The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1741-0398.htm

Extended-enterprise systems' impact on enterprise risk management

Steve G. Sutton
University of Central Florida, Orlando, Florida, USA and
The University of Melbourne, Melbourne, Australia

Abstract

Purpose – This article aims to focus on raising awareness of the limitations of traditional "enterprise-centric" views of enterprise risk management that ignore the risks that are inherited from key business and supply chain partners. In essence, enterprise systems implementations have allowed organizations to couple their operations more tightly with other business partners, particularly in the area of supply chain management, and in the process enterprise systems applications are redefining the boundaries of the entity in terms of risk management concerns and the scope of financial audits.

Design/methodology/approach – The prior literature that has begun to explore aspects of assessing key risk components in these relationships is reviewed with an eye to highlighting the limitations of what is understood about risk in interorganizational relationships. This analysis of the prior research establishes the basis for the logical formation of a framework for future enterprise risk management research in the area of e-commerce relationships.

Findings – Conclusions focus on the overall framework of risks that should be considered when interorganizational relationships are critical to an enterprise's operations and advocate an "extended-enterprise" view of enterprise risk management.

Research limitations/implications – The framework introduced in this paper provides guidance for future research in the area of interorganizational systems control and risk assessment.

Practical implications – The framework further highlights areas of risk that auditors and corporate risk managers should consider in assessing the risk inherited through interorganizational relationships.

Originality/value – The paper highlights the need to shift from an enterprise-centric view of risk management to an extended-enterprise risk management view.

Keywords Manufacturing resource planning, Electronic commerce, Risk management

Paper type Literature review

Introduction

As enterprises in the public, private and governmental sectors all faced the great unknown as to how many of their information systems would fail when the date rolled over to the year 2000 (i.e. the Y2K problem), their was an escalation of enterprise systems[1] implementations – many based on rapid application deployment schedules. Rapid application deployment, along with many ill-conceived and/or poorly planned implementations, led to widely reported failures of systems that either failed to adequately capture and process enterprise information, or failed to support critical business processes. Less widely reported was a booming business in the subsequent years for the large public accountancy firms focusing on the integration of improved internal controls within previously implemented enterprise systems – including basic security features that were often never activated during the original implementation process.

Journal of Enterprise Information Management
Vol. 19 No. 1, 2006
pp. 97-114

1741-0398
DOI 10.1108/17410390610636904

Post-Y2K deployment of enterprise systems, enterprises became much more focused on leveraging these systems using business-to-business (B2B) software products that integrated with the enterprise systems software and facilitated tighter linkages with upstream and downstream supply chain partners. The integration of internal information systems also facilitated the outsourcing of operations that were not considered core competencies of the enterprise as external linkages, or interorganizational systems, allowed easier sharing of information electronically between partnering organizations. However, once again these interorganizational systems were frequently implemented without adequate consideration of the impact on enterprise risk and the necessary changes that should be made to systems of internal controls and more importantly, enterprise risk management policies and procedures.

The recent escalation of corporate failures and the concurrent realization that corporate governance practices were largely inadequate at many companies has led to radical changes in regulatory requirements. The speed of the changes in corporate governance attention has been fueled by the passage of the Sarbanes-Oxley Act (SOX) in the USA. SOX mandates an annual review of a public company's system of internal controls and overall enterprise risk management policies and procedures as a part of the annual financial statement audit[2]. The resultant cost has been extremely high with several large companies receiving adverse opinions reflecting inadequate systems of controls (e.g. Kodak).

While the focus of SOX investigations have forced companies to take a hard look at their corporate governance practices, the focus to date has been largely enterprise-centric and has only touched the surface of the risks embedded in IT-based systems. Still, with the requirement that the chief executive officer (CEO) sign off on the adequacy of internal controls (potentially facing both criminal and civil actions for inadequate corporate governance practices), IT-based systems are considered to be the next major area of focus and review in year two of SOX reporting. The impact of SOX has been to re-shape the roles of multiple involved parties, including among others:

- CEOs who have become much more focused on corporate governance and who have largely mandated that internal audit staffs focus almost entirely on internal control reviews.
- CIOs who have experienced a substantial change in their primary responsibilities as CEOs and board of directors mandate that CIOs invest substantial effort by their IT staffs to integrate, enhance and document internal controls for IT-based systems.
- Corporate auditors (e.g. public accountants) who have experience rapid growth in work, a shortage of new hires needed to complete the work, and whose work has become dominated by internal control review and assessment of corporate risk management procedures.

This paper contributes to the dialog on enterprise risk management in three important ways. First, the enterprise-centric view of contemporary risk management approaches is challenged with an extended-enterprise systems view advocated. An extended-enterprise systems view suggests that the boundaries for evaluation and management of risk should extend beyond just the enterprise or company to include the risks that are inherited from the myriad of interorganizational relationships that

represent upstream and downstream trading partners in the supply chain, outsourcers, and other electronically connected business partners. Second, the contemporary professional literature and related academic research is reviewed to provide insight into what guidance is currently available to CEOs, CIOs, auditors and other stakeholders impacted by IT corporate governance mandates. Third, the limitations in extant research to support all of these stakeholders' understanding of how to effectively implement effective IT corporate governance in an extended-enterprise systems environment are explored and an agenda for future research put forth.

The remainder of this paper is presented in four sections. The first section explores the issues of interorganizational relationships in greater detail to highlight the types of risk that can arise. The next section focuses on the extended-enterprise and the nature of the interrelationships that arise in the myriad of e-commerce relationships. The third section provides a fairly detailed review of the current professional literature on IT corporate governance frameworks and guidance along with the extant academic research supporting development and evolution of the frameworks. The final section summarizes the discussion and presents an agenda for future research that can facilitate the evolution of IT corporate governance practices and related audit procedures for assessing the adequacy of such practices.

