Auditing E-Business: New Challenges for Conventional External Auditors

DR. AHMAD ABD EL-SALAM ABU-MUSA
Department Of Accounting, Tanta University, Egypt; and Department Of Accounting & MIS, KFUPM, Saudi Arabia

1. INTRODUCTION

Electronic Business (E-Business) technologies are rapidly changing the way that the companies buy, sell, and service customers and collaborate with partners. E-Business involves all kinds of commercial activities performed across computer platforms and applications, including direct selling (e-tailing), customer relationship management, supply chain management, and the use of the Internet as the medium for conducting business transactions. The dramatic development Internet technologies and the continuous decline of their prices has made E-Business applications more affordable, and encourages many companies of all sizes to implement them. These include not only business to business (B2B) applications but also business to consumer (B2C), business to government (B2G), and business to employee (B2E). Recognizing that various issues for auditors are emerging from these developments, the Auditing Practices Board published appropriate guidance in April 2001: Bulletin 3, E-Business: Identifying Financial Statement Risks (Billing, 2001; and Price, 2001).

IFAC, (2002) argued that the use of the term *E-Commerce* has already been superseded by the term *E-Business*. E-Commerce can be described as the procurement and distribution of goods and services over the Internet using digital technology. The more encompassing term E-Business can be defined as including all activities carried on by a business via the Internet. This definition for E-Business extends beyond the definition of e-commerce by encompassing a digital approach to the whole enterprise, including other parts of the IT system and other non-transactional activities, such as recruiting employees via the Internet (Figure 1). ISACA (2002) confirmed that the term e-commerce is used by different parties to mean different things. ISACA defined e-commerce as the processes by which organizations conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology. It therefore

* Dr Ahmad Abd El-Salam Abu-Musa is Assistant Professor at Accounting Department, Faculty of Commerce, Tanta University, Egypt. Dr Abu-Musa works now as a visiting Assistant Professor at Department of Accounting & Management Information Systems, King Fahd University of Petroleum and Minerals, Saudi Arabia.

**Acknowledgement:** The author acknowledges the support of the Department of Accounting & Management Information Systems, King Fahd University of Petroleum and Minerals, Saudi Arabia.

* Dr Ahmad Abd El-Salam Abu-Musa is Assistant Professor at Accounting Department, Faculty of Commerce, Tanta University, Egypt. Dr Abu-Musa works now as a visiting Assistant Professor at Department of Accounting & Management Information Systems, King Fahd University of Petroleum and Minerals, Saudi Arabia.

**Acknowledgement:** The author acknowledges the support of the Department of Accounting & Management Information Systems, King Fahd University of Petroleum and Minerals, Saudi Arabia.
encompasses both B2B and B2C e-commerce models, but does not include existing non-Internet e-commerce methods based on private networks, such as EDI and SWIFT.

Evolution of E-Business

(Figure 1)

The Evolution of E-Business

Sun, (2000) mentioned that, the world has been turned upside down by information technology and the Internet. The great boom in E-Business has dramatically changed traditional ways of business. Therefore, professional accountants need to understand how advanced technology affects their operation. They need to acquire the necessary information technology knowledge and skills that enable them to deal with Internet-related tax issues, e-fraud, and the audit of electronic transactions on a daily basis. A part from technical knowledge, accounting professionals now need knowledge of business, industries, the marketplace and competitors.

2. E-BUSINESS RISKS AND OPPORTUNITIES

E-Business changes the way business is conducted. In particular, E-Business requires changes in organizational structures, business partnerships and alliances, delivery mechanisms and methods, and the legislation and regulations under which businesses operate. E-Business also introduces new risks that enterprises may need to address. Furthermore, E-Business alters the roles and responsibilities of employees and different levels of management, therefore affecting personnel requirements. Moreover, E-Business affects business conduct and the character of business itself. These fundamental changes will also have a significant impact on accounting systems, changing business processes and the evidence available to support business transactions, which, in turn, will lead to changes in the accounting records maintained and accounting procedures followed. Consequently, accountants and auditors are facing new challenges and may need to apply new techniques, such as the development of accounting systems based on business processes, to ensure that transactions are appropriately recorded, are in compliance with local and international legislation and regulations, and meet current and evolving accounting standards and guidance.
In the following section the opportunities of E-Business and its related risks will be briefly discussed.

2.1. E-BUSINESS OPPORTUNITIES

E-Business brings many opportunities to many companies. Implementing E-Business provides organizations with new tools and techniques for cutting costs, communicating more effectively, increasing sales, and improving operational efficiency and effectiveness. E-Business drives globalization in several ways. E-Business beats geography and time zones. Physical distance disappears or is circumvented by electronic connectivity, and the scope of the marketplace is broadened beyond traditional spheres. Customers now expect goods and services 24 hours a day form anywhere in the world. As such, virtual connectivity empowers firms to build a truly integrated worldwide network. However, in order to keep pace with the electronic revolution in business, External auditors must be driven to acquire an understanding of new technologies. They must also develop audit approaches that ensure the organization’s E-Business objectives are achieved in a controlled manner (Burr, 2002; and Cavusgil, 2002).

E-Business offers companies at least the following competitive advantage:

- **Productivity and cost reduction.** E-Business helps the enterprise perform value-chain activities more efficiently by helping companies engage in end-to-end integration of entire sales, production, and delivery processes electronically, across borders and time zones. For example, e-commerce in the global marketplace is widespread, with numerous online banking, stock trading, exchanges, and numerous B2B and B2C applications.

- **Speed.** Information and knowledge can move freely within the company and its customers, suppliers, and other constituents. Managers can implement decisions instantaneously. E-Business can also reduce time to market and other cycle times for responding to ongoing or anticipated business needs.

- **New opportunities and value creation.** Web-enabled businesses can thrive because of flexibility, focus, and entrepreneurial initiatives brought to global operations. A prime benefit for global organizations is the ability to implement strategy on a worldwide scale, organize globally, and integrate and rationalize operations worldwide (Cavusgil, 2002).

According to Nearer, (2000) E-Business transactions are expected to grow from approximately $100 billion in 1999 to $7.3 trillion by 2004, according to a recent estimate in the New York Times. Gross domestic product (GDP) for 2004 is estimated at $11 trillion, which would make E-Business represent 66% of the economy within the next four years. Simply put, companies engaged in E-Business or actively planning for it can expect rapidly increasing sales and technological expansion. CPAs prepared to audit E-Businesses will reap the benefits.

