auditors	.082	.327
Organization 2 vs. External IT Auditors	.295	.051
Organization 3 vs. External IT Auditors	.264	.072
Internal Constituency Groups vs. External IT Auditors	.259	.076

three dimensions of the risk model separately, the Spearman's test must accordingly be used within each dimension. Using rank values provides greater statistical power than categorization by selected/not selected as is used in the chi-square test. We test all pair-wise combinations of the three groups. Results in Table 3 indicate significant agreement on rankings of the critical e-commerce risk factors between all pair-wise combinations of internal constituency groups.

The Spearman's rank correlation tests for agreement are also run separately for each level of the risk model to assess the agreement between each of the internal constituency groups with the e-commerce consultant group (Panel A) and the external IT auditor group (Panel B), respectively. Results in Table 4 (Panel A) indicate significant agreement on rankings of the critical B2B e-commerce risk factors between the e-commerce consultant group and the internal constituency groups for both the technical and application user risk components, but not for business risks. This lack of agreement goes beyond the aggregate selection by the internal constituency groups to a lack of significance across all three pair-wise tests with individual companies. This is an interesting result given the strong agreement across both individual company comparisons and aggregate selection comparisons for the technical and application user-level risks. A comparison of the factors generated by the groups suggests a greater focus by the consultant group on management support of projects as opposed to the corporate group's focus on active involvement of trading partners' staff and with systems integration.

Results in Table 4 (Panel B) indicate significant agreement on rankings of risk factors between the external IT audit group and the internal constituency groups for technical-, application user- and business-level risks. Interestingly, however, there appears to be less consistency between the external IT auditors and organization 1 (the railroad and transportation company). There is no particular observable reason for this difference. While there is some mixed evidence, on an overall basis, there is strong support for an agreed upon set of identified risk factors.

Discussion

While the robustness of the methodology is important for the legitimacy of the identified factors, the primary purpose of this study is to identify the critical set of factors. The five focus groups resulted in the identification of 49 critical risk factors across the three risk components—18 technical risks (see Table 5), 16 application user risks (see Table 6), and 15 business risks (see Table 7).

The identified technical risks are listed in Table 5 along with critical items identified by each participant group. Table 5 shows that eight of the 18 factors are identified by at least three of the five groups. A review of the critical factors selected by the most groups shows a broad concern over security of access to applications and networks along with the appropriate level of expertise and change management controls to ensure continued security. The concerns of external constituencies about the robustness of systems over time (both in terms of systems and personnel) are of interest; these concerns are not as prevalent among internal constituencies.

The identified application user risks along with critical items identified by each participant group are listed in Table 6. The table shows that eight of the 16 factors are identified by at least three of the five groups. The factors for this component are less concentrated than for the technical risk factors, as a broad range of application related issues are identified by multiple groups as critical, including staffing issues and management champions, architecture compatibility and capacity issues, partner benefits and market sustainability, and testing for/controls over application reliability. While the external constituencies have more unique technical risk factors (see Table 5), they appear to be more in-line with the internal constituency groups in selecting critical application user risk factors.

Table 7 lists the identified business risk factors as well as each of the participant groups' indications of whether they are critical. The table shows that the risk identification within the business component of the model yields good consistency among the groups for identification of critical factors (nine of the 15 factors are identified by three or more groups). As would be expected, a broad range of issues is covered within the business component, including regulatory, legal, cost/benefit analysis, business

Table 5: Critical Technical Level B2B E-Commerce Risk Factors

Critical Risk Factor	Transportation & Logistics Co.	Insurance Co.	Food Manufacturing Co.	E-Commerce Consultant	External IT Audit Firm
Change management processes in place to assure maintenance of security and integrity of systems as technology evolves rapidly.	•	•	•	•	
Trading partner's security over all networks and network interactions ensure transmission integrity and provide guaranteed delivery transaction to the correct trading partner.	•	•	•	•	•
Technology sophistication/expertise differential between trading partners and related selection of appropriate standards and hardware/software by the right people in this trading partner's organization.	•	•	•	•	•
Trading partner's maintenance of data accuracy during systems conversion and application usage.		•			•
Completeness and accuracy of trading partner's data processing activities.		•			
Metrics related to capacity, resiliency, and monitoring in order to better predict/control performance by trading partner.			•	•	•
Security of communication technology (infrastructure) --including vulnerability of ISP and/or public internet, vulnerability to malicious code (e.g. viruses), security vendors expected survival and the trading partner's general security model.	•	•	•		
Trading partner's vulnerability to loss of availability of data, systems, applications, etc., whether loss is accidental, intentional, or by poor design.		•	•	•	
Trading partner's setting of appropriate user profiles to assure information is appropriately compartmentalized by information types and classified by access levels.	•		•		
Controls to enforce compliance with regulatory requirements and to enforce regulations	•	•			
Comprehensive access management to applications/operating systems protected via controls (e.g. firewalls) in place to assure confidentiality, availability, and integrity (e.g. unauthorized access).	•	•	•	•	•
Channel security through appropriate controls (e.g. encryption implemented according to regulations) including validation and authentication of transaction partner.	•		•		
Ease of transition of information to new B2B systems, ease of integration with trading partner's systems, consistency in methods of partner, and ability to efficiently route B2B transactions to the right internal applications.	•	•	•	•	
Flexibility and scalability of the trading partner's system (hardware/software independence).				•	
Redundancy and failover of trading partner's systems (in relation to downtime tolerance).				•	
Adequacy of trading partner's disaster recovery plan.				•	
Adequate staff expertise available on an as-needed basis.				•	•
Comprehensive systems documentation of trading partner's systems.					•