Background

In the contemporary business environment, corporate enterprises find themselves facing a myriad of challenges that threaten their ability to continue to operate successfully and ensure future survival. First, recent corporate scandals have increased the pressure on top management to improve corporate governance, enhance the effectiveness of internal control systems and to effectively communicate to board of directors and shareholders how they are achieving effective governance and control. This pressure has increased in part due to the USA passing of the Sarbanes-Oxley Act placing an increased burden of responsibility on top management and mandating reporting on internal control systems that go beyond just financial accounting controls. While this Act only directly impacts US entities, it has had more of a global impact as non-US companies wishing to participate in the US stock exchanges have been forced to meet the same guidelines. This has put pressure on other countries to address the same issues and has led to changes in the European Union, Canada and Australia.

The second major factor has been the ever-increasing global market that corporate entities find themselves competing. Competing in the global market has intensified the need to cut costs and generally improve efficiency. The result has been a decade long focus on outsourcing non-strategic components of corporate enterprises' operations, leveraging partnering relationships with other organizations to streamline supply chains, focusing on just-in-time operations that minimize inventory carrying costs, and reducing internal operations to one's own core competencies where there are competitive advantages. The primary catalyst for these movements toward efficiency gains has been the use of enterprise systems to streamline internal operations and B2B e-commerce technologies that facilitate the tight linkages with external organizations.

When viewing both of these factors together (corporate governance accountability and global competition leading to tight linkages with partner enterprises), many corporate enterprises have also turned to outsourcing and partnering relationships in order to shed internal operations that might add complexity to corporate governance processes. The

problem is that shedding these internal responsibilities and focusing on streamlined supply chains do not mean that an organization also sheds the risks – indeed; it could be argued that the risks are less controllable. Consider the following examples:

- In May 2002, Ford Motor Company revealed that someone posing as one of their employees "collected the work and home addresses, social security numbers, account numbers and credit histories of 13,000 people from (one of their credit bureaus" (Vijayan, 2002). The imposter was a worker on the help desk for the software provider that served as the outsourcer for Ford's credit checking process for customer approvals. The imposter used user codes and passwords taken over the system to order credit histories. Ford's credit branch was billed for the credit reports and the imposter sold the reports to an identity theft ring leading to the then largest case of identity theft ever – totaling over US$10 million (Ghahremani, 2003). Ford fell victim to the fraudulent act while having no real control over the processes that were circumvented.
- Examples of supply chain failures and the impact it can have on organizations are frequent in the literature with two of the more publicized being Nike Inc.'s May, 2001 crisis when reported sales for the prior quarter had to be reduced by $100 million because of confusion in its supply chain and the even larger hit taken by Cisco Systems Inc. when $2.2 billion was written off for unusable inventory resulting from problems in the supply chain. The impact on the financial statements is only part of the story, however, when one also considers Nike's stock dropped 20 percent in value after its announcement. Indeed, studies show that a drop of 7.5 percent upon announcement of supply chain interruptions is average and a drop of 18.5 percent is typical over the 12-month period following the announcement (Taylor, 2003).

The risks run deep. Corporate enterprises are now relying increasingly on the internet to implement B2B e-commerce solutions in the hope of further significant reductions in costs across the supply chain. As a result, organizations are increasing their dependence on both upstream and downstream business partners to optimize production schedules and minimize inventories on hand. The goal is to maximize efficiencies, but significant business risks are associated with the increased dependence on business partners to shorten cycle times and deliver materials and supplies on increasingly shorter notice for just-in-time needs. These business partnering organizations may not be able to effectively implement new business processes that enable them to use new technologies – restricting future efficiency gains and placing all enterprises at risk both upstream and downstream in the supply chain (Arnold *et al.*, 2004). Enterprises can outsource the processes, but they cannot outsource the risks associated with work stoppages and supply chain disruptions – nor can they outsource the responsibility for controls over the information flowing across these supply chains into the financial statements (Ernst & Young, 2004). Contemporary enterprise risk management practices are hampered by enterprises' limited understanding of the scope of the risks involved in B2B e-commerce relationships with business partners and the concurrent false sense of security that these outside organizations will have strong controls over their business processes and enterprise systems.

The guidance provided to these enterprises through standards setters and professional bodies' efforts to support improved governance practices only facilitates

and potentially exacerbates the problem. Both standards setters and professional bodies continue to take this same enterprise centric view of enterprise risk management in the formulation of guidance documents and standards. There appears to be an across the board failure to recognize that yesterday's enterprise centric models are no longer applicable in today's extended-enterprise business models. Competition based on supply chain versus supply chain mandates that protection of investors, customer, employees and other stakeholders of an enterprise take on an extended-enterprise risk management focus.

Extended-enterprise systems

As noted in the introduction, the traditional model of one enterprise competing against another enterprise is rapidly becoming extinct with the focus shifting to one enterprise's supply chain competing against another enterprise's supply chain. The steady move towards outsourcing core functions, developing tightly coupled relationships with select vendors and customers, and utilizing advanced B2B e-commerce technologies to link enterprises across the supply chain creates a co-dependency among the various members of the supply chain. The major automobile manufacturers have become renowned for requiring all suppliers to provide electronic data interchange (EDI) capability to support information and payment flows.

A recent PricewaterhouseCoopers CEO risk study indicates that CEOs as a whole continue to increase their emphasis on the outsourcing of core business processes. The surveyed CEOs emphasized the primary drivers of improved costs control, reduced number of employees that must be managed, and in particular enhanced quality through competition for service provision. Over 70 percent of the CEOs viewed outsourcing as a long-term phenomenon that was important strategically to their organizations (PricewaterhouseCoopers, 2004). The cost side of outsourcing is often cited. NOL (Singapore) and Agilent Technologies were both reported recently to have savings from outsourcing the core accounting and finance functions of around US$100 million. NOL's manager also suggests that outsourcing the accounting and finance function really means that an enterprise with about US$5.5 billion in sales only needs an accounting and finance staff of maybe 50 people total – certainly no more than maybe 10 each in treasury, management accounting and financial accounting. Further, Gartner reports a 65 percent growth in business process outsourcing during 2003 (Ramos, 2004).

