General Guidelines of Internal Control over Internet-based Electronic Commerce

Wenli Wang
Emory University
wenli@wenli.net

Minnie Yi-Miin Yen
University of Alaska Anchorage
afmyy@uaa.alaska.edu

Abstract

The rise of the Internet as the medium for electronic commerce (EC) has changed many of the company's business applications. The needs of successful implementation of Internet-based EC applications must be viewed as part of an overall integrated solution to an organization's business requirements. A broader business needs, goals and advantages of developing Internet-based EC applications need to be considered and analyzed while many business processes are required to be reengineered. These changes in businesses as well as in technologies introduce risk that could be minimized through effective internal control implementation and review. The purpose of this paper is to provide internal auditors and the management the general guidelines of developing internal control procedures that should follow the system development life cycle (SDLC) approach and be designed and implemented simultaneously with the development of the Internet-based applications. In addition to describe the fundamental objectives and characteristics of the Internet-based internal control, this paper also discusses many of the design, implementation and monitoring issues important to managers and auditors in developing the internal control systems.

1. Introduction

The growing area of Internet-based Electronic Commerce (IEC) requires a new business paradigm in today's society. In a broad sense, EC is any electronic communication carried out in support of business initiatives. Early EC business transactions processing between entities were conducted on strictly internal LANs or through proprietary value-added networks. The transacting entities were usually technologically proficient and had pre-established contractual relationships with each other. While Internet-based EC activities continue to be defined as the exchange of goods or services for money, or the transfer or exchange of some form of financial instrument by using an electronic medium, the Internet's open and inexpensive access to millions of potential customers creates EC opportunities for companies who could not afford proprietary network systems. In this case, the Internet becomes an enabling technology for an organization to adopt this new form of EC. The needs of successful implementation of Internet-based EC applications must be viewed as part of an overall integrated solution to an organization's business requirements. The Internet should not be used as a stand-alone technology to be simply retrofitted to the existing structures.

In organizations, no matter how much change occurs in their transaction components, platforms and environment, the final goals remain the same: high profitability, successful and continuous business operations, reliable financial reporting are compliance with laws and regulations [1]. These basic internal control objectives are important components in developing the trust of capital providers and others transacting business with an organization. Those who transact with the firm are concerned about profits, about the efficiency and effectiveness of operations and continuing assurance that the organization will remain viable in the long term. Internal control systems contribute significantly to meet the needs of all stakeholders by providing assurance that assets are safeguarded, accounting data are accurate and reliable, operations are efficient and the firm adheres to managerial and legislative policies. However, how to design an efficient and effective internal control system in the new Internet-based EC environment in order to achieve its goals is an important challenge for the organizations. It is believed that to solve these problems in design, implementation and monitoring Internet-based application systems successfully are the responsibilities of management, external and internal auditors.

Effectively integrating Internet-based applications into an organization's information systems involves a wide variety of business and technical issues, such as aligning the implementation of Internet-based applications with an organization's business strategy; following the organization's business goals and long-term system development plan; effectively integrating Internet-based applications into an organization's application systems environment; considering the design of the Internet data communications infrastructure, and other related issues in implementing Internet-based applications. However, it is important to emphasize that all detailed design and implementation issues emanate from the business requirement analysis of stakeholder needs, business goals, and business strategic planning. The general business analysis will help to determine many of the detailed information systems and internal control systems design characteristics first. Then the system development life cycle (SDLC) phased approach will follow it with system analysis, system evaluation, logical design, physical design, system implementation and maintenance tasks in an iterative but continuous improvement manner. By following this structured approach, the organization will assure that controls designed to implement efficient and

effective business processes in support of daily transactions and management information needs and monitoring their processes and data will not only provide assurance of the reliable transaction information but also keep these transactions consistent with the business goals.

The purpose of this paper is to provide the management, internal and external auditors the general guidelines of developing internal control procedures in the Internet-based environment. The control system development should follow the system development life cycle (SDLC) approach and be designed and implemented simultaneously with the development of the Internet-based business applications. This paper discusses many of the design, implementation and monitoring issues important to managers and auditors. By following the SDLC approach to develop the internal control system, the organization starts with the analysis phase. This includes requirement analysis of the internal control systems with a discussion of IEC risks, the rationale of IEC internal control, IEC control environment and IEC control objectives respectively. Next, the fundamental characteristics of an Internet-based internal control system are discussed and developed as the basis for general guidance in the system conceptualization and physical design processes. Ones who design and implement Internet-based applications should keep these control characteristics in mind. Finally, the more detailed consideration is going to internal control systems transactions processing design. This last section is divided into the traditional general control and application level control concerns.