E-Business has become an important and necessary business tool, therefore, highly specialized and developed IT skills would be required to assess the systems associated with it. The growth in Internet business transactions (i.e., E-Business) continues at exponential rates. The anticipated growth in E-Business presents significant challenges for auditing profession. CPAs knowledge regarding the Internet issues has become so important. Auditors should learn more about the affect of implanting E-Business on their clients, practice, and financial statement auditing. A fundamental understanding of IT systems will allow traditional auditors to work in E-Business environments, understand when IT auditors should be consulted, and help them communicate with the IT professionals. The collaboration between operations/financial auditors and IT auditors will ensure a controlled environment for electronic commerce (Nearer, 2000; and Price, 2001).
The dramatic evolution of information technology has a direct impact on the audit profession and both internal and external auditors. Because the exchange of goods and services become electronic in E-Business, auditors become involved with electronic data in entirely new ways. Conventional, manual audit techniques become inadequate for the electronic environment. Therefore, new skills and knowledge are necessary to ensure that electronic transactions and the resulting growth occur in a controlled environment. Price, (2001) mentioned that “E-Business is one of the most common and complex new business solutions, and there are many issues of which internal auditors should be aware when reviewing such applications”. Nearon, (2000) confirmed that, information technology knowledge would have a distinct advantage in the future market for financial statement audits. Many audit firms has already started to provide the following non-attest services to E-Businesses such as Design and implementation of E-Business software; Integration with legacy accounting systems; and Website hosting.

2

.2. E-BUSINESS IS A RISKY BUSINESS

E-Business is a risky business, a recent survey of 1,600 information technology and security professionals in 50 countries performed by Information Technology magazine revealed that organizations engaging in e-tailing, electronic supply chains and enterprise resource planning are three times more likely than other firms to experience information loss and theft of trade secrets. E-tailing was found to be the most risky activity, with revenue loss seven times more prevalent at Web sites offering E-Business than at non-commerce sites. Similarly, a recent reader survey by Information Security magazine found that organizations engaging in e-tailing are 57 percent more likely than the general business population to experience a leak of proprietary information and 24 percent more likely to experience a hacking-related breach (Price, 2001).

E-Business introduces new risks that enterprises may need to address and by implementing a technology infrastructure and controls to mitigate those risks. Furthermore, E-Business alters the roles and responsibilities of employees and different levels of management, therefore affecting personnel requirements. Moreover, E-Business affects not only business conduct, but also the character of business itself (IFAC, 2002). E-Business must protect its electronic data and infrastructure against the perceived security threats such as unauthorized access to systems and data, incomplete and inaccurate data, confidentiality and privacy of data, denial of services, manipulation and destruction of the data either intentionally or accidentally. A disaster recovery plan should exist to ensure uninterrupted availability of its Web site. Software security and physical security should be implemented to provide assurance that only authorized individuals have access to IT resources and that controls are in place to prevent unauthorized modification or destruction of data, software, and equipment. If these controls are not in place, an increased likelihood of fictitious or erroneous data being entered into the information system exists, which in turn could result in poor management decisions. Software security includes the detection of unauthorized attempts to access restricted data and the use of firewalls to permit only authorized users access to corporate data contained on a website. Physical security measures include putting locks on doors, limiting access to the computer equipment room to authorized individuals, and adopting and testing a disaster recovery plan. Such a plan could mitigate the risk of lost transactions and business interruption if an electronic data interchange (EDI) network were to fail (Abu-Musa, 2003).

In accordance with ISA 400 “Risk Assessments and Internal Control,” the auditor should make an assessment of inherent and control risks for material financial statement assertions. The inherent
risks and control risks in a computerized information systems (CIS) environment may have both a pervasive effect and an account-specific effect on the likelihood of material misstatements, as follows:

- The risks may result from deficiencies in pervasive CIS activities such as program development and maintenance, systems software support, operations, physical CIS security, and control over access to special-privilege utility programs.
- The risks may increase the potential for errors or fraudulent activities in specific applications, data bases or master files, or in specific processing activities.

As new information technologies emerge, they are frequently employed by clients to build increasingly complex computer systems that might include micro-to-mainframe links, distributed databases, end-user processing, and business management systems that feed information directly into the accounting systems. Such systems increase the overall sophistication of computerized information systems and the complexity of the specific applications that they affect. As a result, they may increase risk and require further consideration.

2.2.1. E-Business IT Risks

IFAC (2002) has classified E-Business risks under two main groups: E-Business IT risk and E-Business legal risk. Since E-Business invariably involves the use of the Internet through IT, the most important risks associated with E-Business are IT risks. IT risks includes: IT infrastructure, IT application and IT business process risks. IT infrastructure risks relate to the adequacy of the IT infrastructure for information processing. For example, hardware may be susceptible to malfunction. IT infrastructure risks are addressed by a security concept geared to the needs of the entity and by technical and organizational controls defined on this basis. Typical IT infrastructure risks include:

- Inappropriate physical security measures that do not prevent theft, unauthorized access or improper disclosure of information;
- Vulnerability to overheating, water, fire and other physical risks;
• Inadequate or improper emergency plans and procedures;
• Absence of adequate back-up procedures;
• Inadequate configuration and monitoring of firewalls against intrusion attempts; and
• Inadequate encryption.

However, IT application risks might result from: Bugs and errors in IT applications; Uncoordinated or undocumented program changes; Inadequately designed input, processing and output controls in IT applications; or Inadequate procedures to ensure software security in connection with the security infrastructure (inadequate access authorization concepts and data back-up and restart procedures).

According to IFAC (2002), IT business process risks arise where analyses of security and information processing do not extend to entire business processes, but merely to some parts of them. Such risks may arise from: lack of data flow transparency, inadequate integration of systems or deficient reconciliation and control procedures in interfaces between sub processes arising from the exchange of data between two subsystems within business processes. In this situation, there is a risk that IT controls, such as access rights or data back-up procedures, will be effective only for the sub processes, but not for the aggregated processes.