While both the costs savings and the reductions in staffing are significant, ultimately the quality may be too early to tell. Further, the risk model of failure, loss of data, or poor quality is relatively unknown and unstudied. The core problem is that in the rush to outsource core functions to save money, the vast majority of enterprises have retained an enterprise centric view of IT systems, IT control and IT governance. Yet, failure in these core processes that have been outsourced can radically impact the enterprise's operations. Can an organization weather a failure in its accounting systems? A loss of accounts receivables data? Accounts payable? If the outsourcer fails or does not have secure systems and data is corrupted, the enterprise using the outsourcer still has significant business risk. Further, this business risk is inherited by the enterprise's business partners throughout the supply chain. If the enterprise has a disruption in its systems the resulting delays could ripple across the supply chain and cause disruptions for potentially all partnering enterprises upstream and downstream.

This enterprise centric view of IT systems, IT control and IT governance is even more disconcerting when considering the linkages with business partners across the supply chain. In this enterprise centric view of IT, each enterprise is responsible for its own systems with the focus being only on compatibility in sending and receiving information electronically with other members of the supply chain. In recent years, some organizations have also begun to share their production planning systems data in a manner that allows other members of the supply chain to reduce their own inventory stocks and move towards a truer just-in-time mode across the supply chain. This escalates risk, however, as an enterprise lacks reliable information on the information processing capabilities and security of business partners' internal business processing systems and external e-business integration systems. Thus, an enterprise cannot assess the level of risk it absorbs as a member of a supply chain – both from a supply chain disruption perspective and from a safeguarding of shared information perspective (Sutton and Hampton, 2003).

The lack of control that an enterprise has over its business partners in the supply chain escalates the importance of selecting and retaining the right business partners as strategies for reducing business cycle time are integrated into supply chain processes (e.g. vendor managed inventory (VMI), just-in-time (JIT) manufacturing, and quick response retailing (QR)) (Khazanchi and Sutton, 2001; Grieger, 2003). Selection and retention of supply chain partners should be carefully executed in light of the capabilities such partners have to integrate strategic technologies, integrate such technologies with internal business processes, and seamlessly integrate IT systems with other supply chain partners. While the process of such integration can be very taxing, such integration can also lock in viable supply chain partners and provide stability in supply chain partner relationships (Grover *et al.*, 2002; Shin and Leem, 2002).

While the focus on identifying appropriate, reliable supply chain partners may seem completely logical, in many cases an enterprise's business partners are clearly not prepared to operate in a collaborative B2B e-commerce environment. These shortfalls can arise from a variety of areas including primarily technical capability/competence, IT security, and/or IT integration with existing business processes. Some enterprises have elected to maintain existing relationships and simply use their power in the relationship to force the business partner to adopt e-commerce technologies. Research tells us that forcing vendors to implement B2B e-commerce capability impacts trust in the relationship and can inhibit voluntary integration beyond that which is mandated and can often lead to a conflict situation where the relationship degenerates rapidly yielding less rather than more collaboration (Hart and Saunders, 1997; Kumar and van Dissel, 1996). Regardless, the contemporary state of supply chain competition mandates B2B e-commerce integration goes forward and an organization is faced with addressing issues in current relationships or attempting to select alternative business partners that can provide the desired supply chain efficiencies (Angeles and Ravinder, 2000).

The problem is, how does one know a potential trading partner has the IT systems and capabilities to meet supply chain demands? What criteria does an enterprise use to select supply chain partners? How does the enterprise know its partners' systems are reliable? Secure? How do these B2B e-commerce relationships and IT linkages impact the enterprises risk management processes?

Professional guidance and standards

The International Federation of Accountants (IFAC) is the principle international audit standards setting body. Within the IT realm, the Information Systems Audit and Control Association (ISACA) has also been proactive on an international basis in terms of providing guidance to management and auditors on effective IT governance and control frameworks. In some cases, the two organizations have worked together in the development of guidance for managing IT (e.g. IFAC, 1999; ISACA, 2001; IT Governance Institute, 2001). In this section, the guidance for management and auditors are each reviewed.

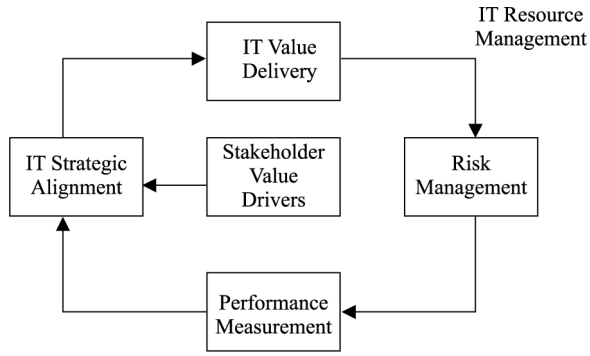
Corporate governance over IT

IFAC provides a central distribution point for guidance on IT governance, bringing together the contemporary thinking of multiple bodies on strategies for establishing corporate governance over IT. In an early guideline issued for executive management, IFAC focused on the IT planning process and the importance of focusing IT investments on strategic alignment (IFAC, 1999). The guidelines focus on several core principles for IT planning, including:

(1) alignment with business direction of enterprise;
(2) relevance of planning scope;
(3) relevance of planning timeline;
(4) identification of how benefits will be realized;
(5) achievability of plan;
(6) basis for measuring and monitoring performance;
(7) period reassessment of plan;
(8) dissemination of plan to create internal awareness;
(9) accountability; and
(10) management commitment to plan implementation is clear.

None of these guidelines are particularly novel to IT researchers, but what is important from the perspective of inter-organizational systems is that an enterprise should also be interested in the effectiveness with which supply chain partners and outsourcing partners adhere to these guidelines. The guidelines are focused on internal corporate monitoring of planning, but it is unlikely that strategically aligned interorganizational systems that link two or more enterprises in the supply chain through B2B e-commerce can be successful if both enterprises are not following good planning processes. Similarly, the core principles for IT governance 1 and 4-10 from the aforementioned IFAC guidance are critical to both enterprises and if either enterprise's alignment is not in place with joint interorganizational systems business objectives and principles 4-10 are not in place to assure alignment is achieved, then success can be hindered for both enterprises.