2.Needs of Internal Control

IEC is growing fast. The success and continued growth of IEC is based on the technology development and business opportunities. IEC is offering some compelling benefits and potentials to its participants through continuous efforts in its technology enhancement. For example, open and inexpensive access to millions of potential customers creates opportunities for companies planning to provide financial transactions and related services on the Internet. Enterprises that have implemented Internet-based applications as part of a business strategy have been successful in reducing business cycle time, improving cash flows, reducing inventories, decreasing administrative costs, and opening new marketing and distribution channels. Although all player groups will eventually benefit as IEC expands, IEC raises important new issues and challenges that cannot be overlooked if a company is to succeed.

The new phenomena of IEC and the emerging new Internet technologies introduce new types of threats and risks to the business world:

1. The interconnectivity and openness not only make the man-in-the-middle attack and unauthorized access easier, but also create lack of trust issues such as lack of trust in players' identities, lack of trust in players' credibility and lack of trust in players' information systems. Unlike the traditional EDI type EC business, conducting Internet-based EC activities often involves transactions between strangers. Because of the anonymity of electronic commerce and the ease with which the electronic identities can be established and abandoned, it is crucial that people know that the entities follow and disclose certain business practice. Given the openness of the Internet and packet switching protocol used in the data transmission, the assets of the Internet-based EC applications are more vulnerable than in traditional electronic or manual systems. Assuring that Web information business entities and the resulting transactions can be trusted is a major concern for all EC participants.
2. Globalization and virtualization enlarge the scale and scope of IEC risks. Computing power, connectivity and speed of computerized transaction processing can spread virus, system break-ins or even errors in seconds and affect interconnected parties. The openness of the Internet results in a highly networked and interconnected IEC business environment. This highly connected network infrastructure increases the inter-links of businesses. However, it also raises the range and magnitude of risks. IEC's wide interconnectivity with outside marketplace makes the organization more prone to external partners' and societal failures. Internet failure could trigger a severe domino effect across all infrastructures' components. This risk can be aggravated by the IEC system features of high-speed system, large transaction volume, and low human intervention. When such a system fails, it fails fast and in a dramatic way. Sharing of technology and information enhances business opportunities with trading partners and third parties as well as increases cross-vulnerabilities.
3. New forms of IEC business assets exposed in IEC environment and result in vulnerability. The IEC business assets are one of the primary targets for damages and theft. Besides the traditional assets listed in the financial report, such as current assets (cash, accounts receivable, inventory, etc.) and fixed assets (buildings, manufacturing and office equipment, etc.), there are assets specifically important to Internet applications (See Table 1). A lot of innovative IEC firms have insignificant physical presence, they possess few of the traditional assets associated with traditional businesses. In Table 1, the assets are categorized by following the categories of information system components. But in the example column, the components that are vital for the functioning of IEC applications are listed.

   The theft of IEC assets can be caused in a variety of formats. Theft of computing resources is a popular type of embezzlement. These Computing resources include CPU time, hard disk spaces, computer memory, cache, input/output ports, etc.

Table 1. Assets of an IEC Business

Assets Cat.	Sub-Category	Examples
Hardware	Hosts/Nodes	Workstations, Servers, Printers; Hubs, Routers, Bridges, Gateways, PBXs; Data Storage Facility
	Links	Cable: Twisted pairs, Coaxial, Optical Fiber, Microwave
Software	System	Operating System
	Purchased Applications	Application packages, Database Management Systems, Web Browsers, Video-Conferencing, and other Software
	In-house Applications	Homepages, CGI Scripts, Special business-related Applets, Internal Collaboration
Data	Digital Products	Research Report, Software, Digital publishing, Entertainment Content
	Digital Process Record	Financial Information, Transaction Trail
Processes	Management	Strategy Planning
	Transaction	Purchasing, Marketing, Selling, Manufacturing
	Internal Control	Monitoring, Reporting
Personnel	Management	CEO, Managers
	IS Personnel	CIO, System Administrator, System Maintenance Personnel, WebMaster
	Operators	Digital Products Creators, Inventory Custody Personnel, Sales, Computer Operators
Market Presence		Brand Name, Reputation, Customer Base, Public Relations, Market Strength and Market Shares

The theft can not only slow down or block the legitimate use of the same resources in conducting normal business functions but also help crackers to collect enough power to run "brute force" attacks against system security. Traditionally, sabotage means physical damage to physical resources. In IEC, sabotage is more likely to be the digital damages to resources, both physical and electronically. Damage of physical computing facilities may be done without physical access. Some software will allow a cracker to remotely reconfigure, disable, or damage hardware such as drivers. Electronic deterioration, such as erasure, data distortion, data loss, or data intractability and modification of message sequences and timing can seriously damage the content of IEC business database and warehouse.

4. Ever-changing environment imposes changes in risks. The continuously changing technological, economic, industrial, operating and regulatory conditions of IEC not only introduce special types of risks, but also continuously reform and add new risks. Advances in Internet technology not only support IEC, but also advance the hacker's tools as well. Hacking techniques never stop evolving. "Repudiation" and "replay attack" are two examples of special forms of Internet fraud.