Typical IT business process risks in an E-Business environment include:

• Transaction data are not transmitted efficiently, completely or accurately from the E-Business subsystem to the accounting application;
• Safeguards protect only a certain subsystem from unauthorized or unapproved transactions and, thereby, allow transaction data to be modified by one of the downstream IT subsystems;
• Improper or inadequate access control mechanisms may make it difficult or impossible to effectively manage access controls for all IT subsystems integrated into the E-Business process;
• Access protection that responds to a single IT application integrated into the business process could be bypassed deliberately by manipulating the upstream or downstream IT subsystems;
• Back-up measures are effective for only the E-Business subsystem and, hence, for the sub process, but not for the entire IT business process; and
• The design and implementation of interfaces between the E-Business subsystem and downstream IT subsystems may not be appropriate.

ISACA (2002) stated that the IS auditor should evaluate the external IS threats to the B2C e-commerce taking into account the nature of the business of the organization. The external threats to be addressed should include denial of service, unauthorized access to data, unauthorized use of the computer equipment, etc., which could arise from various sources, such as casual hackers, competitors, alien governments, terrorists, etc. The characteristics of the business of the organization (intensity of competition, market share, nature and extent of technology usage, innovative/strategic products and or services, etc.) should be used to determine the possible sources of such threats. The likely damage associated with these threats is linked closely to the dependence of the business on the e-commerce processes. The auditor should assess whether the protective measures in place to counter the external threats are commensurate with the level of the assessed risk. In this process, the IS auditor should review the following:

• Technical architecture of the application including the choice of the protocols
• Security architecture of the application
• Virus protection mechanisms
• Firewall implementation: appropriateness of the firewall solution, location of firewall, firewall policies, connections to the firewall and any external connections bypassing the firewall
• Intrusion detection mechanisms
• Existence of relevant logs as well as their ongoing review by competent staff
• Processes in place to verify the compliance with the envisaged architectures, policies and procedures

Billing, (2001) argued that the internet is a global network that enables any computer connected to it to communicate with any other computer, wherever they are, may bring benefits, such as helping maximize access to potential customers, but it also introduces risks. Providing third parties with a connection to the entity’s computer systems increases the risk of unauthorized access to, and manipulation of, applications and data. The level of financial statement risk will be affected by factors such as whether the E-Business systems are separate from, or directly linked to, the accounting systems, and whether the networks are private or public. The method of transferring data between the E-Business and accounting systems can also be risky - manual or poor interfaces may lead to errors in data transfer. Depending on the circumstances, specialist knowledge in areas such as information technology security techniques and understanding software applications might also be required.

2.2.2 E-Business Legal Risks

Management is responsible for ensuring that E-Business operations are conducted in compliance with applicable laws and regulations. Enterprises should be aware that, despite the best efforts of international rule-making bodies, applicable laws and regulations would vary across national boundaries. Nevertheless, enterprises operating in global markets are often not up to date on legal issues and governmental oversight in multiple jurisdictions. Without understanding the regulations and the law applied in different jurisdictions, enterprises may be subject to fines and adverse judgments and may incur other costs, such as legal fees, to defend themselves should they inadvertently breach such laws. Some of the relevant legal issues include:

• Protection of intellectual property, including patent, copyright and trademark laws;
• Enforceability of contracts with Internet service providers; and
• Ownership of software by a software vendor or the right of a software vendor to sell software licenses (IFAC, 2002).

Although e-commerce can open the door to significant opportunities, it can also subject the business to potential legal pitfalls. A company offering goods or services internationally over a Web site may find itself inadvertently infringing the laws of countries in which it trades. Contractual difficulties may also arise from such transactions, particularly when contract terms are not clearly stated or readily accessible to users. In addition, cross-border transactions that fail to specify applicable laws under which the transaction takes place can create jurisdictional problems, and laws that apply to customer data in one country - such as those governing data privacy or intellectual property - may not apply in another (Burr et al., 2002).

Commercial legal risks also arise in connection with contract law and the purchase and sale of goods and services through the Internet across national boundaries. In particular, there may be problems in determining the appropriate jurisdiction for legal actions with respect to cross-border Internet transactions. In addition, it should be noted that certain commercial activities that are not regulated in one jurisdiction might be regulated in another. Management is responsible for ensuring that regulated activities are performed in compliance with the laws in jurisdictions where those
activities are conducted. Billing, (2001) confirmed that an entity's legal registration, its base of operations, its source of goods or services, and its customers, may all be in different countries. It may be difficult in some cases to ascertain which country's laws will apply to the relationship between the trading parties. Ignorance of applicable laws may mean that fines for breaching trading laws, and electronic contracts that are not legally binding and may be repudiated, are among the risks. Also, many countries are still considering and developing laws specifically related to E-Business and, in particular, taxation of internet-based transactions. This means there is a risk that taxes on cross-border transactions may not be correctly recognized and accounted for.

Price, (2001) confirmed that, E-Business transactions can occur at such a fast pace and in such large global volume that continuity is also a major issue. Continuity is defined as a combination of technical and strategic solutions designed to ensure the continuous availability, operation, and high performance of business applications in the event of a disruption or disaster. Natural disasters such as Seattle's recent earthquake can cause mission-critical processes to fail. However, in Seattle's case, the city's business-continuity plan enabled the Department of Information Services to maintain its information technology and telecommunications systems.

Price (2001) has mentioned that another risk of E-Business is that service-level agreements with vendors providing Internet connectivity and network services may not be met or be specific enough to maintain business continuity. Many businesses might find themselves without Internet access especially when their providers shut down practically overnight. Failed or problematic E-Business initiatives could damage a company's reputation and its relationship with suppliers and business partners. Additionally, ineffective E-Business implementations could cost huge amounts of revenue. Emerging new information technology, new E-Business and Web strategies are introduced new risks to many companies.

Auditors need to identify and assess the risks that could lead to material misstatements in the financial statements. Bulletin 2001/3 covers the areas of: knowledge of the business; risk identification and assessment; and specialist skills and knowledge. An appendix to the Bulletin gives some examples of E-Business risks that may affect the financial statements in areas related to:
- The accounting and internal control systems;
- The volume, velocity and nature of transactions processed;
- The taxation, legal and regulatory requirements the entity needs to comply with;
- The accounting policies the entity has chosen;
- Consideration of whether the entity is a going concern (Billing, 2001).