Table 6: Critical Application-User Level B2B E-Commerce Risk Factors

Critical Risk Factor	Transportation & Logistics Company	Insurance Company	Food Manufacturing Company	E-Commerce Consultants	External IT Audit Firm
Appropriate level of training for trading partner's users and related cost constraints.	•	•	•	•	•
Will the target trading partner (TP) use a proposed B2B system (considering such issues of whether there is a champion for the project, sufficient IT sophistication to integrate within TP's systems environment, and ease of use of application)?	•	•	•	•	•
When upgrading systems based on new technologies or business partner request, the trading partner has sufficient coordination and change control procedures in place to maintain reliability and protect transaction validation procedures.	•	•	•	•	•
Trading partner's understanding of and agreement on data structure/scope/business rules for exchange of information.	•	•	•	•	
Is there benefit of B2B ventures to the trading partner and is the e-commerce marketplace sustainable?	•		•	•	
Clear and sufficient contract documentation on policies, procedures, connectivity guidelines, limitations, review plan, etc. (Service Level Agreements).		•	•	•	•
Application controls in place for completeness, accuracy, and processing integrity (i.e. trading partner's applications function as intended).		•	•	•	•
Trading partner's implementation of new B2B applications include testing for assurances on hardware/software capability to support applications, availability of supporting applications 24/7, and performance and capacity of data exchange.	•	•	•	•	•
Third party assurance of transaction validity.	•				
Marketing cost to sell the trading partner on a given B2B application	•				
Privacy of data agreements.			•		
Alignment of trading partner's business processes with implemented B2B e-commerce technologies.			•		
Adequacy of the security over access to trading partner's business application systems.		•			
Inaccurate, inadequate or outdated documentation on systems software/hardware provided by trading partner.		•			
Trading partner's inability to have an enterprise view of the full range of trading partner relationships.					•
Trust in trading partner (internal or external).					•

Table 7: Critical Business Level B2B E-Commerce Risk Factors

Critical Risk Factor	Transportation & Logistics Co.	Insurance Co.	Food Manufacturing Co.	E-Commerce Consultants	External IT Audit Firm
Understanding by trading partner (TP) of their business processes, where e-commerce fits into those processes, value of business process integration with TPs, and where benefits are derived.	•	•	•		
Trading partner's ability to assess the use/success of technology and the benefits of B2B implementation/technology investment (including return on investment).	•	•	•	•	
Trading partner's costs of meeting regulatory requirements and their organization's understanding of associated risks of non-compliance (including inter- and Intra- state compliance issues).	•	•		•	•
Trading partner's technical understanding at a level that facilitates creation of a transformational vision for change and the ability to implement successful change management strategies to achieve objectives, gain acceptance, and support sustainability of the change.		•	•		
Trading partner's understanding of the intended functionality of a system at the analysis/requirements stage and tying of the system to business processes that are evolved or engineered accordingly to meet the business objective.		•	•	•	•
Trading partner's level of adherence to contractual requirements including such things as product volume, sales prices, time/service commitments, and settlement (including legal agreements such as non-repudiation and the level of legal binding).	•	•	•		•
Trading partner's due diligence in implementing B2B relationships at the business, technology and security levels to assure users understand data classification/ownership/security when handling partner data and the partner maintains appropriate segregation of data to appropriate users.		•	•		•
Trading partner's understanding of risks associated with their projects and accordingly executing effective project management.		•	•	•	•
Trading partner's understanding of the technical complexities and associated costs of B2B development, implementation, and maintenance; and the legal ramifications, costs of implementing vs. not implementing non-repudiation agreements, costs of new business rules, and loss of personal marketing contacts.	•	•	•		•
Trading partner's team expertise for guiding all aspects of B2B e-commerce projects along with training for project teams and users.		•			•
Trading partner's broad management involvement in IT/business planning while maintaining independence in the selection of technology preferences.				•	•
Trading partner's integration of applications into organizational procedures and guidelines – including comprehensive documentation.				•	
Auditability of trading partner's system based on effective monitoring controls and audit trail (history of electronic data, updates, changes).		•		•	•
Trading partner's ability to protect a distinguished Brand in an e-commerce environment.					•
Trading partner's resilience to a business interruption.					•

process integration, due diligence, risk management, monitoring controls and management leadership in IT. Yet, despite the breadth, there is strong agreement on the critical factors affecting business risk. On the other hand, as might be expected, there is not necessarily strong agreement between internal constituencies and external constituencies as to the relative importance of the individual factors identified.

Phase II: Instrument Development, Validation & Testing

In this stage of the study, we use the 49 risk factors identified in Phase I to develop a risk assessment instrument. While Khazanchi and Sutton (2001, p. 39) emphasize the need to recognize the interrelatedness of the risk levels as reflected in Figure 1, they do not articulate a specified model of these interrelationships. However, the evolutionary development of the model through their grounded theory approach provides insights into the nature of these interrelationships.