Internal control systems contribute significantly to the traditional businesses for assurance of safeguarding assets, providing assurance for the accurate and reliable accounting data, efficient operations, and for adhering to managerial and legislative policies. Computer security functions such as access control, logging and backup system also provide a mechanism to protect the business transaction system to certain extent. However, many traditional control and security mechanisms can be challenged on effectiveness and efficiency grounds in the new IEC context.

Online digital transactions challenge the concept of "isolated" basic business transaction cycles. The powerful software programs and fast transaction processing may bypass some of the traditional steps in manual transactions and empower individuals with additional necessary privileges. The potential loss of traditional controls, such as separation of duties, when coupled with the speed of transaction processing, challenges existing control and audit technology. Distributed transaction processing further challenges our ability to reconcile transaction records. In a timely basis, these less strict boundaries of virtual organizations require fine grained access control and strong authentication procedures not currently in place. Digital online transactions with their new set of characteristics demand new ways of control.

Defenses that are imperfect and static create increasingly vulnerable as the technology changes. Even though they have once provided perfect protection, from a system perspective, no security technology is perfect, particularly in a changing environment where systemic variety prevails, failure of the technology is merely a matter of time. Control and security systems that are not dynamic cannot fight against changing forms of threats and risks are sometimes even worse than no control and security at all. Often, the security systems capture the trust of the IEC business player, but not function or continue to function as claimed as the environment changes. Mediocre security technology may remove the impetus for development and deployment of higher quality security technology. Therefore, the IEC internal control system should be designed in a more aggressive, preventive and proactive manner.

3. IEC Control Environment Issues

The control environment is the collective effect of various factors on establishing, enhancing, or mitigating the effectiveness of specific policies and procedures. In other words, the control environment sets the overall tone of the organization and influences the control consciousness of

the employee. It is the foundation for all other components of internal control. The control environment has a pervasive influence on the way business activities are structured, objectives established and risks assess. It is executive management's responsibility for the internal control systems. It is executive management's job to set "tone at the top" by creating a control environment. The control environment reflects the organization's general awareness of and commitment to the importance of control throughout the organization. In other words, by setting the example and by addressing the need for control in a positive manner, management can make an organization control conscious.

Since the IEC business environment and the way of doing business in IEC change dramatically, to create a positive and responsive control environment for IEC businesses becomes a big challenge for their managers. Although the way of doing business and the objectives of IEC internal control systems may be changed or enhanced, the fundamental factors which will help to establish a good control environment are still stayed the same. Management philosophy and operating style is important to create high morale and an atmosphere conducive to IEC security. All employees should recognize IEC's risks and threats and the scope of damage it can cause. The audit committee appointed by the board of directors should be responsible for internal auditing functions and periodically consult with the external auditors and top management as to the performance of internal control and security systems. It is important to establish controls relating to the use and accountability of all resources relating the computer and IEC system. The responsibilities of all IEC positions should be carefully assigned and documented using organization chars, policy manuals, job descriptions, and so on. Good relations and effective communication must be kept with employees, business partners, and its associates. The internal control system must be constantly monitored and audited and then modified to meet changing needs. The internal control policies and procedures should be established to the maintenance of current IEC system and future changes to the systems. Internal control policies and procedures should be tested for both compliance and effectiveness.

While some of the fundamental factors need to be reevaluated carefully when establishing an IEC control environment, some other new issues arise in IEC environment and need special attention and discussion. These factors and issues include blurred control boundaries, personnel policies and practices and external influences.

1. Blurred Control Boundaries

When IEC business evolves with integration of systems, high connectivity and openness to global reach, requirement of controls from IEC business evolution represents higher level of sophistication, dependency, and vulnerability. The blurred control boundary issues can be addressed from internal structure and external boundary perspectives based on an organization's IEC business evolution.

When an organization is exploring its IEC business development in the lower levels of evolution, this is especially important when an organization implemented its IEC systems by only taking advantage of its popular medium but handle the same business functions that are also running in the traditional legacy system. In other words, the same business functions may be handled parallel by two different systems, one on IEC and another on traditional system in order to get the best effects for the organization. How to allocate, aggregate and coordinate the job responsibilities and human resources of developing and running these duplication functions in the organizational structure is important. Especially when the IEC application development needs employees with special expertise in graphic and multimedia design, content management and man-machine interface implementation that are different from traditional IS development.

When the IEC applications move from the fundamental web activities to more complicated and sophisticated IEC activities, the control boundaries issues addressed specifically on designating how to integrate these front-end and back-end systems, internal and external systems and who is responsible for these systems integration are the critical issues. Based on the requirements of the IEC business, the functions of the IEC applications can be categorized into front-end merchandising, back-end fulfillment and other supporting features. The front-end merchandising features can include but not limit to search capabilities, product content, product pricing, customer profiling, shopping basket, product bundling and configuration. The back-end fulfillment features include order processing, payment, shipping, order tracking and optimization while the other supporting features include customer service, business image promoting and advertising, and general security and privacy protection.