The subsequent release of the IT Governance framework[3] by the IT Governance Institute (2001) broadens the view of IT Governance and prescribes a much broader view, albeit at a high level prescription. Figure 1 reflects the framework put forth in the 2003 guideline. Note there are five main focus areas that are key to responding to stakeholder value drivers. IT strategic alignment relates to a focus on aligning IT with the business strategy. IT value delivery is concentrated on optimizing expenses and



Source: Adapted from IT Governance Institute (2001) *Board Briefing on IT Governance, 2nd ed.*

Figure 1.
Focus areas of IT governance

proving the value of IT. Risk management is fairly narrowly defined as the safeguarding of IT assets and disaster recovery. Performance Measurement relates to the processes in place to track project delivery and monitor IT services. Resource management (the overarching consideration for the other focus areas) relates to optimizing knowledge and infrastructure from available IT resource investments.

Perhaps one of the more beneficial extensions put forth by the governance framework is the focus on performance measurement in that it takes a position emphasizing a balanced scorecard approach to assessing performance. This balanced scorecard approach (see Figure 2) takes a broader look beyond the financial performance criteria to recognizing the value accrued from meeting customer needs, examining alignment and support of internal business processes, and how IT supports organizational learning and innovation.

Notable again in this framework, and the discussion supporting the framework, is the focus on internal processes, internal value, and internal alignment of processes. While clearly there is value from assessing internal systems, the framework again assumes an enterprise centric model and ignores the implications of interorganizational systems. Also of note, is the general tone taken within the discussion of the framework that addresses IT risk as a separate and distinct subset of

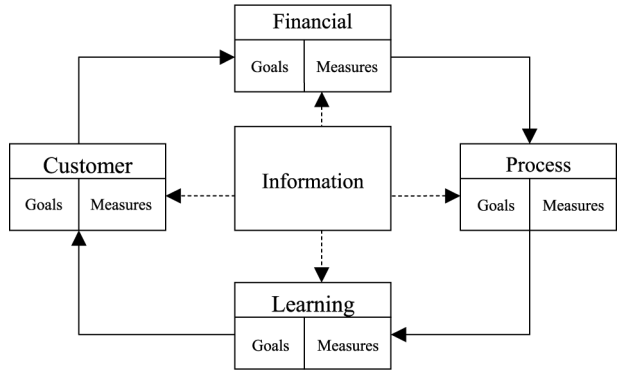


Figure 2.
IT balanced scorecard dimensions

business risk. However, enterprise systems have reshaped most organizations over the past decade to the point where the enterprise systems establish the business rules and the business processes cannot be cleanly separated from the enterprise systems supporting and driving those business processes. This integrated nature of IT and business processes necessitates that business risk be assessed from such an integrated perspective.

IFAC has recognized that e-business alters the risk model. In a white paper entitled: "E-Business and the Accountant" (IFAC, 2002a) notes that risks increase in an e-business environment and management has a responsibility to manage the ensuing risks. The principles and criteria for e-business still treat IT risk as a distinct subset of business risk, though, as it examines the reliability of information security and information processing. The security risk principles include:

- integrity;
- availability;
- confidentiality;
- authenticity;
- authorization; and
- non-repudiation.

It is of note that the latter principle does extend beyond traditional IT controls to recognize a business issue that may arise from e-commerce relationships. IFAC's information processing risk principles include:

- completeness;
- accuracy;
- timeliness;
- accessibility;
- maintenance of chronological order; and
- inalterability of data.

The focus on information security and processing for the principles and criteria for e-business and accounting is curious given that the whitepaper expressly recognizes that IT systems include three basic elements:

(1) IT business processes;

(2) IT applications; and

(3) IT infrastructure.

However, the three components are fairly narrowly defined to focus on the IT components and not the integration. Similarly, the three basic elements are viewed from the enterprise centric view and risks from the partner on the other end of an e-business relationship are not considered other than to consider the need to capture electronically received transaction data from the partner.

One quote in the IT Governance report should resonate heavily with management and researchers, "In IT, if you are playing the game and not keeping score, you are only practising" (IT Governance Institute, 2001). The corporate governance guidelines

presented through the series of guidance documents reviewed to this point all provide valuable information and discussion to support initial IT governance strategies. However, these guidelines still fall short of addressing IT corporate governance needs in enterprise systems and extended-enterprise systems environments. Research is desperately needed that will help guide management in assessing risk in environments where business processes are supported and driven by enterprise systems, and where the two are essentially inseparable and must be jointly assessed. Research is also desperately needed to assist in the development of risk models that recognize that in extended-enterprise environments risks must be evaluated beyond the boundaries of a single enterprise and must encompass all of the partner organizations whose operations and effectiveness have the potential to directly impact the given enterprise's operations and effectiveness. The prior guidance may be useful in informing these research efforts, but they should not serve to limit the scope of the risks that might be considered in such models. Additionally, the balance scorecard approach to assessing effectiveness would seem very beneficial as one means of assessing the success of extended-enterprise relationships. However, this balanced scorecard approach should extend the scope beyond that currently prescribed by the IT Governance Institute (2001).

Audit standards and guidelines

The IFAC (2002a) Whitepaper noted in the prior sub-section was developed in coordination with the development of International Audit Practice Statement 1013 (IFAC, 2002b). This practice statement provides guidance to auditors in the assessment of an auditee's e-commerce relationships. The guideline puts forth the same three basic elements for consideration (i.e. IT business processes, IT applications, and IT infrastructure). The scope is very similar to that in the whitepaper with an emphasis on information security and information processing. Again, the guidance to auditors does not provide for consideration of risk in enterprise systems driven business processes nor the risk inherited from business partners via B2B e-commerce integration.

