A conceptual risk framework for internal auditing in e-commerce

Jagdish Pathak
Louise and Edmond Odette School of Business, University of Windsor, Windsor, Canada

Keywords *Internal auditing, Electronic commerce, Business-to-business marketing*

Abstract *Auditors provide high assurance to executives amidst information and database risk. A framework is provided for auditors within cyber entities. The categories of e-commerce, business-to-business, business-to-customers and mobile commerce use different core technologies. The common factor remains unchanged from the auditors' perception, i.e. risk and its potential to harm the integrity and accuracy of the data and decisions based thereon. E-commerce requires audit to identify risks and show their impact on the information system. The American Institute of CPAs and Canadian Institute of Chartered Accountants jointly offer seals of assurance at Web and system levels. The limitations of these certifications are important for an auditor since they are set by these accounting bodies. The role and functions of an auditor are beyond those of the assurance approval auditors. Organizational decision-making processes depend on segments of information bases, whereas these assurance providers audit a limited amount related to their interest.*

E-commerce technology and auditing

The American Institute of CPAs (AICPA) and Canadian Institute of Chartered Accountants (CICA) have developed specific criteria that an entity must comply with to obtain and maintain the CPA WebTrust seal (Anonymous, 1997; William, 1997). The seal of approval indicates that the particular online business has been subject to an evaluation by a CPA firm. The seal also provides assurance regarding the following:

- *Business practices and information privacy.* The business must disclose how orders are processed and how returns and warranties are handled. The business must also disclose its policy on the maintenance of customer information (e.g. the selling of mailing lists).
- *Transaction integrity.* The business must report how transactions are validated and processed, as well as how the billing process is controlled. Disclosures of billing and settlement terms are also required.
- *Information protection.* The business must protect the privacy of sensitive information, such as credit card numbers, through the use of encryption.

Exponential growth in the Internet and the transmission bandwidth of the communication carrier is transforming the way businesses operate and communicate. In this technology-centric world, customers, partners, suppliers and employees are demanding unparalleled levels of service, collaboration and communications. Organizations must adopt a purposeful electronic commerce (e-commerce) strategy (Doherty and Ellis-Chadwick, 2003; Good and Schultz, 2003) to compete in the emerging marketplace. E-commerce as a technology is not very simple. It gets further complicated with the changes in communication technologies, database and other related information technologies. E-commerce is not adopted by businesses simply to reduce their operating costs and increase their revenue. Not

Managerial Auditing Journal
Vol. 19 No. 4, 2004
pp. 556-564

0268-6902
DOI 10.1108/02686900410530556

everyone always has a genuine desire to conduct business; some may intrude into an organization's systems with specific intent or out of sheer curiosity. The intrusion may be facilitated either by malicious hacking techniques or by sheer chance (Biermann *et al.*, 2001; Gengler, 2002). Thus, any e-business is a sitting duck with regard to the illicit and illegal objectives of a malicious hacker or intruder who may wreak havoc on system resources and data. Any business initiating e-commerce to reduce operational costs may not get the resultant effect without clearly chalking out the strategy and opting for the right model. E-commerce is risk-based due to the technologies involved (Sutton and Hampton, 2003), which may expose a business's data and systems to unknown outsiders. However, e-commerce increasingly appears to be essential for an organization's survival and growth. In an e-commerce environment (Bette and Gilbert, 2001; Wei *et al.*, 2002), the internal systems and processes of an entity are no longer operated in isolation. An organization exchanges information via transactions that link entities together in ways unanticipated in the traditional environment.