The management who are responsible for establishing internal control systems should have a through understanding about these changes and how they will affect the organizations in order to take appropriate actions in making the sound control environment possible.

2. Personnel Policies and Practices

Since it is such a new practice and requires such new ideas supported with cutting-edge and emerging technological skills in IEC, intellectual assets should be prized with much heavier weights than its book value. These intellectual assets usually include people's experience, creativity, intellect, and overall brain power. It is always crucial for an IEC business with creative ideas, to successfully speed up the move from concept to customer, from new ideas through its development and

delivery. For each individual employee, in order to keep being competitive and marketable and let the market determine his/her worth, continuous job training to keep up with the current technological skills and accumulate personal intellectual capital becomes important.

In IEC, an organization should determine how much of its market capitalization and value the company by its growth rate. How does its market capitalization per employee compare with that of other companies making comparable offers or employing comparable talent? In today's competitive and ever changing job market, talented work forces will either be recruited or hired through subcontracting and outsourcing arrangement. Eventually, the talent will often flow to the companies that offer real wealth. In this case, the loyalty toward an organization and professional ethics that has been valued and praised in the past are often belittled and even ignored in this new IEC era. How to keep professional ethics and enforce a positive control environment through personnel policies and practices is an important issue for IEC businesses.

It is impossible to expect formal control policies and procedures can eliminate all risks in highly utilized and computerized systems. The possibility of internal abuse by employees and external intruders always exists. Sense of control and security are established when IEC staffs recognize the risk and threats that systems encountered and the loss due to the compromise of systems. If the sensitivity and cross-vulnerability of IEC applications are recognized by employees, the commitment of responsible members of organization members and their being proactive in security-related behaviors are important, especially for such highly privileged users as system programmers, operators, IS auditors, and security officers. When IEC systems become more integrated and complicated, the transaction amounts, processing loads, and technical complexity increase. At the same time, the probability and consequence of risks can be highly increased and diverse. It is important that organizational member have appropriate commitment and experience to adjust their control activities to be prepared for unexpected risks.

However, in addition to wealthy reward, a variety of intangible rewarding and recognition of individual achievement can be rendered through creating a stimulating work environment with job satisfaction, accountability, privilege, ruling power and accomplishment for the employees. New personal policies and practices are needed to attract and keep the best and capable work force in IEC and it is a critical issue for the executive management.

3. External Influences

The IEC information systems and applications must be in compliance with all federal, state, and local laws and regulations. Among other things, these laws and regulations govern the security and privacy of many types of data, including those relating to customer credit, purchase history, personnel, and government-classified records. They also govern the exportation of certain information to other countries. Copyrighted software and information protection is also an important issue that needs to implement a well-documented internal policy for keeping the company from a variety of legal attacks.

However, technology always changes faster than government can change the regulations to address it. So far, IEC activities and applications often change much faster than the policy makers and lawmakers are capable of addressing [4]. In the mean time, for every IEC movement, the organization should pay attention to the external influences from all aspects of market and address what market wants to create a positive control environment. Because of this open and rapid changing environment, organizations in IEC should be alert to the market signals, de facto standards, and judged by the rules of the market in establishing their control environment.

4. IEC Control Objectives

Fundamental organizational goals remain the same no matter how much change occurs to the component parts of the commercial enterprise. In IEC, the information infrastructure is primarily the Internet and the players, products and services, and transactions become partially or entirely digital, yet the ultimate objective of an IEC business is to achieve its mission and to reach its profitability goal.

While IEC businesses, like all businesses, strive for higher performance, lower costs, and greater productivity, appropriate internal control should be given a prominent role in the firm’s processes. Internal control will serve IEC business practices by achieving control objectives consistent with the business mission and goals. Sound internal controls will provide reasonable assurance to the board of directors, management, employees, and external parties such as investors, legislators and regulators, that the firm’s mission and goals are met, business processes are sound and secure, and information disseminated for their use is relevant and reliable.

In IEC environment, in addition to the objectives of traditional internal control, such as safeguarding of assets, assuring accurate and reliable accounting information, efficient and effective operation, the control objectives of all IEC business processes should achieve confidentiality, integrity, authorization, authentication, and non-repudiation.

1. Confidentiality: This criterion is to protect information content the process possesses from unauthorized access and to prevent disclosure of information content to other related processes unless it is necessary.

2. Integrity: This criterion relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities. This is to guarantee that information pertained to a process is not altered by unauthorized access or due to errors. Process specific information includes information regarding internal events of the process and the messages communicated with this process. It is essential to take steps to ensure that all data is maintained in its intended form.

3. Authorization: This criterion refers to the property that a process of a transaction has permission to access resources and the process is only accessible to privileged players.

4. Authentication: This criterion relates to the assurance that people or systems are who they claim to be. Authentication is the ability of a process of identifying itself in order to access resources and identifying players who have privileged access to this process.