Technical-level risk is considered to be the most fundamental risk level faced by organizations as they begin to first implement B2B e-commerce technologies and systems. Technical level risk relates specifically to whether B2B elements are in place and whether the integration with external and internal applications is feasible given available financial and technological resources (Khazanchi and Sutton, 2001, p. 20). Khazanchi and Sutton (2001, p. 37-38) note that the firms surveyed consistently identified the technical difficulties associated with implementation and integration of B2B e-commerce operations as the dominant challenge during the initial adoption stage of B2B e-commerce. Khazanchi and Sutton (2001, p. 20) also note that analysis of technical-level controls over data integrity and security are critical to reducing the likelihood of business partner and legal disputes—significant business-level risks can potentially arise over failures to safely maintain business data at the technical level.

The implications of technical-level risk to business-level risk are arguably pervasive in the overall risk assessment of B2B operations. Khazanchi and Sutton (2001, 19) note that changes in business processes to maximize benefits from B2B operations also require review of the concurrent changes in internal control systems that assure privacy of data (technical level), reliability of systems (technical and application user levels), and secure electronic transmission (technical level). Khazanchi and Sutton (19) further note that business-level risks are escalated in the presence of B2B operations involving electronic funds transfers, and complete transaction recording is imperative—both are dependent on technical- and/or application user-level activities. In their overview of the three-level model, Khazanchi and Sutton (p. 29-30) summarize the complexity of these relationships in noting,

> *Business-level issues are often more difficult to isolate in that the data collected at the business level often also has implications for either the technical level or the application user level as suggested in the preliminary assurance model.*

It should also be noted that there are direct implications of technical-level risks on application user-level risks. Khazanchi and Sutton (2001, 18) assert that demands for assurance over application user-level risks will likely come from primary customers attempting to improve their suppliers' integration because the suppliers' existing systems were ineffectively or inefficiently implemented. Khazanchi and Sutton (p. 18-19) note that this will likely arise due to "dissatisfaction with the suppliers' ability to effectively implement [B2B] systems and provide the reduced cycle time that partially motivates the move to [B2B]." The underlying B2B systems would be primarily at the technical level and would be the driving force behind failures to implement integrated systems that would reduce cycle time—an application user-level risk.

On an overall basis, the evolution of the three-component B2B risk model as documented by Khazanchi and Sutton (2001) posits that the three types of risk are interrelated and that each can impact overall risk. Figure 2 provides our conceptual model of how the interrelationships should be theorized based on the insights discussed in Khazanchi and Sutton.

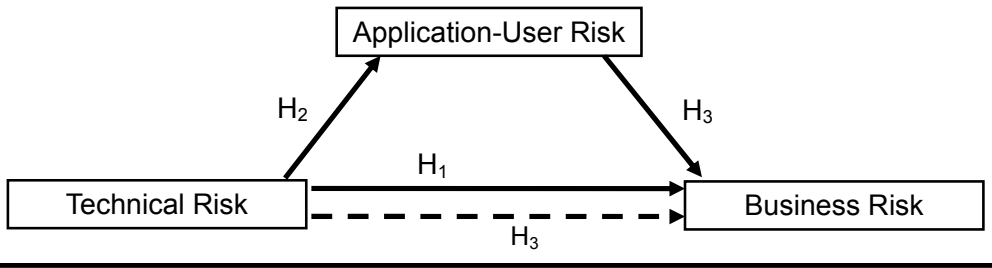

Figure 2. Conceptual Model

The model theorizes that technical-level risk is the foundation of B2B integration and is fundamental to B2B e-commerce acumen. If technical risk is high, business objectives will be difficult to meet and business risk should increase. This relationship is reflected in H_1:

H_1: An increase in B2B technical risk is positively associated with an increase in B2B business risk.

Similarly, poor technical integration through weaknesses in integration and ineffectiveness of B2B systems indicates poor understanding of integration with business processes, failure to realize the impact on business processes and application systems, and ultimately poor reliability of transaction processing. These weaknesses should increase application user risk. This relationship is reflected in

H_2: An increase in B2B technical risk is positively associated with an increase in B2B application user risk.

In turn, the inability of users to effectively and efficiently utilize B2B e-commerce systems hampers the organization's ability to enhance business process workflow efficiencies, adhere to legal and regulatory requirements, identify potential B2B integration benefits, and monitor and assess B2B activities and processes. Thus, increases in application user risk will likely result in increased business risk. This relationship, viewed in conjunction with the hypothesized technical risk/business risk relationship, implies that application user risk partially mediates the relationship between technical risk and business risk. This relationship is reflected in H_3:

H_3: B2B application user risk partially mediates the positive association between B2B technical risk and B2B business risk.

Research Method

To examine the hypothesized model put forth, we used a survey research design to assess perceived risk of business partners in a B2B relationship. The Institute of Internal Auditors Research Foundation (IIARF) hosted a web-survey and the IIARF solicited participation from a broad range of internal auditors, IS security staff, external IT audit specialists, and e-commerce developers via the IIA membership.

We measured the three risk components using an instrument consisting of the 49 risk factors identified in Phase I of the study. The instrument development consisted of adding a seven-point Likert-type scale to each risk factor. Participants evaluate the risk factors based on their organizations' relationship with an e-commerce trading partner. The scale is anchored at the end points with the phrases "Very Low Risk" and "Very High Risk."