Most e-commerce implementations concentrate on optimizing the Internet as a tool to facilitate transactions – on providing networked computers which allow end-users to create and transform business relationships (O'Toole, 2003). At present, the term e-commerce includes all commercial activities performed through information technology and communication engineering such as the Internet, virtual private networks (VPN) (Harding, 2003; Walid and Kerivin, 2003), automated teller machines (ATMs), electronic fund transfers (EFT), electronic data interchange (EDI) (Sangjae and Lim, 2003), e-supply chain management (e-SCM) (Williams *et al.*, 2002) and also e-customer relationship management (e-CRM) (Pan and Lee, 2003). New enterprise applications and various applications of integration technologies provide technology-driven business solutions which improve the quality of dealing with the customers and vendors of goods and services, increase the speed of service delivery and reduce the cost of business operations.

The revamping also contributes to better, improved and standardized internal business processes (Barnes *et al.*, 2002) through business process re-engineering (BPE) (Wu, 2003). Enterprise-wide application integration (Fan *et al.*, 1999) and complex systems integration processes (Pathak and Lind, 2003), though highly technical, play a vital role in holistic improvement of the business processes of any business entity planning to take a jump in the arena of e-commerce. Figure 1 shows the e-commerce technologies on a graphical matrix in relation to structured and unstructured formats and also on high and low level of technology complexity.

A decade back, this type of functionality was limited to EDI transactions. EDI, the precursor of e-commerce category called business-to-business (B2B), is a method of electronic data and information transfers which businesses used to complete transactions. This method saved time and effort over detailed paperwork, but it is relatively an expensive system to install and maintain. Also, it is a closed and proprietary system which is available to and used among only relatively larger corporations. In contrast, the electronic data transfers (Litsikas, 1997) allowed by new forms of e-commerce are fluid and easy to use. Though the Worldwide web (WWW) is still in its growth phase and the processing of transactions in such open domain has its own drawbacks relating to integrity and reliability, it allows a free flow of information across an open, widely available network of WWW. E-commerce allows a variety of interactions, from business-to-consumer (B2C) transactions such as buying and selling information, products and services using the Internet, to transferring and sharing

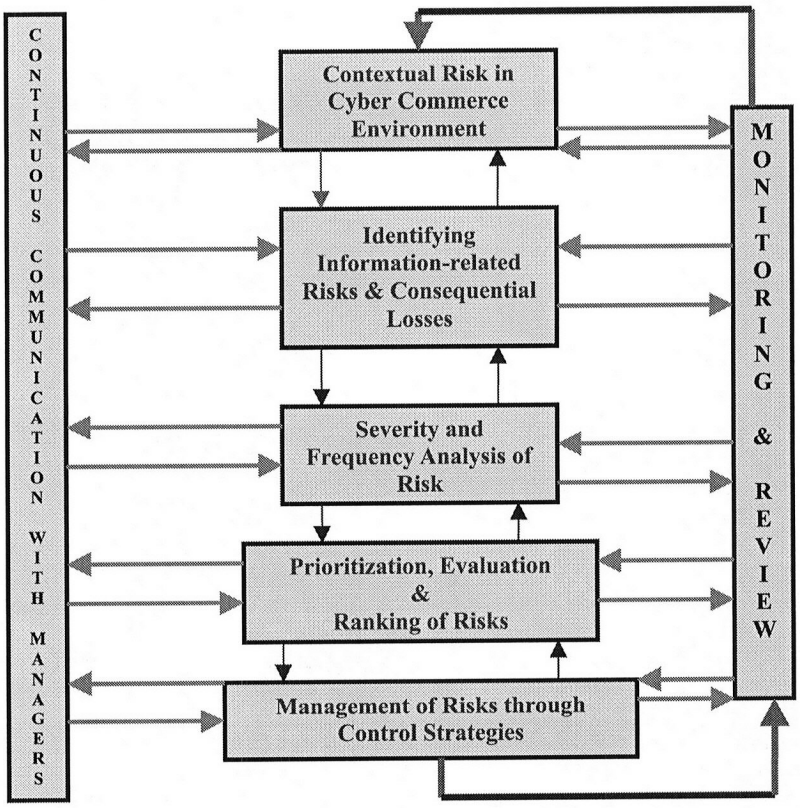

Figure 1.
A graphical matrix showing e-commerce technologies

information within organizations through intranets. Another category which has truly picked up of late is B2B e-commerce dealing with the vendors', dealers' and suppliers' network. It grants such benefits as improved decision making, increased efficiency, less paperwork and greater empowerment. As a business paradigm, e-business supports and complements BPE and integration.