The other applicable audit guidance is International Standard on Auditing (ISA) 402 on the consideration of entities using service organizations. This guideline is geared primarily towards outsourcers that handle information processing activities and focuses on the reliability of information processing. The standard is written such that the auditor can interpret the needs for assessment of the service organization as extending beyond basic information processing controls, but consideration of risks beyond information processing are not addressed nor is the auditor encouraged to take a broader view.

The American Institute of CPAs (AICPA) and the Canadian Institute of CAs (CICA) have jointly worked on a series of assurance services that are outside of the traditional audit model. These services fit under "Trust Services" and provide for both attestation over system reliability (SysTrust) and attestation over B2C e-commerce (WebTrust). The trust services do provide for the examination of the integration of technology with the goals of the specific application, thus extending the focus slightly beyond just the IT systems. This is a first move forward.

The call for research supporting a broader view of IT governance practice in the prior subsection of the paper parallels closely what is also needed at the audit guideline level. First, research is desperately needed that will help guide auditors in assessing risk in environments where business processes are supported and driven by enterprise

systems, where the accounting rules used by an organization are embedded in the enterprise software, and where the IT systems and the business processes are essentially inseparable and must be jointly assessed. Second, research is also desperately needed to assist in the development of risk models that recognize that in extended-enterprise environments, risks must be evaluated beyond the boundaries of a single enterprise and must encompass all of the partner organizations whose operations and effectiveness have the potential to directly impact the given enterprise's operations and effectiveness. Failure to assess these risks limits the auditor's ability to assess an auditee's viability and ultimately its continuance as a going concern. The work that has been initiated on WebTrust and SysTrust services may aid the expansion of business risk analysis in future audit processes; however, both are still limited in their ability to capture the integration of business processes and IT systems.

Extended-enterprise risk management

An extended-enterprise risk management perspective works off the assumption that risk must be managed across the entire supply chain. Figure 3 reflects a simple supply chain (or segment of a supply chain) with Company B reflecting the enterprise of concern, Company A being an upstream supplier, and Company C being a downstream customer. The circled area focuses on the enterprise centric model of risk management and assurance. Note that in the traditional enterprise centric model the focus is on the enterprise, its information systems and B2B connections. Elliott (2001) suggests that such an enterprise can attain assurance over its own IT systems primarily through using existing Trust Services – i.e. using SysTrust to assess the reliability of the IT systems including security and information processing, and using an adapted form of WebTrust to assess the security and reliability of e-commerce linkages.

Elliott (2001) does raise the issue that an enterprise may want assurance over the security and reliability of trading partners' systems with which the enterprise is connected. His vision is that this can be accomplished by extrapolating the Trust Services model to the systems of these connected enterprises. Figure 4 reflects the assurance model as suggested by Elliott through the application of SysTrust and WebTrust to trading partners' systems.

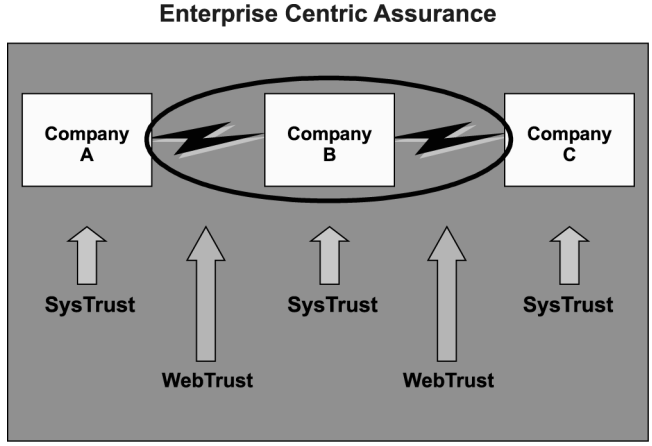


Figure 3.
Enterprise centric risk model

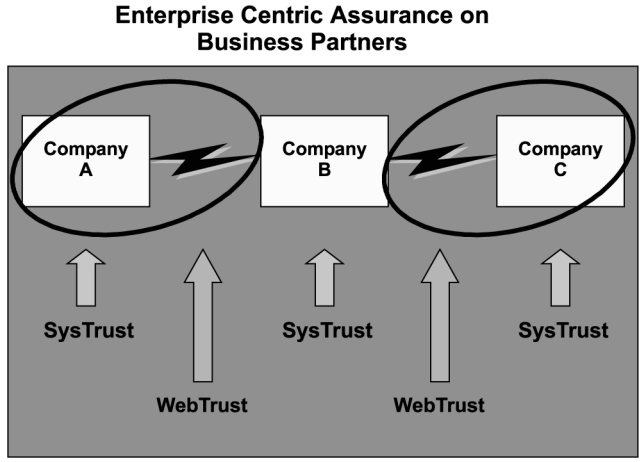


Figure 4.
Enterprise centric assurance on business partners

The conceptual model put forth by Elliott in many ways reflects an extrapolation of the risk assessment concepts put forth by IFAC (2002a, 2002b) for business partners' systems. The specifications under Trust Services capture the three levels of the IFAC guideline (i.e. IT infrastructure, IT applications, and IT business processes). However, the application of Trust Services moves the examination from recommended guidelines for risk consideration in an audit (IFAC, 2002b) to a detailed audit of IT systems at the three levels under specified criteria (Elliott, 2001). Still, Elliott's model fails to take the next step, which is the explicit recognition that the assessment of risk for an enterprise (e.g. Company B) requires an assessment of the reliability of not only that enterprise's systems but also the supply chain partners' systems in the formulation of an overall extended-enterprise risk assessment (see Figure 5).