The goal of this research was to attain evaluations of a diverse set of business partners from a wide range of companies and industries to facilitate the evaluation of the reliability of the risk assessment questionnaire. Each participant was given detailed instructions about the objectives of the research study.

Participants

We primarily solicited participants through the Institute of Internal Auditors Research Foundation

(IIARF).[1] The IIARF maintains a survey-based system with a database of Institute of Internal Auditors' members willing to be contacted for survey participation. The IIARF sent an e-mail to each of the members in the database requesting participation in an IIARF sponsored project on e-commerce risk by all such members with an interest in the area. A second request was sent a month later. Responses were acquired through completion of an online questionnaire made available through the IIARF's benchmarking site.

Forty-nine complete responses were received. The number of individuals contacted was not disclosed to us, but response rate can be assumed to be quite low given the relative complexity of the questionnaire for the respondent group and the limited percentage of contacted individuals that would actually have the e-commerce interest requested. The questionnaire also required fairly extensive information about a business partner organization that would further limit the number of potential participants. Demographics for the resulting set of participants suggest that the approach was effective in reaching the types of individuals desired as respondents to the survey (see Table 8).

Survey respondents can be classified into three groups based on organizational position and function. The first group, accounting for 61.9 percent of survey respondents, includes individuals working in an internal audit environment—half of which are information technology auditors. External auditors, at 9.5 percent of survey respondents, comprise the second group. Within the external auditor group, half of the respondents function as consultants. The third group, comprising 28.6 percent of survey respondents, consists of managers and senior level executives. The individuals within this group include operational managers, production specialists, programmers, chief accountants, and sole-proprietors. The majority of respondents (87.8 percent) are male. The most frequently occurring age range of respondents is 47 to 52 years. All respondents have some college education, with a master's degree being the most frequently completed level of education. IT experience ranged from less than a year to more than 29 years, with the most common category being 1 to 5 years.[2] Survey participants' IT-related work percentage ranges from less than 10 percent to more than 80 percent with the majority of participants indicating at least 80 percent of their daily work is related to IT functions and responsibilities.

Results

Survey responses for all variables in the questionnaire were assessed for reliability. We used Cronbach's alpha to assess scale structure prior to combining individual scale questions into single measures. All scales met recommended thresholds for scale reliability based on Cronbach's alpha: technical risks (cronbach's $\alpha = .962$), application user risks (cronbach's $\alpha = .947$), and business risks (cronbach's $\alpha = .919$).

We used Ordinary Least Squares regression to estimate links between the various exogenous and endogenous variables in the model. Overall model results in Figure 3 provide beta weights on the paths and adjusted r-squares alongside constructs representing the hypothesized dependent variables.

[1] We also contacted individuals in industry with interests in e-commerce consulting and/or e-commerce systems development, or IT audit specialization in an external audit environment, and requested they complete the IIARF online survey.

[2] Three participants had less than one year IT experience. Eliminating these individuals from our sample minimally strengthens all ordinary least squares regression results. The results reported in this paper are based on the full sample.

Table 8: Survey Respondent Demographic Data

Years Experience in IT Activities	<1	1-5	5-9	9-13	13-17	17-21	21-25	25-29	>29	No Response
	3	10	7	6	6	5	5	4	3	0
Percent of IT Related Work	<10%	10-20%	20-30%	30-40%	40-50%	50-60%	60-70%	70-80%	>80%	No Response
	2	3	3	4	4	4	3	2	23	1
Education Level	Bachelor	Master	Ph.D	Some College						No Response
	17	29	2	1						0
Age (Years)	22-27	27-32	32-37	37-42	42-47	47-52	52-57	>57		No Response
	3	4	6	4	4	10	6	5		7
Professional Certification	CIA	CPA	CISA	CFE	CDP					No Response
	17	11	24	5	5					1
Primary Work Function	External	Internal	Other							
	9.5%	61.9%	28.6%							
Gender	Female	Male								
	12.2%	87.8%								

H_1 hypothesized a positive relationship between the technical risk and business risk components. The results of the analysis are highly significant (see Table 9), with an adjusted r-square of .582 and a .769 path coefficient ($p < .001$). Accordingly, the null hypothesis is rejected and support is found for H_1.

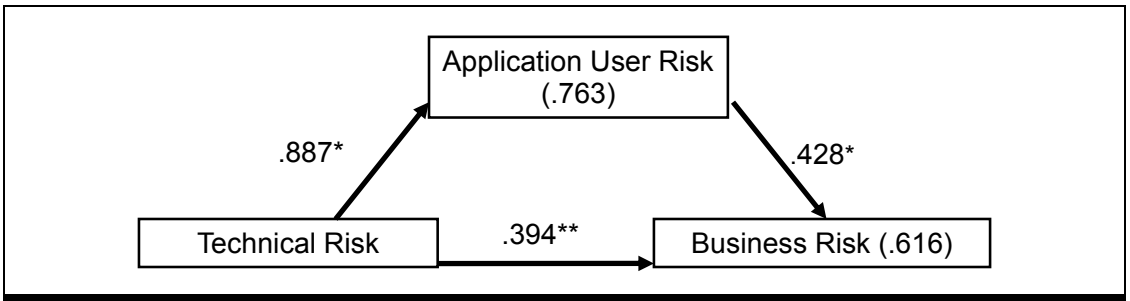

Figure 3. Model Testing Results

Note: Numbers along lines indicate path coefficients.
Numbers within variable boxes indicate adjusted R_2.
*denotes significance at the p<.05 level.
** p = .058.