Billing, (2001) argued that, the nature of the E-Business strategy the entity has adopted, and the complexity of its operations, will influence which specialist skills and knowledge are needed, either in-house or bought in from third parties. The auditors may need those specialist skills and knowledge as well, so that they can make appropriate enquiries and understand the implications of the responses. Where the auditors can't call on the necessary expertise within their firm, they may need to consult external experts. The possibility of a relatively high volume and velocity of transactions processed over the internet, and the remote location of some customers, may lead to increased credit risks if, for example, there are inadequate checks to confirm customers' authenticity and integrity. Retailers that do not make adequate credit card checks can find themselves bearing the full cost of fraudulent transactions. A number of entities’ E-Business strategies have led to new accounting issues relating to revenue and cost recognition and the capitalization of certain types of expenditure. The Accounting Standards Board's Urgent Issues Task Force has issued guidance on relevant areas, but entities undertaking E-Business, and their auditors, should still be on the alert.
The recent dot-com failures are proof that the potential for realizing catastrophic loss is greater than some may think. According to Robert Simons, author of Performance Measurements & Control Systems for Implementing Strategy, there are three risk exposures that might affect E-Business: growth, culture, and information management. Risk managers who understand and measure these exposures can approach the risk-management process with greater confidence (Chan, 2001).

3. THE AUDITOR CHANGING ROLE

Auditing E-Business forces auditors to reevaluate the effectiveness of traditional audit procedures, and to explore the possibilities and opportunities by using information technology and data analysis software. Auditing financial statements of E-Businesses according to generally accepted auditing standards (GAAS) presents new challenges for external auditors. Current GAAS contains numerous standards relevant to E-Business, but they are not currently compiled into a single authoritative document. Nearon, (2000) had proposed a guide for external auditors engaged in the proper application of GAAS to audits of E-Businesses is presented. By carefully applying audit standards and increasing their IT knowledge, external auditors could improve the quality of audited financial statements of E-Businesses. Higher-quality financial information about Internet companies allows investors to make better decisions, which reduces stock market volatility and increases the efficiency of economy-wide asset allocations. IFAC, (2002) argued that accountants and auditors will face new challenges and may need to apply new techniques, such as development of accounting systems based on business processes, to ensure that transactions are appropriately recorded, are in compliance with local and international legislation and regulations, and meet current and evolving accounting standards and guidance.

One the most important differences between conventional audit techniques and techniques that utilize data analysis software is the ability to access and analyze all of the data. Instead of evaluating controls relying on samples, auditors can investigate 100 percent of the data using data analysis approach to audit. Without full and unrestricted access to an E-Business’s data, auditors are ill equipped to deal with the challenges posed by the engagement. Data analysis software tools give auditors independent access to a wide variety of electronic data sources. In addition to verifying the accuracy of the company’s accounting records and assessing the business’s exposure risk, E-Business auditors can offer significant value-added services. The electronic nature of the data forces them to use data analysis software tools and techniques. These tools and techniques allow them to go fat beyond traditional audit objectives to offer considerable analytical expertise and value to the organization they serve.

Burr et al. (2002) argued when businesses began adopting e-commerce technology, applications were developed and deployed at a rapid pace, sometimes at the expense of adequate security measures. Unfortunately, many firms did not appreciate the value of addressing security issues up front and spent considerable time and money trying to compensate after implementation. Therefore, ensuring that adequate security measures are in place prior to application development could reduce the likelihood and cost of retrofitting, help maintain the confidentiality of customer information, and safeguard intellectual property. In general, however, a business’ e-commerce security needs can be expressed in terms of four characteristics that represent the value of information

- **Confidentiality:** Covers any business sensitivity, such as access rights, the privacy of data surrounding the customer relationship, and the protection of any information that might have a direct or indirect market impact.
- **Integrity:** Refers to the need for ensuring the accuracy of key data that, if compromised, could result in direct financial loss or customer liabilities.
• **Availability:** Encompasses the business-process and information-systems requirements that help to ensure customer loyalty by enabling information to be accessed whenever needed and protecting that information against loss.

• **Accountability:** Covers the need to preserve a clear, demonstrable record of actions and responsibilities as business is conducted.

• **External auditors should check the automated controls implemented in the e-commerce applications to minimize the risk of unauthorized, invalid, incomplete, or inaccurate data and transactions, as well as to ensure timely processing. Controls should focus on information integrity at the point of entry. The auditor should have sufficient knowledge of the CIS to plan, direct, supervise and review the work performed.**

According to ISACA (2002) the auditor should evaluate the e-commerce objectives, strategy and business model critically. The existing and emerging competition also should be considered in evaluating the relative position of the client’s business. This is essential for evaluating the appropriateness of the objectives and strategies as well as evaluating the effectiveness and efficiency of the B2C application in fulfilling these objectives and strategies. The auditor should evaluate whether the E-Business initiative is a new business by itself or is an additional channel to the existing line of business and to what extent the success and financial viability of the client depends on the E-Business initiative being reviewed. The greater the dependency on the E-Business, the higher the impacts of the risks should they materialize. The IS auditor should review the business case to assess whether the costs and benefits of the E-Business are reflected in an objective manner. Considering the huge and ever-increasing number of Internet users, at times the business potential and volumes are projected at levels way beyond what could be achieved pragmatically. If the IS auditor has concerns regarding the underlying assumptions, the same should be clarified with the appropriate management.

Depending on the E-Business activities permitted by the E-Business application - particularly where transactions and payments are processed - the user should be identified and authenticated uniquely to prevent non-repudiation and to preserve confidentiality. The external auditor should evaluate whether the controls/mechanisms/technologies (ID and passwords, digital certificates, digital signatures, etc.) deployed regarding identification and authentication are commensurate with the intended use of the B2C e-commerce application. The auditor should also verify whether adequate validations built into the application ensure the appropriateness of the data being entered and that such validations are being performed. Whenever E-Business application accepts electronic payments through credit cards, etc., the IS auditor should verify whether there are adequate validation and payment authorization processes to ensure the authenticity as well as the actual receipt of the payments.

In the case of E-Business applications processing transactions and payments as well as accepting and or displaying any personal details confidential in nature (such as statement of accounts), the auditor should verify whether an appropriate encryption technology is being used to encrypt the transmission between the user and the application. Where appropriate and necessary, the IS auditor should ascertain whether the communication across the network is made secure using virtual private network (VPN) and related encryption. The auditor should verify whether there are adequate application controls to ensure the integrity and correctness of the processing.

