E-Commerce—Implications for Auditor

Tremendous growth of e-commerce in the last few years has not only changed our lives, but has also had a great impact on business and the audit environment. The audit profession faces a new challenge today, particularly when organisations are adopting e-commerce systems and increasing their sophistication through business process reengineering. This article delves into crucial issues such as what changes e-commerce brings on business processes, how e-commerce affects audit, why audit risk is intensified in e-commerce environment and what auditors need to do in response.

In this digital era, e-commerce systems have become essential to run the transactions, handle business contacts and manage information necessary to initiate and sustain the business activities. In many enterprises, they have become an integral part of the business and are fundamental to their growth, prosperity and, above all, survival.

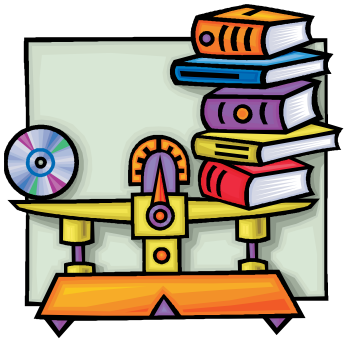
The widespread use and continuing development of e-commerce systems has enabled the organisations to improve the efficiency of their operations tremendously. On the other hand, it has also introduced enormous amount of risk that needs to be addressed by the management and assessed by the auditor while planning and conducting their audit.

E-commerce does not give rise to new audit objectives nor does it change the same. However, it essentially forces the auditors to review their audit processes and procedures in the light of changes brought by e-commerce in the ways of doing business and resultant risks. It requires auditors to upgrade their professional skills with the adequate knowledge of e-commerce systems to apprehend their impact on client's business and audit process in its right spirit.

From the audit point of view, e-commerce brings two vital changes in the organisation:

(a) New risks introduced by or changed level of risks coupled with the use of e-commerce systems, causing organisation to deploy appropriate additional controls and

(b) New form of records--electronic records, resulting in evaporation of paper trail of transactions



In the e-commerce environment, business events are identified, captured, measured, categorized, aggregated and recorded without any paper documentation. It is the duty of the management to assure their increasingly learned stakeholders and auditors that their electronic records, which lead to the generation of financial statements, are reliable. In this process they need to convince the auditors that the controls over the information systems being used for processing transactions and generating records are appropriate to the value of the records.

The auditors, in turn, are expected to evaluate various controls in the course of gathering sufficient, reliable and appropriate audit evidence before forming the audit opinion which calls for a heightened understanding of environment in which the business operates.

E-commerce environment itself is a very complex environment comprising technologies, processes and business strategies that allow the instant communication for fast and boundary-less business transactions.

E-commerce is based on client-server architecture. The elements of e-commerce architecture may be categorised as follows:

Client Software

Client software means the software running on the client machine, i.e. the user interface including local processing software, web-browsers (windows Internet explorer, etc.) and client plug-ins to enable the browser to read certain types and formats of file, such as documents, images and multimedia files.

Kavita Gorwani

(The author is a member of the Institute. She can be reached at gorwanik@rediffmail.com)

Business Applications and Allied Software

It means the software installed on the server enabling business transactions and processing of data. It includes web servers to manage the web pages and making them available to the client on request, application servers, e-commerce business application software, document management system, digitisation software, EDI, interactive voice recognition system (IVRS), load balancing software for web requests, RDBMS, application management tools, on-line transaction processing (OLTP) software, on-line analytical processing (OLAP) software and middleware.

Security Software

It intends to provide security to the information resources. It includes firewalls, proxy servers, encryption systems, gateway managers and access management software.

Depending upon the elements in e-commerce architecture, the nature of services offered by e-commerce vary tremendously from electronic fund transfer (EFT), electronic benefits transfer (EBT), electronic forms, digital cash, interoperable database access, bulletin boards, electronic catalogue, cable services, electronic banking, web-broadcasting, Internet telephony, Internet-electronic forms, Internet publishing, etc.

The auditors' assessment of risk will be severely affected by the complexity of e-commerce architecture as well as the nature and range of services offered and used by the client.

E-commerce: Risk Implications

As per Auditing and Assurance Standard -5 'Risk Assessments and Internal Controls';

"The auditor should obtain an understanding of accounting and internal control systems sufficient to plan the audit and develop an effective audit approach. The auditor should use professional judgement to assess audit risk and to design audit procedures to ensure that it is reduced to an acceptably low level."

It further states that "audit risk" means the risk that the auditor gives an inappropriate audit opinion when the financial statements are materially misstated.