Table 9: H_1 - Technical Risk to Business Risk

	Standard Error	Beta Coefficient	*t*	Significance
Constant	.340		3.620	.001
Technical Risk	.086	.769	7.618	< .001

Note: Dependent variable is Business Risk

H_2 hypothesized a positive relationship between technical risk and application user risk. Analysis indicates a positive relationship between technical risk and application user risk (see Table 10). The path coefficient of .877 is significant ($p < .001$) with an adjusted r-square of .763. Accordingly, the null hypothesis is rejected and support is found for H_2.

Table 10: H_2 - Technical Risk to Application-User Risk

	Standard Error	Beta Coefficient	*t*	Significance
Constant	.275		2.080	.044
Technical Risk	.070	.877	11.540	< .001

Note: Dependent variable is Application-User Risk

H_3 hypothesized that the positive relationship between technical risk and business-level risk is partially mediated by application user risk. We test partial mediation using the three-step approach recommended by Baron and Kenney (1986). Step one requires a significant relationship between the technical risk and business risk components—this requirement is fulfilled by the test results for H_1. Step two requires a significant relationship between the application user risk and business risk components. Regressing business risk on application user risk yields a path coefficient of .774 ($p < .001$) and an adjusted r-squared of .588. Step three tests all model relationships by regressing business risk on technical risk and application user risk. If partial mediation exists, all paths should have significant coefficients while the relationship between technical-level and business-level risk in step one diminishes but remains significant. Per Figure 3, all paths remain significant in the predicted direction. The path coefficient from technical-level risk to business-level risk decreased from .769 in step one to .394 ($p = .058$) in step three. The path coefficient from application user risk to business risk decreased from .774 in step 2 to .428 ($p = .040$) in step 3. The business risk adjusted r-square remains high at .616. To confirm the partial mediation effect, we use the Goodman I version of the Sobel test to test the hypothesized mediation effect (Baron and Kenney, 1986). The results shown in Table 11 support the existence of the hypothesized partial mediation effect (t=2.084, p=.037).

Table 11: Mediation Tests

Mediation Step	IV(s)	Standard Error	Beta Coefficient	t	Significance
1	Technical Risk	.086	.769	7.618	< .001
2	Application-User Risk	.093	.774	7.720	< .001
3	*Constant*	.343		2.922	.006
	Application User Risk	.187	.428	2.124	.040
	Technical Risk	.171	.394	1.956	.058

Note: Dependent variable is Business Risk

3. Discussion and Implications

In the emerging Internet-driven B2B environment, the true benefits appear to come from tight collaboration with trading partners (Lee et al., 2003; Cooper and Slagmulder, 2001); but at the same time, significant enterprise risks emerge from the increased dependence on a small set of trading partners (Khazanchi and Sutton, 2001; McIvor et al., 2003; Sutton and Hampton, 2003). While prior research raises many concerns and recognizes a variety of general risk factors related to the tight coupling of extended enterprise systems (e.g., Papazoglou et al., 2000; Unal, 2000; McIvor et al., 2003; Hempel and Kwong, 2001; Westland, 2002; Kumar and van Dissel, 1996), the extant research does not provide a focused examination of specific factors that can be utilized by corporate chiefs for effective enterprise risk management, nor for auditors and other monitoring organizations that evaluate the riskiness of B2B activities to the viability of the organization. In general, the extended enterprise systems research has largely avoided dealing with risk as a measurable issue. While research models have addressed risk- mitigating conventions such as trust, prior research lacks a validated instrument for partner-risk assessment in extended enterprise relationships. This research explores the critical factors associated with B2B e-commerce risk, develops and validates a research instrument for risk assessment, and tests hypothesized interrelationships between the technical, business, and application user components of B2B risk.

The research reported in Phase I of this study focuses on the identification of critical factors that can be used by management, auditors, and other related parties to monitor and assess the overall enterprise risk arising from B2B interaction with a particular focus on extended enterprise systems. The study applies the Khazanchi and Sutton (2001) three-component B2B risk assessment model, focusing across the three categories of risk: (1) technical risk, (2) application-user risk, and (3) business risk. Based on a series of structured focus groups with internal constituency groups representing information systems security, internal IT audit, and e-commerce development and representing three diverse industries, we identified a set of critical factors for each of the three components in the framework. The set of critical factors were further refined and validated using two external constituency focus groups (e.g. e-commerce consultants and external IT auditors). The results of the study show strong consistency between all of the groups in the identification of critical risk factors and strong agreement between internal constituency groups on the relative importance of factors. These statistical results support the desired objective of identifying a set of critical factors that is applicable across a broad range of organizations having concerns related to e-commerce activities. The 49 critical factors (i.e., 18 technical risks, 16 application-user risks and 15 business risk factors) provide broad coverage of the critical risk concerns while at the same time remaining relatively parsimonious.

The purpose of Phase II in the study was to validate the risk assessment instrument developed based on the results of Phase I and to test the theorized interrelationships among the risk components of the model. In the process of establishing the aforementioned relationships, the research adds empirical support for the three-component B2B assurance model and for the usability of the 49 risk measurement factors identified in Phase I to form a risk measurement instrument for future research use. The relationships between the risk components were significant and in the direction theorized

within this study based on the evolution of the model as presented in Khazanchi and Sutton (2001).