Some of the E-Business applications require back-end processes for fulfillment of orders, receipt of money, accounting for transactions, etc. While some of this may be handled through detached applications or manual processes, it may call for integration of the E-Business application with some of the other applications. In such instances, the auditor should verify whether there are
sufficient controls including reconciliation processes to ensure integrity of original data across the related applications and processes (including manual processes). The auditor should evaluate the controls over the database to confirm that there are adequate checks and balances to prevent intentional or inadvertent damage, destruction or modification of data. In this context, the IS auditor should review the database access privileges as well as the access logs. The auditor also should review the controls over the archived data to ensure that the confidentiality and integrity are protected adequately. If specialized skills were needed, the auditor would seek the assistance of a professional possessing such skills, who may be either on the auditor’s staff or an outside professional. If the use of such a professional is planned, the auditor should obtain sufficient appropriate audit evidence that such work is adequate for the purposes of the audit, in accordance with ISA 620 “Using the Work of an Expert.”

4. **E-BUSINESS AUDIT OBJECTIVES**

The information systems auditor should, in consultation with the client, where appropriate, define clearly the scope and objective of the review of the E-Business. The aspects to be covered by the review should be stated explicitly as part of the scope. The high-level risk assessment referred to above would dictate which aspects need to be reviewed and the extent and depth of the review. For the purpose of the review, the stakeholders in the solution also should be identified and agreed upon with the client. The auditor should formulate the approach in such a way that the scope and objectives of the review could be fulfilled in an objective and professional manner. The approach followed should depend on whether the review is a pre-review or a post-implementation review. The approach should be documented appropriately. When and where external expert inputs would be used also should be specified as part of the approach (ISACA, 2002).

In accordance with ISA 400 “Risk Assessments and Internal Control,” the auditor should consider the CIS environment in designing audit procedures to reduce audit risk to an acceptably low level. The auditor’s specific audit objectives do not change whether accounting data is processed manually or by computer. However, the methods of applying audit procedures to gather evidence may be influenced by the methods of computer processing. The auditor could use manual audit procedures, computer-assisted audit techniques, or a combination of both to obtain sufficient evidential matter. However, in some accounting systems that use a computer for processing significant applications, it may be difficult or impossible for the auditor to obtain certain data for inspection, inquiry, or confirmation without computer assistance.

An audit of an online E-Business could include the following objectives:

- Verify that all online orders were received, captured, and invoiced accurately in the accounting records
- Evaluate access control to member-only domains

In addition, the audit may also include secondary value-added objectives, such as:

- Analyze trends in online orders
- Identify lost customers
- Substantiate amounts charged to advertisers on the company web site
- Analyze web server traffic to verify management claims regarding web site availability, stability, hits, etc.
- Evaluate efficiency of company’s help disk

In order to achieve the above objectives, auditors must consider the nature of electronic information available, and how to access the data that contains it. While data is plentiful, it often exists in
different forms and on different data platforms. Data analysis software would provide the key to successfully accessing and analyzing incompatible data types. Auditors should know which questions to ask in order to identify the data sources they need, how to access the required data sources, and which data analysis techniques will give them the answer they need. However, most data analysis software supports common operations such as data extraction, and joining of two data files to produce an output file of matched or unmatched records. The auditor should ascertain whether there are appropriate mechanisms to monitor the effectiveness and efficiency of the E-Business on an ongoing basis. This should include the processes to detect and report exceptions so as to prevent errors and frauds.

According to current professional standards, CPA firms that design, implement, or integrate E-Business systems may under certain conditions retain their independence but hosting a client’s website will cause outsiders to doubt the auditor’s independence. Independence rules that prevent CPAs from hosting audit client websites strengthen the profession’s credibility and provide state regulators and the SEC with a strong rationale for continuing the profession’s audit franchise (Nearon, 2000).

In order to exercise due professional care, CPAs must gain a competent understanding of internal controls and the nature of electronic evidence. Due to the nature of E-Business processing, auditors with a detailed understanding of controls will be able to determine whether evidence obtained in substantive tests is sufficient for their audit conclusions. The 1994 Internal Control-Integrated Framework (COSO Report) identified circumstances that increase E-Business risks. In April 2000 the stock market suffered a significant correction, and during the ensuing two months many E-Businesses lost 50-90% of their market value. Before the correction, investors ignored low sales, mounting losses, and continual cash infusions into the Internet sector. Auditors considered whether their dot-com clients satisfied the going concern assumption and determined it was valid because of the commitment by investors to continuously refinance. In the current environment, however, the auditors of an E-Business with no profits on the horizon and low cash reserves should consider qualifying their audit report because of substantial doubts about the entity continuing as a going concern (Nearon, 2000).

5. PLANNING AND AUDIT EVIDENCE

ISACA Standard 060.020 (Evidence) states, “During the course of the audit, the information systems auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence”. While AU section 150.02, Standards of Fieldwork, requires the audit to be adequately planned. According to AU section 326.18, Evidential Matter: Certain electronic evidence may exist at a certain point in time. However, such evidence may not be retrievable after a specified period of time if files are changed and if backup files do not exist. Therefore, the auditor should consider the time during which information exists or is available in determining the nature, timing, and extent of substantive tests, and, if applicable, tests of controls.

In accordance with ISA 400 “Risk Assessments and Internal Control,” the auditor should obtain an understanding of the accounting and internal control systems sufficient to plan the audit and develop an effective audit approach. In planning the portions of the audit, which may be affected by the client’s CIS environment, the auditor should obtain an understanding of the significance and complexity of the CIS activities and the availability of data for use in the audit. This understanding would include such matters as:
• The significance and complexity of computer processing in each significant accounting application. Significance relates to materiality of the financial statement assertions affected by the computer processing. An application may be considered to be complex when, for example:
  - The volume of transactions is such that users would find it difficult to identify and correct errors in processing.
  - The computer automatically generates material transactions or entries directly to another application.
  - The computer performs complicated computations of financial information and/or automatically generates material transactions or entries that cannot be (or are not) validated independently.
  - Transactions are exchanged electronically with other organizations (as in electronic data interchange (EDI) systems) without manual review for propriety or reasonableness.
• The organizational structure of the client’s CIS activities and the extent of concentration or distribution of computer processing throughout the entity, particularly as they may affect segregation of duties.
• The availability of data. Source documents, certain computer files, and other evidential matter that may be required by the auditor may exist only for a short period or only in machine-readable form. Client CIS may generate internal reporting that may be useful in performing substantive tests (particularly analytical procedures). The potential for use of computer-assisted audit techniques may allow increased efficiency in the performance of audit procedures, or may enable the auditor to economically apply certain procedures to an entire population of accounts or transactions.