The auditor should obtain an understanding of accounting and internal control systems sufficient to plan the audit and develop an effective audit approach.

In e-commerce environments, audit risk is intensified because of the following threats coupled with the use of highly sophisticated electronic systems:

a) Faded accountability:

Electronic records do not contain any physical marks for the identification of the person making or authorizing the transactions. As a result, individual users cannot be held responsible for such transactions and resultant records. The very nature of e-records raises the possibility of unauthorised transactions.

Moreover, it is very difficult for the auditor to identify and segregate unauthorised transactions and assess their overall impact on the profitability and financial position of the entity. Such unauthorised transactions may be an indication of a fraud already committed or to be committed in near future and are, therefore, to be considered carefully while planning and conducting the audit.

b) Vulnerability to amendment:

Electronic records are innately easy to amend and the amendment is, by default, invisible, as it does not leave any trace of amendment. It results in the auditors being unable to rely on authenticity of records.

c) Ease of duplication:

It is very easy to duplicate data and files and extremely difficult to differentiate the duplicate from the original. In case of financial transactions, it becomes very important to apply controls in the form of sequence numbers, unique IDs, etc. for the prevention and detection of duplication records, as duplicity may directly result in financial losses.

Basic e-commerce architecture

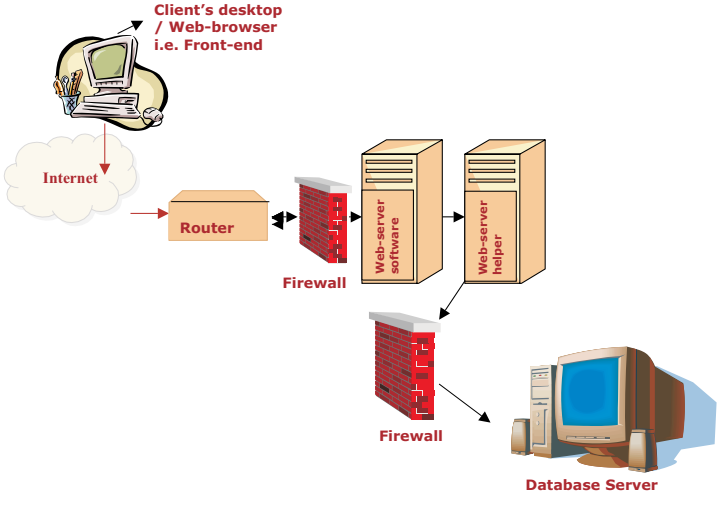


Figure: 1

d) Evaporated paper trail of transactions

E-commerce systems process transactions in an invisible form. Only input and output can be available for auditing. The invisible form of transaction processing makes it vulnerable to unauthorised amendments during processing itself, without leaving any trace of the amendments.

It becomes more risky when organisation uses electronic interface with the key suppliers, distributors, banks and other outside agencies and the transaction is processed at two or more ends, because it is very difficult to place assurance on the controls employed by the other partner especially when transaction takes place on untrusted networks.

e) Remote access

The essence of e-commerce lies in the availability of Internet. Internet, by its very nature, is vulnerable to attack as it is open for access to the world at large.

f) Placing reliance on outsourced processes

When any business process is outsourced by the client, it becomes very difficult for the auditor to ensure compliance of security and control standard. It becomes more risky in case of open networks, where it is impossible for one to assess the identity and extent of the involvement of third parties.

E-commerce: Security Controls and Audit Implications

An International report on the Financial Statement Audit acknowledges that many auditors now believe that the audit methodology that was appropriate for the industrial age may not be sufficiently broad for the information age, when assets are intangible, commerce is electronic, markets are global and the pace of change is ever-accelerating. It is because the responsibility of the auditor with regard to the detection of misstatement arising from fraud and error remains the same irrespective of the added risk of e-commerce and non-availability of paper evidence. In the e-commerce environment, it is the security concern that becomes worthy of special consideration and causes auditor to redefine the audit procedures to meet responsibilities. Security has three main dimensions:

Confidentiality, which is concerned with the protection of sensitive information from unauthorised disclosure,

Integrity, which relates to accuracy and completeness of information as well as to its validity in accordance with business values and expectations and

Availability, which relates to information being available at the moment when required. It also involves the safeguarding of necessary information resources and associated capabilities.