There are limitations to the research that should be considered when reviewing the output results. First, application of the structured focus group methodology necessitates the use of small groups. While we made attempts to gather data from a comprehensive set of constituencies within each of the internal and external groups, generalizations to other organization members and to other organizations cannot be assured. Second, consensus-based measures do not necessarily assure accuracy even when highly experienced and knowledgeable participants are included. Third, the use of the three- component B2B risk model provides a guiding framework for helping structure participants' thought processes, but the possibility exists that there are other risk factors that do not fall within one of these three categories. However, based on research outcomes, there was no feedback from group participants to suggest this was the case. Fourth, large organizations dominated the internal constituency participants and smaller organizations may possibly have some varying concerns. However, both external groups deal with a broad range of organizations, which helps to minimize any such risk. Fifth, the response rate to the survey was low and cannot be assured to be representative of the general population. This research was funded by the Institute of Internal Auditors Research Foundation and, accordingly, used its network of members open to survey completion. However, very few of the IIARF's surveys deal with IT-related issues; and it is expected that a very small portion of their normal respondent pool would be appropriate participants—the likely driver of the low response rate. While the sample attained was sufficient for testing the model, future studies should focus on attaining larger sample sizes that could enhance our understanding of the generalizability of the research. Nonetheless, the research presented here provides the additional information necessary to better understand the relative importance of various risk factors mentioned in various publications and provides guidance to managers, e-commerce developers, and auditors on the selection of a more parsimonious set of factors that captures the critical risk dimensions.

Our results should be of particular value to both corporate chief officers in addressing enterprise risk management concerns and e-commerce managers concerned with secure and effective extended enterprise systems. While the risk measurement instruments provide a specific means for assessing B2B risks, the specific measures to be used in assessing risk across the three components in the overall B2B risk model should be tailored to the specific extended enterprise system of interest. Consideration should also be given to which risk measures might be automated, which risk measures require human monitoring, and how this human monitoring might take place. For those measures that can be automated, continuous assurance mechanisms should be considered. This type of automated continuous assurance would seem particularly feasible at the technical level. For those factors requiring human monitoring, consideration should be given to whether such monitoring is possible and most desirable from internal IT auditors, external auditors, or other independent providers that assure/certify trading partners. The key is that it would appear to be critical that corporate chief officers and information systems managers consider the risks that exude from interorganizational systems and take appropriate steps to mitigate such risks to an acceptable level.

The factors should also be of assistance in helping corporate managers establish a balance between tight partnering relationships and resulting enterprise risk exposure. The development of a metric to assist in evaluating current and potential trading partners will help such managers evaluate the absorbed risk and facilitate a portfolio risk management approach to control the overall resulting extended enterprise risk. Similarly, assessment of the critical risk factors should provide guidance in designing new B2B applications and in establishing new trading partner relationships.

With the recent global spate of corporate frauds and mismanagement, there is certainly a heightened focus on overall enterprise risk management. The focus on enterprise risk management goes beyond just the concerns of corporate chief officers to the auditors who are saddled with the responsibility to protect the public interest. The results of this study provide a framework of e-commerce risk factors that should be considered under the broad guidelines of the IFAC audit statements on e-commerce risk assessment (e.g., IFAC, 2002a; 2002b). Clearly, contemporary audit approaches that are focused on business measurement and enterprise risk models should include consideration of the risks absorbed from such extended enterprise relationships. Furthermore, the results of this study may be

useful for extending extant IT governance frameworks (e.g., COBIT, ITIL, ISO/IEC 17799), which do not specifically provide any guidelines for assessing or addressing B2B (inter-organizational) concerns and risks associated with extended enterprise linkages (IT Governance Institute and the Office of Government Commerce, 2005).

There are also implications for researchers, as further research on extended enterprise systems risk is still of great need. While the research presented in this paper documents specific risk factors across each of the three components of the B2B risk model, there may be other characteristics of trading partner relationships that provide insight into why such risks fluctuate. For instance, Hart and Saunders (1997) found that differences in trust and power within EDI-based relationships were related to the diversity of transactions used between trading partners, and imbalances could affect voluntary use of EDI. There are likely many other factors that may affect risk, and exploration of these relationships should be beneficial to both research in the area and managers participating in B2B e-commerce arrangements. Understanding these relationships would be highly beneficial in attempts to control variations in risks that may affect overall enterprise risk—particularly to the degree that such factors help assess risks associated with a potential trading partner prior to entering into a relationship.

Finally, future research should consider the relationship between business partner risks and the desirability of proposed assurance processes, as well as the impact on relationship satisfaction with a given trading partner. Consideration should also be given to other influences on the B2B trading relationship in extended enterprise systems environments that may influence assurance desirability and relationship satisfaction. Such research would also shed additional light on the importance of B2B e-commerce business partner risk relative to these other influencing factors in affecting managers' perceptions.

Acknowledgements

We gratefully acknowledge financial support from the Institute of Internal Auditors Research Foundation. This paper has benefited greatly from the comments on earlier drafts of portions presented at the Fourth Annual CABIT Symposium, Rutgers Continuous Assurance and Reporting Symposiums, Boston Accounting Research Colloquium, American Accounting Association Annual Meetings, University of Waterloo Symposium on Governance, Transparency and Integrity: The Role of IT, University of Central Florida workshop series, and in particular Jonathan Andrews, David Bateman, Jean Bedard, James Bierstaker, James Courtney, Peggy Dwyer, Jane Fedorowicz, Mihir Pahtik, Robin Roberts, Arnold Wright, and Sally Wright.