5. Non-repudiation: This criterion relates to the ability to consummate a transaction without fear that one party will back out. This is the provision of information with the assurance that an initiated transaction will be completed by all the parties involved.

After we understand the control objectives and the special needs of the internal controls, the guidelines described in the next section can help the management, internal auditors and the systems designers understand the important issues and concerns in developing the internal control procedures. These procedures should be analyzed and designed simultaneously with the Internet-based applications development.

5. Characteristics of Internet-based Internal Control

The fundamental concepts of internal control can be applied no matter what data processing mechanism is used. When an organization decides to implement a new application or modify the existing one, control and security measures need to be analyzed. Many of these control measures will apply equally well to any operations platform: manual systems, computer processing systems, proprietary EDI or open Internet systems. These broadly applicable controls should be retained. However, because of the new risks of Internet-based EC, some internal control processes need to be modified and expanded. Also, certain new controls and security measures need to be added where unique new risks are created in the Internet environment. In this context, certain fundamental characteristics of the new EC environment should be considered when developing an Internet-based internal control system.

1. Real-time:

Control activities and monitoring need to fit into a real time control and risk assessment environment. Since the transaction cycle is shortened in an Internet-based EC environment, the transaction data become more time-sensitive as well. Only real-time control can reflect real-time business conditions and protect the firm's resources.

2. Integrated:

That internal control should be part of the design at the organizational level and transaction processing systems has been understood for a long time. However, in the Internet EC environment, this understanding must become reality. For example, control mechanisms must be directly integrated with the reengineered business processes and transactions systems design to achieve both control and efficiency in Internet EC. All control requirements including segregation of duties, authorization, approval and verification must be embedded in the integrated system.

3. Automatic:

The higher the level and the more automatic the control, the more positive the influence the controls will have on the efficiency and effectiveness of electronic transactions processing and control. For example, the validity of data should be established before processing. This can be accomplished by using automatic front-end controls. Further, it is best to use computerized control procedures and sensors to automatically monitor on going transaction and asset disposition rather than traditional expost or sampling procedures. Automatic warning systems, reporting systems and even correcting systems should be built in as digitized control mechanisms.

4. Dynamic:

Internet provides the dynamic information of business processes which presents an up-to-date business environment more accurately than less comprehensive traditional systems. Decision making in a dynamic business processes setting requires reliable and current information in order to reflect the real time situation. Being part of the monitoring mechanism, internal control, by itself, can be and should be dynamic as well. Internal control should take advantage of the availability of real-time control-related information. Control strategies and procedures should be dynamic not only to reflect up-to-date business requirements but also to fit in real-time processing situation. Feedback controls should provide automatic inputs to digital notice and correction systems. Only flexible and dynamic internal controls can appropriately complement and support the dynamic Internet-based EC business processes.

5. Reactive- and Proactive- Techniques Combined:

To complement real-time control requirements, mixed strategies can be used. The new technologies can be used

as proactive enforcement controls, such as using automatic email to provide notice of a deadline or expected action. This contrasts with a transaction effectively requesting (reactive) appropriate controls, such as requesting and waiting for verifications. Combining these strategies increases the efficiency of control over efficient transactions.

6. Preventive:

Due to the unpredictable and potentially severe consequences of system wide attacks, controls that rely on error detection and correction do not match the need of a real time system. To prevent errors rather than rescue after-the-fact, requires that Reliability-by-Design modeling be applied in designing and implementing internal control mechanisms.

7. Multi-Compensating:

It is important to maintain transaction integrity throughout transactions processing so that each transaction is completed and properly identified with its related entities. Any incomplete action in a transaction should trigger a compensating control response. Computerized control allows for the implementation of complex multiple-state compensation systems.

8. Automatically Generated Audit Trail

Because on-line real time access, registration and transaction processing on the Internet, it is crucial to create transaction logs and audit trails automatically. This feature, properly used, will enhance the auditability of the Internet-based system.

The above features of the Internet EC control environment can be exploited to strengthen firm-wide control. The new power of Internet-based internal control will support not only supervising real-time Internet-based business applications but also satisfying the requirements of sound security and assurance as to system performance and control.

Although a highly secure internal control system is important and desirable in Internet-based EC, they are expensive in terms of monetary costs, human resources and time. Cost-effectiveness and reasonable assurance rules should be applied to the implementation of internal control systems in the new EC business paradigm. The issue that can not be ignored in developing internal controls of Internet-based EC is control policy establishment. It is management's responsibility to develop good internal controls with (1) well-defined control policies; (2) strict follow-ups on defined policies; (3) design of complementary incentive schemes to encourage employee protection of the assets; and (4) efficient enforcement tools.

After this broader IEC business processes analysis and a consideration of the fundamental characteristics of Internet-based internal control system, we move to a more detailed discussion to support actual internal control detailed design.