E-commerce entity and its defined goals

Successful e-commerce implementation should have defined goals including:

- reduced transaction costs;
- greater productivity and service availability for two hours a day/seven days a week;
- opportunities for fundamental reform in how organizations and their supply chains communicate and work with other businesses; and
- opportunities for local businesses to grow and compete in the global marketplace.

Perhaps the most important facet of e-commerce is the way customers become empowered through the routes that companies use to reach and interact with them. These changes affect four areas which shape customer relationships:

(1) Advertising.
(2) Order taking.
(3) Customer service.
(4) Customized products/services.

Prior to the installation or shifting over to e-commerce, an organization deserves to ascertain the level of risk exposure on two counts: the number of people involved and the value of the transaction (payment or contract). As a general rule, the more parties involved, the greater the risk. Similarly, a higher value transaction will generate greater risk. Because e-commerce allows international trading, the number and location of parties that can attempt to access the systems create new challenges related to protecting critical applications and activities. Streamlining approvals through electronic processes (Louis *et al.*, 2002) may remove existing internal controls and potentially increase the risk further. Whatever the competitive strategy (Gill, 2003) chosen, it is important to decide the extent to which the investment should be deployed, and the time frame for such investment. Such investment can include personnel and equipment needed to develop a Web presence, communicate with customers, monitor the competitive environment (Avishalom and Bazerman, 2003), develop new products or a niche, and expand the supplier base.

A framework for understanding the risks for auditors

An organization's auditors are in a unique position to ensure that changes, whether they are new business models and processes or new systems, support the organization's mission and objectives and that adequate control procedures are an integral component from the beginning of the systems development process. In many organizations, to mitigate the risks associated with accounting information systems, the internal audit function is assigned the responsibility of implementing a system of internal control. Owing to additional risks associated with e-commerce systems, and the resulting need for strong control procedures, it is important that management appreciates the significance of having auditors participate in the systems development process. These internal controls are activities performed to eliminate risks or minimize them to an acceptable level. In most cases, it is cost-prohibitive to implement every type of control in an effort to eliminate all elements of risk. Thus, internal auditors must be aware of an organization's objectives and must weigh the costs of implementing a control against the potential benefits of that control. Maximizing organizational benefits through judicious use of controls in e-commerce systems can enhance control over the systems and reduce the costs of implementing these controls. Accounting professionals refer to rules, policies, and procedures involved in managing an organization's risks as the "system of internal controls". The way accountants view internal controls changed in the early 1990s as a result of the landmark study, "Internal control – integrated framework by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)" (Vinten, 2001).

Fraud is a highly publicized risk in an e-commerce environment. E-commerce fraud can either be perpetrated by an employee within the firewall or an anonymous party in a foreign country. Figure 2 is an attempt to provide a schema of the framework to be followed by internal auditors of e-commerce entities under review.