References

Abernethy, M.A., M. Horne, A.M. Lillis, M.A. Malina, F.H. Selto (2005) "A multi-method approach to building causal performance maps from expert knowledge," *Management Accounting Research* (16), pp. 135-155.

Adam, E.E., Jr., Hershauer, J. and Ruch, W. (1986) *Productivity and Quality Measurement as a Basis for Improvement.* Columbia, Missouri: University of Missouri College of Business Research Center.

Ambrosini, V., and C. Bowman (2001) "Tacit knowledge: some suggestions for operationalization," *Journal of Management Studies* (38), pp. 811-829.

Banham, R. (2003) "Fear Factor: Sarbanes-Oxley Offers One More Reason To Tackle Enterprise Risk Management," *CFO Magazine* (June 1).

Baron, R.M., and D.A. Kenny (1986) "The moderator-mediator variable distinction in social psychological research," *Journal of Personality and Social Psychology* (51), pp. 1173-1182.

Cooper, R. and R. Slagmulder (2004) "Interorganizational Cost Management and Relational Context," *Accounting Organizations and Society* (29), pp. 1-26.

Delbecq, A.L., A.H. Van de Ven, and D.H. Gustafson (1975) *Group Techniques for Program Planning: a Guide to Nominal Group and Delphi Processes*. Glenview, IL: Scott, Foresman and Company.

Delbecq, A.L., A.H. Van de Ven, and D.H. Gustafson (1982) "Guidelines for conducting NGT meetings," in D.R. Hampton, C.E. Summer, and R.A. Webber (eds.) *Organizational Behavior and the Practice of Management,* 4th edition, Glenview, IL: Scott, Foresman, and Company, pp. 279- Forrester, J. (1994) "Policies, decisions, and information sources for modeling" in J. Morecroft, J. Sterman (eds.) *Modeling for Learning Organizations,* Portland: Productivity Press, pp. 51-84.

Grover, V., J.T.C. Teng, and K.D. Fiedler (2002) "Investigating the role of information technology in building buyer-supplier relationships," *Journal of the Association for Information Systems* (3), pp. 217-245.

Hart P.J. and C.S. Saunders (1997) "Power and trust: critical factors in the adoption and use of electronic data interchange," *Organization Science* (8) 1, pp. 23-42

Havelka, D., S.G. Sutton, and V. Arnold (1998) "A methodology for developing measurement criteria for assurance services: an application in information systems assurance," *Auditing, A Journal of Practice & Theory* (17), pp. 73-92.

Hempel, P.S. and Y.K. Kwong (2001) "B2B e-commerce in emerging economies: i-metal.com's non-ferrous metals exchange in China," *Journal of Strategic Information Systems* (10), pp. 335-355.

Huber, G. and A.L. Delbecq (1972) "Guidelines for combining the judgements of individual group members in decision conferences," *Academy of Management Journal* (15), pp. 161-174.

IFAC (2002a) *e-Business and the Accountant*, (International Federation of Accountants), March.

IFAC (2002b) *International Audit Practice Statement 1013,* (International Federation of Accountants).

Iacovou, C.L., I. Benbasat, and A.S. Dexter (1995) "Electronic data interchange and small organizations: adoption and impact of technology," *MIS Quarterly* (December), pp. 465-485.

IT Governance Institute and the Office of Government Commerce. *Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit: A Management Briefing from the IT Governance Institute and the Office of Government Commerce*, 2005. Available at URL: http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22493, Last Accessed: May 22nd, 2007.

Katz, D.M. (2003) "What you don't know about Sarbanes-Oxley: snares, pitfalls, and trapdoors." *CFO.com* (April 22).

Kerlinger, F. (1973) *Foundations of Behavioral Research*, New York: Holt, Rinehart, and Winston.

Khazanchi, D. and S.G. Sutton (2001) "Assurance services for business-to-business electronic commerce: a framework and implications," *Journal of the Association for Information Systems* (1), pp. 1-53.

Kumar, K. and H.G. van Dissel (1996) "Sustainable collaboration: managing conflict and cooperation in interorganizational systems," *MIS Quarterly* (September), pp. 279-300.

298.

Lampe, J.C. and S.G. Sutton (1994) "Evaluating the work of internal audit: a comparison of standards and empirical evidence," *Accounting and Business Research* (Autumn), pp. 335-348.

Lee, S.C., B.Y. Pak, and H.G. Lee (2003) "Business value of B2B electronic commerce: the critical role of inter-firm collaboration," *Electronic Commerce Research and Applications* (1), www.ComputerScienceWeb.com.

Lorino, P. and J.C. Tarondeau (2002) "From resources to processes in competence-based strategic management," in J. Morecroft, R. Sanchez, A. Heene (eds.) *Systems Perspectives on Resources, Capabilities, and Management Processes, Advanced Series in Management,* Amsterdam: Pergamon, pp. 127-152.

Massetti, B. and R. Zmud (1996) "Measuring the extent of EDI usage in complex organizations: strategies and illustrative examples," *MIS Quarterly* (September), pp. 331-345.