Integrity and continued availability of information resources to authorised users can be ensured and confidentiality of sensitive information can be preserved by implementing appropriate security features, which fall in mainly three categories:

I. Logical access controls

Logical access controls prescribe who or what can access a specified information resource and the type of access that is permitted. These controls may be built into operating system, application programs, RDBMS, Communication Systems or add-on security packages in the form of requiring user to key in some secret information to gain access like password, PIN etc., or asking him to use some device like smart card.

The auditor should review the access control mechanism to ensure its adequacy, efficiency, effectiveness and appropriateness to the value of records.

E-commerce obscures the boundaries of sites to be physically protected. The use of open networks for e-commerce makes strong logical access controls very important.

An effective and efficient logical access control system not only ensures the protection of data, software and information processing facilities from unauthorised disclosures, amendments and deletions but also injects accountability by enforcing identification of user, authentication of his identity, access rights, i.e. authorising user for certain actions (read/write/modify/delete, etc.) on eligible IS resources, and Accounting for the use of resources by the users and actions performed by them.

The auditor should review the access control mechanism to ensure its adequacy, efficiency, effectiveness and appropriateness to the value of records. He should ensure that

- all users are subjected to identification, authentication and authorisation;
- all transactions, financial or non-financial are tagged with the user ID of maker and checker, if applicable,
- all system generated transactions are easily identifiable,
- there are no anonymous USER IDs and right to deal with the user IDs and access privileges is limited to designated personnel only,
- access is allowed on 'need-to-know and need-to-do' basis, and
- a clear separation of duties among staff members is in place.

II. Data security controls

Specific data security controls like encryption, digital

signature, digital certificates, firewalls, etc. may be used to strengthen the level of security provided to critical data. An auditor should check the system for adequate level of security controls and integrity constraints to maintain the accuracy, completeness, and uniqueness of the transactions and ensure that the controls so applied are reliable and are operating effectively. Data security controls may be classified into following categories:

Encryption: Encryption entails transforming a clear-text message into a coded illegible message called cipher-text by using encryption key i.e. a secret mathematical function / algorithm. Clear-text message can be retrieved back by using encryption key again. It can be of two types:

- Private Key infrastructure: It is also known as symmetric encryption, as a single key is used for encryption as well as decryption.
- Public Key infrastructure: It entails asymmetric encryption where two keys called public key and private key are used to encrypt and decrypt the data respectively. Public key is open for public at large. Any body can encrypt the message with public key and send to the intended receipt holding private key to decrypt.