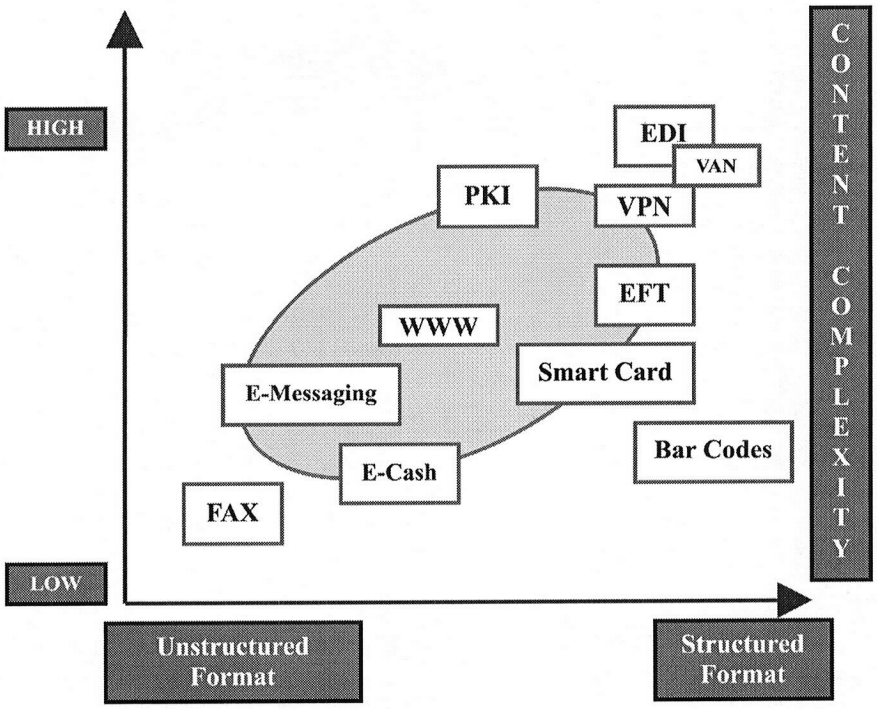

Figure 2.
Understanding of e-commerce technology for auditors

This schema has a characteristic of obtaining information assurance at each level of the hierarchy of operations and management. All companies are vulnerable to sabotage and espionage from the inside and the outside, a risk heightened but not created by the Internet. Not all of it is malicious, and software companies in particular are prone to in-house high jinks by employees. Do you know how safe your company's secrets are? Perhaps you have measures in place to prevent large-scale corporate espionage, but do you have protection against the disgruntled employee who is fired or resigns? How can you prevent an employee in accounting from stealing trade secrets and using them personally or selling them to a competitor? Unfortunately, a company probably cannot easily prevent a disgruntled employee from damaging its business. But companies can make it more difficult for an internal saboteur from a legal, physical and technical point of view. Protective measures are also advisable if someone leaves on amicable terms.

Possible fraudulent activities include the following:

- unauthorized movement of money such as payments to fictitious suppliers located in jurisdictions where recovery of money will be difficult;
- misrepresentations of company tenders;
- corruption of the electronic ordering or invoicing systems;
- duplication of payment;
- denying an order was placed;

- denying an order was received;
- denying receipt of goods;
- denying that payment was received; and
- falsely declaring that a payment was made.

For e-commerce implementation to be successful, information about the organization needs to be made available to other participants in the trading community. However, people are becoming concerned at the amount of information required and the security of the data the other party collects. If people or organizations are not confident that data are properly protected, they may be unwilling to provide it. Public confidence can be adversely impacted if information is accessed without proper authorization.

Information at risk

What type of information of any entity is at risk? An internal auditor is expected to identify such information from their origin or centre of creation. Any information emanating from lesser assured or partially assured systems cannot be called assured information as regards to its accuracy and integrity (Pathak and Baldwin, 2003). Internal auditors make efforts to ascertain the quality of information to identify whether such information is at a risk of being corrupt or potentially corrupt. Information at risk may include the following:

- services and prices which are not normally provided to the general public;
- cost structures, particularly those relating to tenders;
- an individual's information – name, address, contact detail, earlier purchases or services provided; and
- restricted information – information that should be shared only between specific parties, such as medical records, prison records and personnel files.

Risks may be caused by internal or external malicious activity – virus attacks, hacking, and the interception of data by unauthorized person, unauthorized viewing or corruption of data, and data that are archived or disposed of improperly. Poor access protection of information can be another cause of risk, especially when dealing with the separation of private and public data.