Morecroft, J., R. Sanchez, and A. Heene (eds.) (2002) *Systems Perspectives on Resources, Capabilities, and Management Processes, Advanced Series in Management*. Amsterdam: Pergamon.

McIvor, R., P. Humphreys, and L. McCurry (2003) "Electronic commerce: supporting collaboration in the supply chain?" *Journal of Materials Processing Technology* (6736), pp. 1-6.

Papazoglou, M.P., P. Ribbers, and A. Tsalgatidou (2000) "Integrated value chains and their implications from a business and technology standpoint," *Decision Support Systems* (29), pp. 323-342.

Sanchez, R. (ed.) (2001) *Knowledge Management and Organizational Competence.* Oxford: Oxford University Press.
Sutton, S. G. (1993) "Toward an understanding of the factors affecting audit quality," *Decision Sciences* (January-February), pp. 88-105.
Sutton, S.G. and C. Hampton. (2003) "Risk assessment in an extended enterprise environment: re-defining the audit model. *International Journal of Accounting Information Systems* (4) 1, pp. 57-73.
Ünal, A. (2000) "Electronic commerce and multi-enterprise supply/value/business chains," *Information Sciences* (127), pp. 63-68.
Westland, J.C. (2002) "Transaction risk in electronic commerce," *Decision Support Systems* (33), pp. 87-103.

About the Authors

Steve G. Sutton is KPMG Professor in the Dixon School of Accounting at the University of Central Florida and Professorial Fellow in Accounting & Business Information Systems at the University of Melbourne. He currently serves as the editor of the *International Journal of Accounting Information Systems* and formerly served as a departmental editor for *DATABASE for Advances in Information Systems.* His current research focus is on the impact of intelligent decision aids on human judgment and decision-making, and assurance models for electronic commerce in business-to-business relationships. His research appears in *MIS Quarterly, Decision Sciences, Journal of the Association for Information Systems, DATABASE of Advances in Information Systems, Auditing: A Journal of Practice and Theory, Journal of the American Taxation Association, Accounting and Business Research, Accounting and Finance, Behavioral Research in Accounting, International Journal of Intelligent Systems in Accounting Finance & Management, Journal of Emerging Technologies in Accounting, Journal of Information Systems,* among others. He is also the author/editor for four research monographs. Professor Sutton was the founding president for AIS (SIG-ASYS) and a past chair of the AAA Information Systems Section.

Deepak Khazanchi is Associate Dean for Academic Affairs and Professor of Information Systems and Quantitative Analysis in The Peter Kiewit Institute's College of Information Science & Technology at the University of Nebraska in Omaha. Dr. Khazanchi's current research interests are focused in the areas of virtual project management, project management best practices, B2B assurance services and risk analysis in extended enterprise environments and the application of philosophy of science in the Information Systems discipline. His research has been published in various peer-reviewed journals including *Communications of the Association of Information Systems, Journal of the Association of Information Systems, Decision Support Systems*, *Information Systems Management*, *Journal of Information Technology Management, ACM's DATA BASE for Advances in Information Systems, Journal of Computer Information Systems, and Information Processing and Management*. Professor Khazanchi has also made numerous presentations in national/international peer-reviewed conferences and given practitioner-oriented talks/seminars to companies and organizations in the USA and Norway on topics ranging from issues in global project management, best practices in IT project management, and patterns of virtual project management. He is the current President of the Midwest Association for Information Systems and founding President of the AIS Special Interest Group for IT Project Management (http://www.SIGITProjMgmt.org).

Clark J. Hampton, MSA, is a Ph.D. student in accounting information systems at the University of Central Florida. He completed his MSA at Texas Tech University with a concentration in Accounting Systems Design and Control. His internal audit, information systems, and management experiences with Marriott Corporation, American Restaurant Group, Sexton Enterprises, Duke Energy, and Texas Tech University (Department of Internal Audit) provide a foundation for his continuing educational pursuits and research interests in accounting information systems and auditing. His research has been published in the *International Journal of Accounting Information Systems* and presented at the Continuous Auditing Research Symposium, Boston Accounting Research Colloquium, University of Waterloo Symposium on Corporate Governance and IT, and American Accounting Association Annual Meetings.

Vicky Arnold is Ernst & Young Professor in the Dixon School of Accounting at the University of Central Florida and Professorial Fellow in Accounting & Business Information Systems at the University of Melbourne; she currently serves as editor of *Advances in Accounting Behavioral Research* and associate editor of *International Journal of Accounting Information Systems*. She recently co-edited a monograph for the Information Systems section of the American Accounting Association entitled *Researching Accounting as an Information Systems Discipline*. Her research interests are in judgment and decision-making and the impact of information technology on decision making by individuals, organizations and society. Her research appears in *MIS Quarterly, DATABASE of Advances in Information Systems*, *International Journal of Accounting Information Systems, Journal of Information Systems, Journal of Emerging Technologies in Accounting, Accounting and Finance; Advances in Accounting Behavioral Research; Advances in Accounting Information Systems; Auditing: A Journal of Practice and Theory; Behavioral Research in Accounting; Critical Perspectives on Accounting; International Journal of Intelligent Systems in Accounting, Finance and Management, Issues in Accounting Education, Journal of American Taxation Association,* and *Research on Accounting Ethics*, among others.

Journal of the Association for Information Systems
ISSN: 1536-9323