Public Key Infrastructure

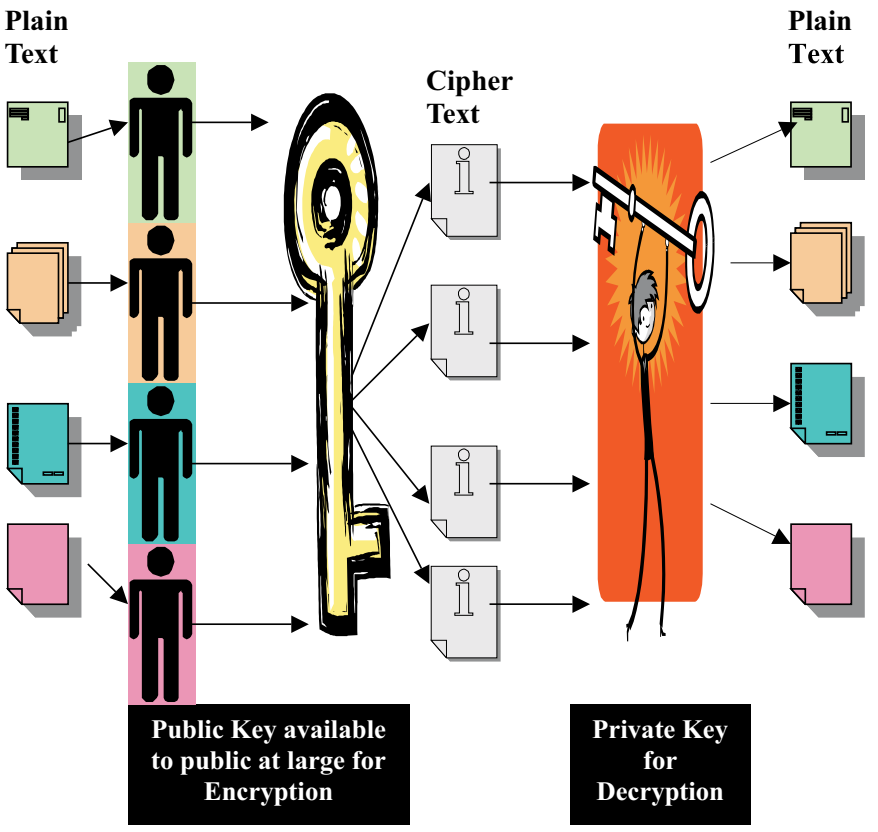


Figure: 3

Private Key Infrastructure

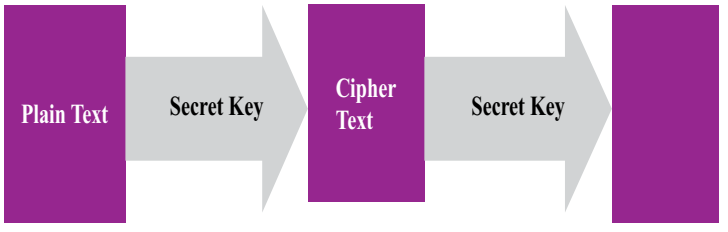


Figure: 2

Digital Signature: It is an electronic authentication technique that validates the identity of message sender, the integrity of transmitted message and enforces non-repudiation i.e. the sender cannot later deny sending message. Public key infrastructure is the administrative infrastructure for digital signatures and encryption key pairs. To protect against unauthorised duplication of messages, sequence no. and unique ID can also be used more particularly in case of messages involving monetary matters.

Digital certificate: It is like an electronic identification card that is used with a public key encryption system to authenticate the identity of the message sender.

Firewalls: The devices, software or hardware installed at a point where network connection enter a site to provide security by channeling all network connections through a control gateway and by applying rules to control the type of incoming and outgoing network traffic.

III Audit trail

To ensure integrity of the transactions, it is essential that the transactions are capable of being traced back to their input and forwarded to the output through processing cycle.

An audit trail is a set of

An auditor should check the system for adequate level of security controls and integrity constraints.

transaction that

- helps an organisation to trace transaction from input to output i.e. from the point of customer contact to sale and
- reflects all changes made to the transaction data, parameters, masters, access control tables, security tables and also the exceptional and undesirable events and transactions.

Ideally and essentially, an audit trail should contain identity of the maker and checker, if any, of the transactions, transaction time, nature of transaction and their outcome.

An audit trail helps an organisation to

- affect recovery when an unauthorised user incorrectly amends or deletes a record,
- monitor security breaches,
- recover from a system failure,
- recover from massive file destruction,
- probe into the causes of any anomaly, etc.

As in an e-commerce environment the transactions are processed in invisible form, an auditor should use audit trail effectively to follow the history of transactions. The review and analysis of audit trail becomes more critical in case of transactions processed in open networks.

An auditor should familiarise himself with the type and level of various controls employed by the client and check if these controls are appropriate to the value of information resources. He should thoroughly analyse the security policy with reference to the use of various security measures such as firewalls, encryption, user IDs, Passwords, smart cards, digital signatures and certificate to ensure their adequacy and appropriateness for securing critical data.

In addition, the auditor should apply procedures to ensure use of integrity checks, control totals and check digits as detective and corrective controls to protect the organisation against the unauthorised amendments to data. He should also ensure that a system of generating sequence numbers and randomly generated unique codes is in place to ensure uniqueness of the transactions and to provide a safeguard against duplicity, particularly in monetary transactions.

The e-commerce environment, resultant risks and their implications for auditors can be understood simply with the help of the case study enumerated below.

CASE STUDY

Consider the case of a domestic airlines company say e-Fly Ltd. The company uses e-commerce systems to enable its customers to book air tickets on-line.

e-Fly Ltd. offers three ways of booking e-tickets depending upon the type of its customers:

1. One time customers:
   Anybody can access the website and book e-tickets by simply giving the details of passengers and making paying through credit card. The e-tickets, so booked, can be printed and used for travel.
   In such a case, user can reschedule the flights by entering ticket form serial no. and PNR, a randomly generated 6 digits' unique alpha code printed on e-ticket.
2. Register Users:

a. Frequent Fliers

The customer can register themselves as frequent fliers. They are allotted a 10-digit unique number called e-Flyer privilege number (EFP no.).

The customer can use EFP no. with their password to log-in into the system and do the transactions i.e. enquire, book, view, reschedule and cancel the e-tickets. The customers are required to make instant payments through credit card while booking an e-ticket.