Repudiation is another area of risk in electronic transactions. Although the system shows that the transaction took place, one of the parties denies that it occurred. Given that paper trails are limited in the electronic world, how does one party prove irrefutably that the transaction has taken place? A lack of authentication can lead to another area of risk in electronic transactions. Proper authentication is a critical component of an e-commerce transaction, since once a party has been accepted into the system, a legally binding transaction process has begun. Because paper-based controls are limited during an electronic transaction, an unauthorized party may be accepted and go undetected.

These issues all deal with the question of data integrity. Risks involve activities that can be performed remotely through Web resources. But although those are sources of risk, almost all corruption of data takes place within the system. One of the major concerns associated with data corruption is the possibility that the data may become invalid. Some examples of malicious activity that can invalidate data include:

- amending catalogues without authorization;
- destruction of audit trail;
- tampering with the ordering process;
- interrupting the transaction recording;
- disrupting online tendering; and
- business interruptions.

Business interruptions are a major risk; if companies cannot promptly and adequately resume business activities after a crisis; legal liabilities may arise when services or goods are not delivered or when payments are not made on time.

The role of an internal auditor is important in a scenario that contains this amount of risk, and in assessing the impact of these risks on the overall activities of e-commerce.

Conclusion

Inadequate funding may force some organizations to tolerate a higher than acceptable risk when implementing e-commerce. The need for an e-commerce site is becoming more apparent day after day, but so is the potential risk. An audit review program for e-commerce Web sites will be a critical tool for internal auditors (Pathak, 2000). E-commerce creates new dimensions for transactions, but these new dimensions require a set of security tools and an infrastructure that necessitates business processes being re-engineered. As e-commerce assurance continues to capture headlines in our daily lives, it is imperative that e-businesses have an information assurance framework – a solid plan of action with the required tools, trained personnel, and tested procedures – that is capable of protecting valuable information regarding the privacy and financial aspects of the prospective customers. The audit review process will provide the closed-loop cycle of continuous improvement that is imperative in today's e-commerce world. I have identified the framework that needs to be implemented by the internal auditors and they need to make the beginning of the arduous process of making it a reality. Auditors must understand that the solution is not quick-fix and will build over time with the awareness of all employees and the support of management.

References

Anonymous (1997), "AICPA/CICA unveils new assurance service", *The CPA Journal*, Vol. 67 No. 11, p. 9.

Avishalom, T. and Bazerman, M.H. (2003), "Focusing failures in competitive environments: explaining decision errors in the Monty Hall game, the acquiring of a company problem, and multiparty ultimatums", *Journal of Behavioural Decision Making*, Vol. 16 No. 5, p. 353.

Barnes, D., Hinton, M. and Mecgkowska, S. (2002), "Developing a framework to investigate the impact of e-commerce on the management of internal business processes", *Knowledge and Process Management*, Vol. 9 No. 3, p. 133.

Bette, A.S. and Gilbert, J. (2001), "Ethical issues in e-commerce", *Journal of Business Ethics*, Vol. 34 No. 2, pp. 75-86.

Biermann, E., Cloete, E. and Venter, L.M. (2001), "A comparison of intrusion detection system", *Computers and Security*, Vol. 20 No. 8, pp. 676-83.

Doherty, N. and Ellis-Chadwick, F. (2003), "The relationship between retailers' targeting and e-commerce strategies: an empirical analysis", *Internet Research*, Vol. 13 No. 3, p. 170.

Fan, Y., Shi, W and Wu, C. (1999), "Enterprise-wide application integration platform for CIMS implementation", *Journal of Intelligent Manufacturing*, Vol. 10 No. 6, p. 587.

Gengler, B. (2002), "Intrusion detection system new to market", *Computers Fraud and Security*, No. 5, p. 4.

Gill, T. (2003), "Competitive strategic dynamics", *Systems Dynamics Review*, Vol. 19 No. 3, p. 265.