6. Developing Internal Control Procedures

Similar to any other computing technology, Internet-based applications should not be implemented simply for the sake of doing Internet business. The strategic and tactical business requirements of the firm must be the driving force for installing an IEC application. Treating Internet-based applications development as a business initiative, the fundamental business objectives of quality, service level, and competitive advantages need to be addressed and analyzed.

In the life cycle development of an Internet-based application system, it is essential to consider the integrated control procedures while system analysis and design is conducted.
Understanding the business environment by analyzing stakeholders, analyzing and redesigning business processes, identifying areas of competitive advantage for Internet applications and their impacts will be the starting point of any design process. Only after a broad based business and system analysis should we consider more detailed general and application controls in the internal control development phase. In this fashion we can assure that the control processes solve the broader business objectives and mitigate the key business risks.

Detailed control procedures designed to meet stakeholder needs can be classified as general controls and application controls. In a computerized environment, the company designs general controls to ensure that its overall computerized environment is stable and well managed. This usually includes segregation of duties within the systems function, physical access controls, logical access controls, data storage controls, data transmission controls, documentation standards, decreased system downtime, disaster recovery planning, and protection of PCs and client/server networks. The primary objective of application controls is to ensure the accuracy of a specific application's input, files, programs, and outputs. Application controls are used to prevent, detect, and correct errors and irregularities in transactions as they are processed.

6.1Considerations of General Control

While all of the traditional general control procedures for computerized systems still apply, there are several new concerns to address in the Internet-based EC.

1. Access Controls Concerns:

Given that openness is a key feature of the Internet, unauthorized access becomes a more significant

security problem than in traditional systems. In addition to the traditional approaches to access control, such as passwords and physical possession identification, access control in Internet-based EC requires additional enhanced control procedures. Access controls should address such issues as outsiders accessing company data and employees surfing an insecure or an invalid site. Firewalls, bastion hosts and proxy servers are currently the most common ways to solve these problems.

Firewalls are built to selectively pass incoming and outgoing traffic between an organization's internal networks (Intranets) and the Internet. The objective is to protect trusted networks from those that cannot be trusted. All traffic between the two networks is forced to pass through the firewall, where it can be analyzed before it is released. A firewall is a concept rather than a specific model or product. Thus, the architecture of firewalls is quite varied. They may be composed of a single networking device, such as a router; or they may have many devices, including routers and computers, all performing the function of a firewall [7]. Firewalls can be effective in preventing some hacker activities such as TCP/IP Spoofing.

The proxy servers and bastion hosts are special forms of firewall. A bastion host sits between internal users and other networks. A bastion host is used to collect valid incoming traffic and forward it to appropriate locations on the internal network. In the reverse manner, it can act as a single collection point for internal traffic destined for the Internet. The proxy service providers are somewhat transparent to the users, who are unaware that an intermediary is acting on their behalf when they access Internet services. A proxy server can perform services on behalf of valid users and does not require that the user actually log in to the bastion host. [6] The use of an audit trail on a proxy server can detect employees who have accessed inappropriate Internet sites. In addition, a proxy server can restrict unsecured usage of FTP and Telnet services.

2. Segregation of Duties Concerns:

In a highly integrated Internet-based EC system, procedures used to be performed by separate individuals or programs are combined. This situation can provide individuals with opportunities to both perpetrate and conceal fraud. To combat this threat, organizations must implement compensating control procedures such as the effective segregation of duties within the transaction processing functions and procedures [7]. Authority and responsibility must be clearly divided among the functions. If it is necessary, internal control procedures will require organizations to use separate agents (functional programs), separate servers and even separate input/output devices to handle specific processes and implement certain control mechanisms. The use of digital signatures to verify an identity and preserve the integrity of messages can be applied to achieve segregation of duties in Internet-based EC. Applying asymmetric key (public and private key) and digital signatures associated with appropriate authorization rules can be used to fulfill the segregation of duties in approving and handling transaction related documents and business processes.

3. Data Storage Controls Concerns:

Information can give a company a competitive edge making it not only a viable organization but also an extremely successful one. Since information is such a valuable resource, it must be protected from unauthorized disclosure and destruction. In Internet-based EC, the need for protecting electronic information becomes even more important than in traditional systems since the openness features of Internet causes the data to be more vulnerable. For a company that sells digital products (such as software, CD, movies in the electronic form), implementing internal control procedures in order to protect their digital inventory is of vital importance. A company should identify the types of data maintained and the level of protection required for each type of data. Obviously, the more confidential, important, and valuable the information are, the greater the need for their protection. How to document and keep track of security efforts in storing, maintaining, accessing these data is an important concern.

4.Data Transmission Concerns:

To reduce the risk of data transmission failures, companies should monitor the network to detect weak points, maintain backup components, and design networks so that capacity is sufficient to handle peak-processing loads. Data transmission threats and risks are minimized through dial-back systems, parity checking, echo checking, caller-ID, virus scanning and data encryption [7].