While conceptually Elliott's model is an improvement, to date there is little experience with Trust Services – particularly on the SysTrust front. Experimental work indicates that there would be demand for both WebTrust (Hunton *et al.*, 2000; Lala *et al.*, 2002) and SysTrust (Boritz and Hunton, 2002) in the marketplace. Yet, as Bedard *et al.* (2005) note,

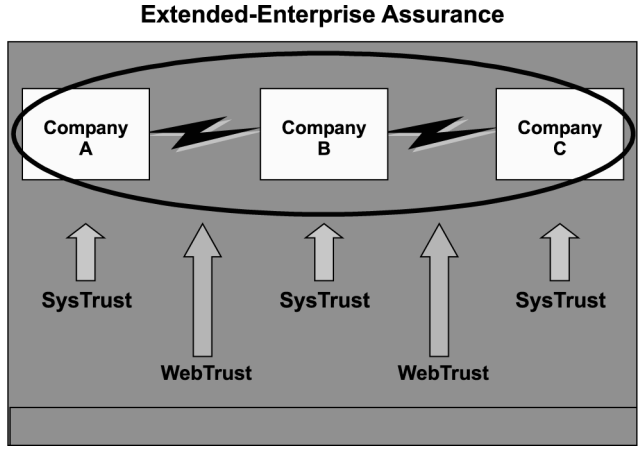


Figure 5.
Extended-enterprise risk assessment model

there are a lot of issues, questions and risks in SysTrust engagements and most auditors are leery about delving into the ill-defined arena of systems reliability assurance. Only limited research to date has looked at ways in which to improve and deliver systems reliability assurance. Havelka *et al.* (1998) conducted a series of focus groups with systems development teams in order to establish criteria for assessing the quality of the information requirements definition process as a first step in assessing systems quality. Arnold *et al.* (2000) explore the market demand for graded reporting of systems quality versus use of a traditional auditor's binary reporting model. These studies represent the first incremental steps in understanding systems reliability assurance. The domain is wide open and in great need of additional research. While SysTrust provides some broad criteria that must be considered in assessing systems reliability, little is known about how to go about assessing these criteria effectively. Given the major role that IT systems play, particularly in enterprise systems environments, the profession must rapidly advance its ability to assess systems quality and academic researchers need to step forward in helping answer the difficult questions that to date present barriers to widespread systems reliability assurance efforts.

Not all of the answers are going to be found through simply enhanced models of Trust Services (i.e. SysTrust and WebTrust). Recall from the earlier discussion that such models focus on the IT systems as separate components from the business processes. In an enterprise systems driven environment, the enterprise system drives the business processes and the business processes are essentially defined by the specifications of the system. This integration is both a necessary condition for effective and efficient business processes and a fundamental limitation to current IT governance and audit/assurance models. An organization can have highly reliable information processing, but poor coupling with the supported business processes resulting in poor efficiency within these processes.

Consider the results reported by Khazanchi and Sutton (2001). In a study of small- and medium-sized enterprises (SMEs) adopting EDI, Khazanchi and Sutton found that the prevalent e-commerce model for these enterprises was to use EDI essentially as a fax machine. The electronic transactions are received and printed in order to facilitate traditional manual processing of transaction information within internal business processes. While these systems may have been quite reliable, the failure to integrate the technology with the business processes provided barriers to the improvement of process efficiencies and prohibited further reductions in cycle time within the supply chain. These SMEs were not in a position to rapidly re-align with changes in technology and efforts to improve the integration of systems across enterprises in the supply chain.

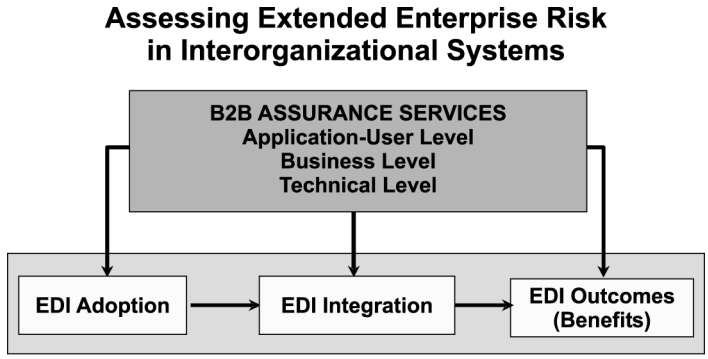
Khazanchi and Sutton (2001) use the results of their study to formulate a three-tier model for B2B e-commerce assurance for interorganizational linkages. Figure 6 and Table I provide the basic assurance model and a description of the three levels in the model:

(1) application-user level;

(2) technical level; and

(3) business level.

The model proposes that audit/attestation (and implicitly IT governance models) should go beyond just technical level risks related to system security, integrity and liability, and application-user level risks related to business partner selection and application policies and procedures. Rather, the model suggests that a fundamental



Source: D Khazanchi and S G Sutton (2001): "Assurance Services for Business-to-Business Electronic Commerce: A Framework and Implications" *Journal of the Association for Information Systems*

Figure 6.
Extended-enterprise risk management model

Category of assurance	Purpose of assurance
Application-user level	The services at this level will focus on assuring that trading partners trust and use EDI for conducting B2B commerce This may include assurance issues relating to establishing relationships with new trading partners, developing "good business practices" and related policies
Business level	The services at this level will focus on assuring that business processes, internal controls, and policies are amenable to EDI adoption and that the processes are altered to allow for seamless integration with the EDI application. This will include addressing legal, privacy of data, and administrative issues for conducting reliable, secure and safe electronic commerce with trading partners transmission security and auditability of B2B (EDI) transactions
Technical level	The services at this level will focus on assuring that all technical elements of EDI are in place and that EDI is seamlessly integrated with internal applications. This will include issues relating to transaction integrity, choice of applications, expansion of trading partner base and transaction volume, system reliability, data security (risk assessment) and encryption, and transmission error

Table I.
Assurance model

Source: Khazanchi and Sutton (2001)

level of risk consideration includes business level issues such as seamless integration with business processes, privacy issues and legal issues. The model focuses on the recognition that the internal integration of IT systems with business processes may have a direct impact on other members of the supply chain and assurance over risks related to not only technical and application issues, but also business integration are critical to overall risk assessment and risk management.