Good, D. and Schultz, R. (2003), "E-commerce strategies for B2B service firm in the global environment", *American Business Review*, Vol. 20 No. 2, pp. 111-19.

Harding, A. (2003), "SSL virtual private networks", *Computers and Security*, Vol. 22 No. 5, p. 416.

Litsikas, M. (1997), "Electronic downloads eliminate inspection audits", *Quality*, Vol. 36 No. 1, pp. 50-1.

Louis, S., Carvalho, L., Jeffrey, R., D'Ambra, J. and Becker-Kornstaedt, U. (2002), "Understanding the use of an electronic process guide", *Information and Software Technology*, Vol. 44 No. 10, p. 601.

O'Toole, T. (2003), "E-relationships: emergence and the small firm", *Marketing Intelligence & Planning*, Vol. 21 No. 2, p. 115.

Pan, S. and Lee, J-N. (2003), "Using e-CRM for a unified view of the customer", *Communications of ACM*, Vol. 46 No. 4, p. 95.

Pathak, J. (2000), "E-commerce: a Web site audit review program", *Chartered Accountant*, pp. 25-9.

Pathak, J. and Baldwin, A. (2003), "Generation-X technology and auditors: a paradigm shift", *Proceedings of 12th Annual Research Workshop of Artificial Intelligence/Emerging Technology Section*, 2 August, American Accounting Association, Honolulu, HI.

Pathak, J. and Lind, M. (2003), "Audit risk, complex technology and auditing processes", *EDPACS*, Vol. XXXI No. 5, pp. 1-9.

Sangjae, L. and Lim, G.G. (2003), "The impact of partnership attributes on EDI implementation issues", *Information and Management*, Vol. 41 No. 2, p. 135.

Sutton, S. and Hampton, C. (2003), "Risk assessment in an extended enterprise environment: redefining the audit model", *International Journal of Accounting Information Systems*, Vol. 4 No. 1, pp. 37-73.

Vinten, G. (2001), "Corporate governance and the sons of Cadbury", *Corporate Governance*, Vol. 1 No. 4, pp. 4-9.

Walid, B-A. and Kerivin, H. (2003), "New economical virtual private networks", *Communications of ACM*, Vol. 46 No. 6, p. 69.

Wei, C.P., Hue, P.J. and Dong, Y-X. (2002), "Managing document categories in e-commerce environments: an evolution-based approach", *European Journal of Information Systems*, Vol. 11 No. 3, pp. 208-18.

William, K. (1997), "AICPA launches electronic commerce seal", *Strategic Finance*, Vol. 79 No. 4, p. 16.

Williams, L., Terry, E. and Ogment, J. (2002), "The electronic supply chain: its impact on the current and future structure of strategic alliances, partnerships and logistic leadership", *International Journal of Physical Distribution & Logistics Management*, Vol. 32 No. 8, pp. 703-20.

Wu, I-L. (2003), "Understanding senior management's behaviour in promoting the strategic role of IT in process re-engineering: the use of the theory of reasoned actions", *Information and Management*, Vol. 41 No. 1, p. 1.

Further reading

Cashell, J. and Aldhizer, G.D. III (1999), "Web trust: a seal of approval", *Internal Auditor*, Vol. 56 No. 3, pp. 50-4.

Maxy, D. (2001), "E-commerce (a special report); cover story – the people behind the sites: expedia; testing, testing", *Wall Street Journal (Eastern)*, 10 December, pp. R-8.

Pathak, J. (2003), "Internal audit and e-commerce controls", *Internal Auditing Journal*, Vol. 18 No. 2.

Primoff, W. (1998), "Electronic commerce and Web trust", *The CPA Journal*, Vol. 68 No. 11, pp. 11-19.

Salazar, A., Hackney, R. and Howells, J. (2003), "The strategic impact of Internet technology in bio-technology and pharmaceutical firms: insights from a knowledge management perspective", *Information Technology and Management*, Vol. 4 No. 23, p. 289.