The encryption of data is generally considered to be the best method of providing confidentiality for both data storage and transmission. Encryption is the transformation of data using an algorithm, from one form to another utilizing one or more encryption keys during the transformation process. Encryption should be implemented whenever data that must be kept secret is sent over a open public network. Encryption can be applied either to the whole message or to a slice of the transaction message. The data needs to be protected and the transaction needs to keep its integrity and to be protected with appropriate authentication.

4. Real Time Assurance Monitoring Concerns:

In their working paper [8], Wang et al. addressed the issues of collecting related and reliable transaction data to provide the assurance of the data integrity and preserves causality among processes. Since IEC transactions system is a distributed computing system that consists of several processes, we can found it is common to have these processes communicate with each other continuously and concurrently. Because of HTTP is a stateless protocol and cgi-bin programs can generate Web pages dynamically at run time, to monitor what have occurred in the real time with a better accountability transaction data and auditability audit trails is important. In order to solve the problems of repudiation and transaction event lost in IEC, Wang et al. suggested using a real-time assurance monitor server with vector clocks mechanism to monitor and record the events and processes are delivered completely in a right causal order.

6.2Business Processes and Security Requirements

1. Developing a Processes/Documents and Security Requirements Matrix

The objectives of internal control listed in Section II describe the required quality criteria of the system. In addition to the traditional criteria, Internet-based systems need to pay more attention on security criteria. When Internet-based applications are integrated with existing financial transactions processing systems, input/data transmission/output controls need to be enhanced. This is due, in part, to the packet-switching feature of Internet traffic and the open connectivity feature of the Internet infrastructure making the system vulnerable to the security breach such as eavesdropping. These security criteria should also be considered while business processes and documents are studied during the analysis and design stage,. Using information flow, data flow diagrams, and document flowcharts in the analysis and design/reengineering stages will help identify the processes and documents used in each application. Each process and document must meet certain security criteria to be included as part of an application. A matrix can be developed with processes/documentation listed vertically and security requirements listed horizontally as in the following example. We use the sales application in the revenue cycle which includes processes such as catalog/product information search, customer's purchase order submission, sales confirmation, sales status check, shipment notification and back order notification. Customer's purchase order is the document received first in the sales application. Then the customer's purchased order will be confirmed and used to create the sales order.

2. Developing a Processes/Documents and Security Protocols/Tools Matrix

A variety of security tools and protocols have been developed to improve Internet security. As often happens, one of the side effects of rapid interest and growth in the application of a new technical base is that a great number of conflicting standards are created. It remains to be seen which one will be the universally accepted standard in Internet-based EC. Although none of the existing tools is foolproof and some of them are pretty expensive, today it is commercially viable to implement some of these tools/protocols in Internet-based EC applications. Security is required at both the content and the transport level of the network messages and is best implemented at the application level.

Table 2. Processes/Documents and Security Requirements Matrix

Process/ Documents	Confidentiality	Integrity	Authentication	Authorization	Non-repudiation
Product Information Search			x		
Customer's Purchase Order (CPO)	x	x	x		
Submit CPO (no/ Payment)	x	x	x		x
Submit CPO (w/payment)	x	x	x		x
Sales confirmation	x	x	x	x	x
Sales status check	x	x	x	x	

Applying cryptographic schemes is considered appropriate for the more sophisticated Internet EC threats and risks. Using a cryptosystem, various criteria of electronic business transaction security can be achieved. In most applied cryptosystem designs, symmetric and asymmetric cryptosystems (also called the public-key cryptosystem) are combined to achieve better cost-efficiency. For authentication by the public-key cryptosystem, digital certificates are necessary for identifying, electronically and remotely, non-acquainted end users. A digital certificate binds an entity with its public key. The binding can be verified by the Certificate Authorities (CAs) and maintained through multiple channels. The uniqueness of the binding enhances the accountability of the entity. This type of assurance service needs to be provided by a trusted third party. Thus controls over Internet-based EC are closely related to the development of new assurance services.

Smart cards can be used for many different functions related to security. The most common use of a smart card is to provide multiple functions authentication. One function of authentication is based on something you have in your possession (i.e., the smart card) and another function positively identifies you (e.g., a thumbprint or eye scan). With a tiny processor and storage system

realized in a microcircuit embedded in a plastic card the same size as a familiar plastic credit card enhanced personal authentication can be provided [5]. Message encryption and identity authentication by certification are major applications based on cryptography. Internet Protocols, such as Secure Socket Layer (SSL), Secure HTTP (SHTTP), Pretty Good Privacy (PGP) and Secured Electronic Transaction (SET) have applied cryptography to authenticate communication entities. Secure Socket Layer (SSL) and Secure HTTP (SHTTP) protocols have been added into web browsers (Microsoft's PCT and Netscape's SSL) and servers to authenticate end-users identifications in Internet sessions. PGP encrypts message with digital signature while SET secured credit card transactions. Multipurpose Mail Extensions (MIME) is an Internet standard to define how message types, other than ASCII text, can be passed using an Internet mail message. The types of content definitions include text, multipart, message, application, image, audio and video. The basic MIMI specification does not include specific security protection. Security Multi-parts for MIME (S/MIME) defines the interface to the security services which may be applied to the parts of the MIME message. It defines two new types of the parts of a MIME message: multipart signed and multipart encrypted [6]. The Kerberos model was based on the concept that the network cannot be trusted. Kerberos uses a combination of secret key techniques to allow the mutual authentication of both client and server in a distributed computing environment.