Initial research efforts on expanding the Khazanchi and Sutton (2001) model have only recently emerged with the first major project being funded by the Institute of Internal Auditors Research Foundation. Arnold *et al.*'s (2004) monograph overviews a

project focused on identifying the critical risk factors that should be examined at each of the three levels of the model. The research also explores the links between various relationship factors (e.g. satisfaction, trust, justice, etc.) and assessments of B2B e-commerce partners' risk assessments across the three dimensions. These initial results indicate that there is a desire for assurance of partners B2B e-commerce systems when risk assessments rise.

The research to date is again very scarce in this area. Substantially more research is needed to better understand all of the dimensions in the extended-enterprise model that should be monitored for risk fluctuations. Do the critical B2B e-commerce risk factors shift based on the level of e-commerce maturity in an enterprise? Should B2B e-commerce assurance be mandated for all interorganizational linkages? Are there other dimensions of risk in the extended-enterprise model that are not captured in the three-level assurance model? Can reliable assurance processes be designed to effectively evaluate risk across the supply chain? Are there ways to enhance current audit procedures for service bureaus to a level consistent with the scope and level of integration in extended enterprise systems such that audit standards adequately capture the need for assurance of business partners and provide a mechanism for attaining assessments of business partners' risk without every auditor having to visit every business partner? There is no shortage of research opportunities in the area, only a desperate need for more researchers to take on the challenging studies and problems that lie ahead.

Concluding thoughts

Enterprise systems and the coupling with B2B e-commerce technologies have radically altered the business environment. Organizations have re-engineered their business processes to take advantage of the efficiency and effectiveness gains that accrue from tight integration of enterprise software with business processes. B2B e-commerce technologies have leveraged off of enterprise systems to tap into the power of such software and provide tightly coupled, complex linkages between trading partners and supply chain partners. Unfortunately, IT governance practices and enterprise risk management strategies have not kept pace with these rapid changes, leaving many enterprises vulnerable to unidentified risks inherited from business partners.

This paper details an examination of the changes that enterprise systems and B2B e-commerce technologies have brought to the risk management arena. The discussion has reviewed the efforts that have been made by both the practitioner and the academic communities to address these shifting risk models. The research to date has provided modest gains in addressing the need for new risk management models. Overall, however, the studies to date primarily tell us how little we know about risks in these complex extended-enterprise environments and highlight the critical need for a widespread research effort to facilitate the development of improved risk assessment models. There is a shortage of researchers working in this arena and this critical shortage is restricting the flow of research in a time when it is desperately needed to provide the leadership to practice in improving IT governance frameworks and expanding audit risk models.

The research reviewed in the current study can be integrated into a framework for the assessment of risk across the extended enterprise. The framework put forth here combines the scope of the supply chain coverage advocated by Elliott (2001) (with the extensions recommended within this study) with the three-level architecture put forth by Khazanchi and Sutton (1991). Figure 7 presents the framework combining these two

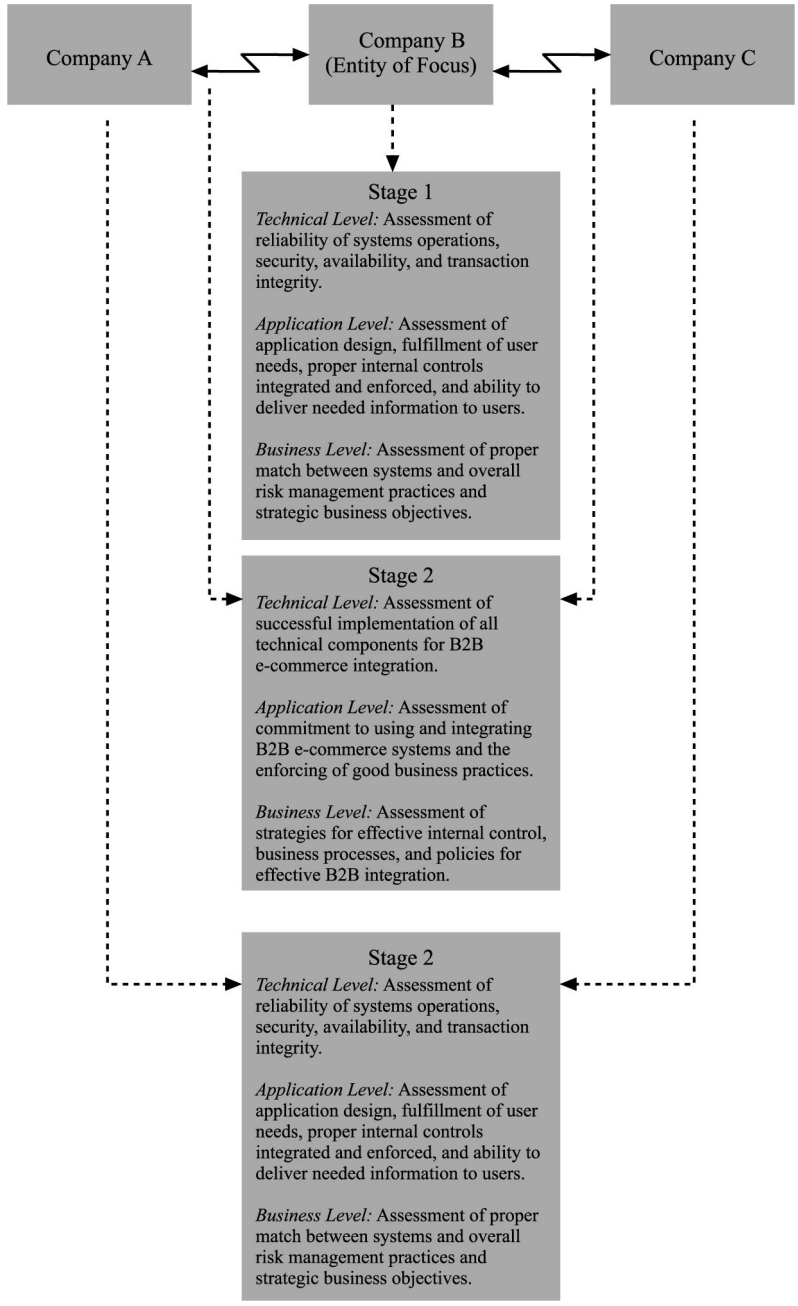


Figure 7.
Extended-enterprise risk management framework

aspects into a three-stage model of extended enterprise risk assessment. In considering the framework, it should be recognized that stages 2 and 3 repeat for each business partner further upstream or downstream in the supply chain and for each outsourcer used to streamline business processes. It should also be recognized that neither current professional guidance and standards or extant research provide a means of implementing this framework. Rather, research is in great need to explore each dimension of the framework in order to provide guidance to managers and standards-setters on the implementation of the extended-enterprise risk management framework.