When the CIS are significant, the auditor should also obtain an understanding of the CIS environment and whether it may influence the assessment of inherent and control risks. The risks and the internal control characteristics in CIS environments include the following:

• **Lack of transaction trails.** Some CIS are designed so that a complete transaction trail that is useful for audit purposes might exist for only a short period or only in computer readable form. Where a complex application system performs a large number of processing steps, there may not be a complete trail. Accordingly, errors embedded in an application’s program logic may be difficult to detect on a timely basis by manual (user) procedures.

• **Uniform processing of transactions.** Computer processing uniformly processes like transactions with the same processing instructions. Thus, the clerical errors ordinarily associated with manual processing are virtually eliminated. Conversely, programming errors (or other systematic errors in hardware or software) will ordinarily result in all transactions being processed incorrectly.

• **Lack of segregation of functions.** Many control procedures that would ordinarily be performed by separate individuals in manual systems may be concentrated in CIS. Thus, an individual who has access to computer programs, processing or data may be in a position to perform incompatible functions.

• **Potential errors and irregularities.** The potential for human error in the development, maintenance and execution of CIS may be greater than in manual systems, partially because of the level of detail inherent in these activities. Also, the potential for individuals to gain unauthorized access to data or to alter data without visible evidence may be greater in CIS than in manual systems.

In addition, decreased human involvement in handling transactions processed by CIS can reduce the potential for observing errors and irregularities. Errors or irregularities occurring during the
design or modification of application programs or systems software can remain undetected for long periods of time.

- **Initiation or execution of transactions.** CIS may include the capability to initiate or cause the execution of certain types of transactions, automatically. The authorization of these transactions or procedures may not be documented in the same way as those in a manual system, and management’s authorization of these transactions may be implicit in its acceptance of the design of the CIS and subsequent modification.

- **Dependence of other controls on computer processing.** Computer processing may produce reports and other output that are used in performing manual control procedures. The effectiveness of these manual control procedures can be dependent on the effectiveness of controls over the completeness and accuracy of computer processing. In turn, the effectiveness and consistent operation of transaction processing controls in computer applications is often dependent on the effectiveness of general CIS controls.

- **Potential for increased management supervision.** CIS can offer management a variety of analytical tools that may be used to review and supervise the operations of the entity. The availability of these additional controls, if used, may serve to enhance the entire internal control structure.

- **Potential for the use of computer-assisted audit techniques.** The case of processing and analyzing large quantities of data using computers may provide the auditor with opportunities to apply general or specialized computer audit techniques and tools in the execution of audit tests. Both the risks and the controls introduced as a result of these characteristics of CIS have a potential impact on the auditor’s assessment of risk, and the nature, timing and extent of audit procedures.

The challenge is that the audit evidence is in electronic form, and that the volume of electronic data accumulated by an E-Business is enormous. E-Business auditors must be able to access a wide variety of data types, and then sift through large data sets to identify trends and irregularities. Therefore, auditors are increasingly relying on data analysis techniques for auditing E-Business. Nreon, (2000) mentioned that, Adequate planning of E-Business audit procedures is critical because most of the audit evidence is in electronic form. In some cases, there may not be any physical evidence, for example the online sale, purchase, and delivery of music, books, documents, and information. Evidence of subsequent settlement may also exist only in electronic form. In such situations, auditors should begin audit procedures during the fiscal year in order to ensure that sufficient evidence is available.

Automatic processing of customer orders is one of the keys to the profitability of an E-Business. The online sale cycle starts with an online order form the customer via the Internet. Accompanying the online order will be the customer’s credit card detail as payment. Electronic payment and updating of the accounting records will take place automatically when title is shipped to the customer. The entire sales cycle is captured electronically in real time. There is no physical evidence of the transaction. It would be unrealistic to expect such a business to produce a hard copy of all orders, invoices, payments, and bank statements only for audit purposes. E-Business needs fewer administrative controls such as manual reconciliation, segregation of duties and so on. This means there are few manual controls available to the auditor. Most controls will have to be integrated into the electronic business applications, such as electronic verification of credit card details, protection of access to web servers and to accounting records and so on.

Nreon, (2000) argued that, by 2005, the entire supply chain will be automated and, over the next five years, will witness enormous pressure on all companies to conduct business electronically. 7 Because E-Business transactions will affect all entities, practitioners should begin ascertaining their
audit clients’ involvement in E-Business as soon as possible. A logical starting place is to include considerations about the nature of actual and planned Internet operations in engagement acceptance procedures. Many boards of directors are keenly aware of the opportunities and threats the Internet poses and their minutes often reveal the client’s E-Business strategy. Budget reports also provide indications of Internet activity, but projected E-Business revenues and expenses may be lumped in with other sales and expenses, or combined in the technology or marketing budget. Unusual projected increases in these areas may indicate the client’s planned involvement in the Internet. An obvious place to find evidence of the client’s E-Business activity is the web itself. The client’s website should be carefully examined and an Internet search for indications of the client’s E-Business activity conducted.

6. ADEQUATE TECHNICAL TRAINING

External auditor should ensure that he/she has the necessary business knowledge and technical training to audit the E-Business transactions. According to ISACA (2002) the IS auditor also should ensure he/she has access to the relevant technical skill and knowledge to carry out the review of E-Business application. Such reviews would call for technical knowledge to evaluate aspects, including the encryption technologies used, network security architecture and security technologies, such as firewalls, intrusion detection and virus protection. The IS auditor should have adequate knowledge to review these aspects. Where expert inputs are necessary, appropriate inputs should be obtained from external professional resources. The fact that external expert resources would be used should be communicated to the client in writing. Again, ISACA Standard 04 (Competence) confirmed, “The information systems auditor is to be technically competent, having the skills and knowledge necessary to perform the auditor’s work. The information systems auditor is to maintain technical competence through appropriate continuing professional education”.