There are other security mechanism may be selected other than the application layer of data communication such as secure IPv6. Secure IP (IPv6) is a specification for extensions to the IP protocol that includes additional security functions. The IPv6 includes two security mechanisms: an authentication header and the encapsulating security payload (ESP) protocol. The integrity of the message can be verified using the authentication header while the EXP protocol provides the ability to encrypt some or all of the message.

It is important to understand that these security protocols/tools are not mutually exclusive. As a matter of fact, a robust security system will have more than a single protection mechanism. Different schemes should be applied together to enhance the protection power. The complementary of different protections will enhance overall security. Each process and document has certain security criteria it must meet to be part of an application as described in the processes/documents and security requirements matrix. These criteria are based on the level of protection necessary to perform the business objectives within the acceptable level of risk. In an Internet environment, the most common ways to convey information and conduct transactions among entities are through the Web forms and/or E-mail systems as the front-end tools in the application level. After a matrix with the business processes/documents listed vertically and possible security implementations listed horizontally has been carefully developed and costs of them were evaluated, we can design the most optimal solution of security mechanism for each business process and document. We are using the same example as described in the previous section. There are different types of digital certificates can be applied in different security implement. Some processes and documents need higher level of accountability, such as online payment. Thus it requires both vendors and consumers' private digital certificates. Others may only require secure document transmission. In this situation, only general digital certificates for client/server secure protocol applications are needed. Usually, the security protocols/tools support both types of digital certificate through a trusted third Certificate Authorities.

Table 3. Processes/Documents and Security Protocols/Tools Matrix

Processes/Documents	Possible Security Implement				
	Web			E-Mail	
	HTTP	SSL	SET	MIME	S/MIME , PGP
Product Information search	x			x	
Customer's Purchase Order (CPO)		x			
Submit CPO (no/Payment)		x			
Submit CPO (w/payment)		x	x		
Sales confirmation		x			x
Sales status check		x			x

7. Conclusion

Developing Internet-based EC transaction systems is a new business movement driven by the organizational requirements and Internet technology. To be implemented successfully, the Internet must be viewed as part of an integrated solution of the whole organizational business processes. Management should conduct a careful broader business scope analysis of the organization and approach business processes reengineering in a strategic fashion. Because of the on-line, real time, open and dynamic features of the Internet-based transactions, the internal control systems should be integrated within the application systems and be designed and developed simultaneously.
At the same time, the system must be able to maintain appropriate continuous monitoring of business practices and internal controls to ensure their continued currency and effectiveness.

In this paper, we provide the general guidelines of designing internal controls for any organization interested in riding the Internet-based EC bandwagon while developing its Internet-based business applications. By following the approach of system development life cycle, the organization can design and implement their internal

control systems while the Internet-based EC applications are under development. This is just a beginning. More detailed general and application control features and control technologies will be explored and discussed in the future studies.

References

[1] Internal Control - Integrated Framework, published by the Committee of Sponsoring Organizations of the Treadway Commission Committee, 1992

[2] American Institute of Certified Public Accountants (AICPA), Committee on Auditing Procedure, Internal Control - elements of a Coordinated System and Its Importance to Management and the Independent Public Accountant, Statement on Auditing Standards No. 48 (AU320.27), AICPA, 1973

[3] Control Objectives for Information and Related Technology, Information Systems Audit and Control Foundation: Rolling Meadows, IL, 1996

[4] Soon-Yong Choi, Dale O. Stahl, and Andrew B. Whinston, *The Economics of electronic Commerce*, Macmillan Technical Publishing, Indianapolis, Indiana, 1997

[5] Thomas P. Colberg, Nicole W. Gardner, Kerry Horan, Dennis McGinnis, Phillip McLauchlin, Yuk-Ho So, *The Price Waterhouse EDI Handbook*, John Wiley & Sons, Inc., 1995

[6] Glen Bruce and Rob Dempsey, *Security in Distributed Computing*, Prentice Hall PTR, Prentice-Hall Inc., 1997

[7] Cushing, B. E., Steinbart, P.J. and Romney, M. B., *Accounting Information Systems*, 7th Edition, Addison-Wesley Publishing Company, 1997.

[8] Wang, W. Bailey, A. D. and Whinston, A. "A Conceptual Model for the Design of Autable Electronic Commerce Control Systems", Working Paper, November, 1999.