Notes

1. Enterprise systems is the more contemporary term for a class of integrated systems that largely include enterprise resource planning (ERP) systems such as SAP, Oracle, Peoplesoft, JDEdwards OneWorld, Baan, and Navison.
2. Subsequent to the passing of the Sarbanes-Oxley Act in the US, similar requirements on internal control and corporate governance reporting have been adopted by a number of other jurisdictions such as Australia, Canada, and the European Union.
3. This project was also supported by IFAC, American Institute of CPAs, Association Francais de L'Audit et du Conseil Informatiques, Center for Internet Security, Canadian Institute of CAs, Deloitte & Touche, Ernst & Young, IBM, Japanese Institute of CPAs, Institute of CAs in England & Wales, KPMG, and PricewaterhouseCoopers.

References

Angeles, R. and Ravinder, N. (2000), "An empirical study of EDI trading partner selection criteria in customer-supplier relationships", *Information & Management*, Vol. 37 No. 2, pp. 241-55.

Arnold, V., Hampton, D., Khazanchi, D. and Sutton, S.G. (2004), *Enterprise Risk Management: Identifying Risks in B2B E-Commerce Relationships*, Institute of Internal Auditors Research Foundation, Altamonte Springs, FL.

Arnold, V., Lampe, J.C., Masselli, J.J. and Sutton, S.G. (2000), "An analysis of the market for systems reliability assurance services", *Journal of Information Systems*, Supplement, pp. 65-82.

Bedard, J.C., Jackson, C.M. and Graham, L. (2005), "Issues and risks in performing Systrust engagements: implications for research and practice", *International Journal of Accounting Information Systems*, March, pp. 55-79.

Boritz, E. and Hunton, J.E. (2002), "Investigating the impact of auditor-provided systems reliability assurance on potential service recipients", *Journal of Information Systems*, Supplement, pp. 69-82.

Elliott, R. (2001), "21st century assurance", paper presented at the AAA Auditing Section Mid-Year Meeting, Atlanta, GA, January 12-15.

Ernst & Young (2004), *Emerging Trends in Internal Controls: Initial Survey*, available at: www.ey.com

Ghahremani, T. (2003), "Gremlin in the works", *CFO Magazine*, October 28.

Grieger, M. (2003), "Electronic marketplaces: a literature review and a call for supply chain management research", *European Journal of Operational Research*, Vol. 144 No. 2, pp. 280-94.

Grover, V., Teng, J.T.C. and Fiedler, K.D. (2002), "Investigating the role of information technology in building buyer-supplier relationships", *Journal of the Association for Information Systems*, Vol. 3 No. 2, pp. 217-45.

Hart, P.J. and Saunders, C.S. (1997), "Power and trust: critical factors in the adoption and use of electronic data interchange", *Organization Science*, Vol. 8 No. 1, pp. 23-42.

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

Hunton, J.E., Benford, T., Arnold, V. and Sutton, S.G. (2000), "The impact of electronic commerce assurance on financial analysts' earnings forecasts and stock price estimates", *Auditing: A Journal of Practice and Theory*, Supplement, pp. 5-22.

IFAC (1999), *Information Technology Planning for Business Impact*, International Federation of Accountants, New York, NY.

IFAC (2002a), *IFAC E-Business and the Accountant*, International Federation of Accountants, New York, NY.

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

ISACA (2001), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, Information Systems Audit and Control Association, Rolling Meadows, IL.

IT Governance Institute (2001), *Institute Board Briefing on IT Governance*, 2nd ed., IT Governance Institute, Rolling Meadows, IL.

Khazanchi, D. and Sutton, S.G. (2001), "Electronic commerce assurance services: a framework and implications", *Journal of the Association for Information Systems*, Vol. 1 No. 12, pp. 1-54.

Kumar, K. and van Dissel, H.G. (1996), "Sustainable collaboration: managing conflict and cooperation in interorganizational systems", *MIS Quarterly*, Vol. 20 No. 3, pp. 279-300.

Lala, V., Arnold, V., Sutton, S.G. and Guan, L. (2002), "The impact of relative information quality of e-commerce assurance seals on internet purchasing behavior", *International Journal of Accounting Information Systems*, Vol. 3 No. 4, pp. 237-54.

PricewaterhouseCoopers (2004), *Managing Risk: An Assessment of CEO Preparedness*, available at: www.pwc.com

Ramos, A.D. (2004), "Farewell, finance", *Computerworld*, July 14.

Shin, K. and Leem, C.S. (2002), "A reference system for internet based inter-enterprise electronic commerce", *Journal of Systems and Software*, Vol. 60 No. 2, pp. 195-209.

Sutton, S.G. and Hampton, C. (2003), "Risk assessment in an extended enterprise environment: re-defining the audit model", *International Journal of Accounting Information Systems*, Vol. 4 No. 1, pp. 57-74.

Taylor, D.A. (2003), "Supply chain vs supply chain", *Computerworld*, Vol. 37 No. 45, pp. 44-5.

Vijayan, J. (2002), "Business partners, third parties can pose security risk", *Computerworld*, Vol. 36 No. 26, pp. 43-55.

Corresponding author
Steve G. Sutton can be contacted at: sgsutton@unimelb.edu.au