According to AU section 210, Training and Proficiency: The audit is to be performed by a person or persons having adequate technical training and proficiency as an auditor. It should be recognized that the training of a professional person includes a continual awareness of developments taking place in business and [the] profession. One possible concern is that college accounting programs trail other business disciplines in adopting formal E-Business curriculums. Although most of the top business schools offer E-Business courses, few accounting schools do. If accounting schools placed greater emphasis on technical competence, clients and regulators would feel more confident that CPAs have the requisite skills to audit E-Business. And as E-Business expands to encompass the majority of financial transactions, the accounting profession's audit franchise can be strengthened by the perception that CPAs are the most qualified professionals to serve the E-Business audit market (Nearon, 2000).

7. INDEPENDENCE

ISACA Standard 020 (Independence) states, “In all matters related to auditing, the information systems auditors are to be independent of the auditee in attitude and appearance. The information systems audit function is to be sufficiently independent of the area being audited to permit objective completion of the audit”. While AU section 220, Independence, the second general standard states that: In all matters relating to the assignment, independence in mental attitude is to be maintained by the auditor or auditors. The auditor is required to perform the engagement without bias and should avoid situations that might lead outsiders to doubt the auditor’s independence. With respect to E-Business, an audit firm could be providing nonattest services to a client that would cast doubt on an outsider's perception of the firm's independence. Some CPA firms design, implement, or host client websites. Hosting a website could mean that the audit firm has physical control of the client’s
web servers, serves as network administrator or webmaster, or maintains the E-Business software and databases. Some CPA firms that host websites for nonpublic companies do not think this service impairs independence, likening it to providing bookkeeping services. According to ET section 101, Independence, an audit firm’s independence would be impaired if the firm supervised client personnel in the daily operation of a client’s information system or managed a client’s local area network. Although hosting or managing a website is not specifically addressed in the ET standards, the extension of the logic and intent is obvious. An outsider might reasonably doubt the independence of a firm that hosts a client’s website (Nearon, 2000).

Even if one makes the analogy that a website is like a bookkeeping service, according to ET section 101.05, independence would be impaired if the auditor determines or changes journal entries or account classifications for transactions or other accounting records without obtaining client approval, prepares source documents or originates data, or makes changes to source documents without client approval. Because a website that conducts E-Business transactions could be performing all of the above functions under the control of the server host, webmaster, or network administrator, an outsider might believe auditor independence has been impaired. For auditors of public companies, the case against hosting an audit client’s website is even stronger.

It is the Commission’s position that an accounting firm cannot be deemed independent with regard to auditing financial statements of a client if it has participated closely, either manually or through its computer services, in maintenance of the basic accounting records. ... In this situation the accountant, by preparing the basic accounting records, has placed himself in a position where he would be reviewing his own record keeping and could therefore appear to a reasonable third party to lack the objectivity and impartiality with respect to that client which an independent audit requires. Neither case specifically addresses Internet hosting, but the intent of the SEC is clear. A client’s website hosted by its auditor records transactions and performs both bookkeeping and computer processing. According to the SEC, both of these activities, separately or taken together, impair independence (Nearon, 2000).

8. INTERNAL CONTROL AND EVIDENTIAL MATTER

The International Auditing Practices Committee (1991) mentioned that, the use of computers might result in the design of systems that provide less visible evidence than those using manual procedures. In addition, these systems may be accessible by a larger number of persons. System characteristics that may result from the nature of CIS processing include:

a. Absence of input documents. Data may be entered directly into the computer system without supporting documents. In some on-line transaction systems, written evidence of individual data entry authorization (e.g., approval for order entry) may be replaced by other procedures, such as authorization controls contained in computer programs (e.g., credit limit approval).

b. Lack of visible transaction trail. Certain data may be maintained on computer files only. In a manual system, it is normally possible to follow a transaction through the system by examining source documents, books of account, records, files and reports. In a CIS environment, however, the transaction trail may be partly in machine-readable form, and furthermore it may exist only for a limited period of time.

c. Lack of visible output. Certain transactions or results of processing may not be printed. In a manual system, and in some CIS, it is normally possible to examine visually the results of processing. In other CIS, the results of processing may not be printed, or only summary data may be printed. Thus, the lack of visible output may result in the need to access data retained on files readable only by the computer.
d. **Ease of access to data and computer programs.** Data and computer programs may be accessed and altered at the computer or through the use of computer equipment at remote locations. Therefore, in the absence of appropriate controls, there is an increased potential for unauthorized access to, and alteration of, data and programs by persons inside or outside the entity.

According to AU section 150, Generally Accepted Auditing Standards: A sufficient understanding of internal control is to be obtained to plan the audit and determine the nature, timing, and extent of tests to be performed. Sufficient competent evidential matter is to be obtained through inspection, observation, inquiries, and confirmations to afford a reasonable basis for an opinion regarding the financial statements under audit. Proper application of these standards is critical for audits of E-Businesses because the inherent nature of electronic evidence requires internal control for electronic transactions. According to Auditing Procedure Study, The Information Technology Age: Evidential Matter in the Electronic Environment, the basic accounting issues in an electronic environment are the validity, completeness, and integrity of the accounting records. The relevant auditing and internal control concepts are segregation of duties, information security, and techniques for error correction. In an E-Business environment: The intended purpose of electronic evidence does not differ from traditional forms of evidence, but it is distinguished by the need for controls to ensure validity. The competence of the electronic evidence usually depends on the effectiveness of internal controls over its validity and completeness (Nearon, 2000).