The customers gain the advantage of a reward program run by the company, which allows customer to have 1 point for every Rs.100 spent on booking e-tickets.

b. Privileged Fliers

The customers in this category are shifted from frequent flier category, when they accumulate 10000 reward points. The privileged fliers are allowed a credit of 15 days for booking e-tickets up to the specified limit of Rs.1,00000. They continue to be the part of reward program in the same manner.

Nature of transactions, both financial as well as non-financial, associated risks and respective controls to ensure integrity of the transactions

a) Booking ticket

One-time customers: No logical access controls are applicable as no identification of the customer is needed so far as passengers' details are valid, credit card details are verified and payment is secured.

Frequent flier: Though in the case of frequent fliers also, payment is secured at the time of booking tickets, they get the advantage of reward program. Therefore, the identification and authentication becomes essential. User should be asked to enter EFP no. and password.

Privileged Fliers: In addition to the risk with frequent flier transactions, the risk of booking tickets up to Rs.

The auditor should apply procedures to ensure use of integrity checks, control totals and check digits as detective and corrective controls to protect the organisation against the unauthorised amendments to data.

100000 on credit also exists which may cause immediate financial loss to the company.

Therefore, in addition to the control required in the form of entering EFP no. and password at the time of booking e-ticket on credit, the system may ask the user to supply some secret information with was asked for at the time of creating EFP account like mothers' maiden name, name of first school, etc. and to supply credit card no., which can be debited on expiry of 15 days.

b) Rescheduling flights, no financial adjustment

One-time customers: The controls in the form of entering PNR and ticket form serial no. should be in place and work effectively for rescheduling the flights.

Registered users: In addition to the above controls, logical access controls exist in the form of EFP no. and password, which protect personal details and transactions to be modified unauthorisedly.

c) Canceling e-ticket

One-time customers: The controls in the form of entering PNR and ticket form serial no. should be in place and work effectively for affecting cancellation also.

Moreover, auditor should ensure that no cash refunds are allowed and the amount is credited to the same credit card account.

Registered users: In addition to the above controls, logical access controls protect against unauthorised cancellations.

d) Requesting public information e.g. a flight schedule:

The information is not specific to a customer; hence there is no need of identification and authentication. In case, a non-registered user requests company to send schedule by post, though name & address is required, no verification is needed, information desired being open for public.

e) Creating EFP A/c:

The form for creating EPF a/c should incorporate essential field validations like completeness check, range check, limit check, reasonableness check, field interdependency check etc.

The risk of one person having multiple accounts also exists which should be mitigated by unique sequence no. or ID like EFP no.

f) Requesting personal information e.g. monthly activity statement

One time customers: Not applicable

Registered Users: Identification and authentication required. To ensure accountability, integrity and confidentiality of personal information, user should be asked to log in using his EFP no. and password. It is also essential to log the logging time, nature of request made, logout time, etc.

g) Updating personal information

One time customers: Not applicable

Registered Users: The risk of security breach exists by unauthorised user viewing, printing or incorrectly amending personal details, therefore, identification and authentication should be insisted upon. All changes made should also be incorporated into the audit trail.

h) Redeeming/ encashing award points:

One time customers: Not applicable.

Registered Users: The risk of unauthorised user encashing/redeeming reward points exists, which may result in loss of customer faith, reputation and even business.

Therefore, strong logical access controls enforcing customer to login using his EFP No. and password required before the user is allowed to deal with the reward points.

i) Correspondence - enquiry, feedback, complaints, etc.

All correspondence should be recorded and made part of audit trail. It should consist of the nature of correspondence, the reply given in case of enquiries and complaints, user ID of the staff member who handled the correspondence, date & time of all correspondences and identity of the user / person who initiated / did correspondence.

An auditor should thoroughly review all customer correspondences particularly complaints as they may provide auditor an insight into the efficiency or otherwise of the controls.

The auditor should also ensure that all critical transactions, financial or non-financial by or with registered users are intimated to them via e-mail, which can work as a detective measure.

The risk of one person having multiple accounts also exists, which should be mitigated by unique sequence no. or ID like EFP no.

Conclusion

The shift to the seamlessly connected organisations has already placed greater value on the auditors who are skilled at identifying and handling complex technological issues and adapting with the ever-changing business environment.

Therefore, instead of considering e-commerce a necessary evil, we must welcome and support this worthwhile reform made possible by information technology. We should realize that, with e-commerce being so pervasive within the economy, we, as auditors, cannot discharge our duties effectively and efficiently without thorough understanding of the e-commerce systems; resultant changes particularly new risks and their effect on the client's business and also on our audit. ❐