E-Business involves obtaining details about the customers and prospects using and or transacting through E-Business applications. ISACA (2002) confirmed that the privacy of such details should be ensured. In other words, the details gathered should be used for the intended purposes only and, as per the agreement, with the persons providing the information. There are various legal provisions being evolved in various countries. In this context, any review of E-Business should address the compliance with the legal provisions of the relevant countries as well as the best practices relating to privacy. According to ISACA (2002) Application audit trails have more significance in the E-Business environment, due to the absence of paper trails for the transactions and payments. In this context, the review of E-Business should address the adequacy of audit trails as well as the processes for reviewing the audit trails. This would be important from the point of confirming the authenticity and integrity (including non-repudiation) of the transactions. As against other channels of business, E-Business depends largely on the availability of the application and the access to the Internet. In this context, there should be appropriate capacity planning processes, redundancies and fallback options as well as disaster recovery procedures in place for both the system and communication link. These should be given due attention while evaluating the availability aspects of the E-Business application. Integrity of data between the E-Business application and the related back-end applications and processes (including manual processes such as delivery/dispatch, receipt of non-electronic payments, etc.) is an important aspect. The adequacy of the application and manual controls to ensure such integrity should be an essential part of the E-Business audit. E-Business involves receiving online payments, therefore appropriate processing controls should be implemented to obtain authorizations for the payments and to ensure that the considerations are duly received. In such cases, the appropriateness and adequacy of the controls need to be evaluated as part of the E-Business audit.

According to AU section 326, Evidential Matter: If control risk is assessed at a maximum, an auditor who performs only substantive tests of electronic evidence may not be able to obtain sufficient competent evidential matter. Electronic evidence adds new dimensions for the auditor's consideration, such as the reliability of the system producing and controlling evidence. Frequently, E-Business applications run on operating systems with security weaknesses that render them unreliable. Often, E-Business software is custom written and lacks controls. Even some commercially available packages are developed and implemented without consideration of internal
controls. However, without testing the internal controls surrounding the electronic evidence (for example, controls over generation, storage, manipulation, and transmission), a lack of credibility may not be recognized by the auditor. In order to audit E-Business transactions, the auditor will have to perform special procedures: The auditor may be required to use report writers, specialized audit software, data extraction tools, or other system-based techniques in order to use the information in electronic form (Nearon, 2000).

In order to audit E-Business transactions, the auditor must have access to the underlying system and data, but the client's IT department may be reluctant to grant the auditor access. For some clients, accounting records may be processed and stored by third-party Internet service providers (ISP). In the past, an auditor could sometimes obtain an SAS 70 report from a computer service bureau's auditor on the policies and procedures placed in operation and possibly on tests of operating effectiveness. In today's environment, an auditor generally cannot obtain an SAS 70 letter from an ISP that hosts a client's E-Business. If the volume of a client's E-Business transactions processed by an ISP is material to the financial statements, lacking an SAS 70 letter or access to the ISP could cause a scope limitation when the auditor is unable to obtain a sufficient understanding of internal control.

E-Business operating and application systems are new, yet their expected useful life is only about two years. Even established E-Businesses continually upgrade their systems and make significant modifications. Existing companies that add Internet operations face the complex task of integrating E-Business technology with legacy systems. Often, the new and old systems have radically different architectures. The pressure of fast track development and implementation creates an atmosphere in which the existing controls in legacy systems may fail when they are merged with or replaced by new systems. Implementers of new Internet systems want to "go live" as soon as possible, and controls are often an afterthought. Nearon, (2000) argued that once new Internet operations get their site up and running, many become the victim of their own success if maximum capacity is reached sooner than expected. If this occurs, controls over other functions such as fulfillment, customer service, and support may break down under unanticipated demand. Existing supervisors might not be able to maintain control of hastily added additional support systems. In addition, excess demand on unreliable operating systems may cause frequent server crashes, resulting in lost accounting records. Moreover, when new technologies are incorporated into existing systems, previously reliable internal controls may no longer be effective. As companies add new E-Business lines and activities, managers may be unfamiliar with the control features of the new systems. For new systems, as well as those merged with legacy systems, this unfamiliarity could result in a serious under Auditing E-Business estimation of risk.

ISACA (2002) mentioned that E-Business quite often involves use of third-party service providers for various aspects, such as application development and maintenance, managing the web site and related databases. In such cases, the appropriateness and adequacy of the controls and contractual protection which ensure appropriate levels of service and the protection of the information relating to the organization and its customers, needs to be evaluated as part of the E-Business audit.

9. GOING CONCERN

Auditors of E-Businesses need to take a hard look at their clients' short-term expected cash needs and cash generating abilities. The conjunction of low sales, a high ratio of marketing costs to total expenses, low (less than 12 months) cash reserves, and dependence on funding continued operations with new cash infusions from investors should raise doubts in the auditor's mind about the entity's ability to continue as a going concern. Nearon, (2000) argued that many Internet companies that counted on continued funding by investors have shut their doors or gone bankrupt, and Silicon
Valley lawyers are expecting many more such failures. Most dot-coms are not expected to survive, and in such an environment auditors should carefully consider the provisions of AU section 341, The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern. Indications of substantial doubt about the entity’s ability to continue as a going concern include negative financial trends and the need to seek new sources or methods of financing. Ordinarily, information that significantly contradicts the going concern assumption relates to the entity’s inability to continue to meet its obligations as they become due. If the auditor believes there is substantial doubt about the entity’s ability to continue as a going concern for a reasonable period of time, he should obtain management’s plan to mitigate the conditions and assess the effectiveness of the plan. If the auditor concludes there is substantial doubt, he should consider the adequacy of the disclosure about the entity’s inability to continue as a going concern and include an explanatory paragraph in his audit report to reflect his conclusion.

10. CONCLUSION

E-Business has become an important and necessary business tool since many companies are using the Internet to conduct their transactions and it is expected to continue their exponential growth in the near future. E-Business introduces new challenges to conventional external auditors and the audit profession. Therefore, conventional manual audit techniques become inadequate for the electronic age. External auditors need to understand how the advanced technology affects their audit process. They also need to acquire the necessary knowledge and skills about this technology to be able to deal with the audit of electronic transactions on a daily basis using continuous audit approach. Adequate planning of E-Business audit procedures becomes critical because most of the audit evidence might be available only in electronic form. External auditors should be able to evaluate the adequacy and accuracy of the electronic audit evidences. External auditors need to judge the validity, completeness, and integrity of the accounting records; and the ability of the company to satisfy the going concern assumption. External auditors should also acquire the technical skills necessary to audit E-Business and maintain independence to enhance the profession’s credibility. Auditing E-Business forces auditors to reexamine and evaluate the effectiveness of traditional audit procedures. They should also explore the possibilities and opportunities of using information technology and data analysis software. The current paper examined the auditing process of E-Business as a new challenge to external auditors and audit profession. It proposed some guidelines that might help external auditors in facing such challenges.

REFERENCES


