

PAPER – 6 : INFORMATION SYSTEMS CONTROL & AUDIT

Answer all questions. Each question carries 20 marks.

Question 1

Worldwide, a global telecom company is serving to more than 10 million customers in the area of communications through fixed land lines, mobiles, internet services, digital TV and satellite system etc.

The financial analysts of the company are located in different functional groups in six geographical regions. These analysts are missing the access to the same data, as well as timely access to the information. Dated budget and actual numbers for each business unit reside in seven different systems, separating critical components of the Profit and Loss account and inhibiting analyst's ability to assess results. The problem gets further complicated as the field analysts are not able to go to one universal place to retrieve the data themselves and they have to rely upon the home office for the same.

The objective of the company is to set some critical financial goals so that the company could remain competitive and increase market share.

Read the above carefully and answer the following with justifications:

- (a) To overcome the problems which the financial analysts are facing, what kind of software the company should select? (10 Marks)
- (b) The company is advised that the adoption of BS7799 International Standard will help in overcoming the problems and achieving its goals. Discuss. (5 Marks)
- (c) How should the human resources be enriched for effective utilization of the proposed new systems and standards? (5 Marks)

Answer

- (a) As the financial analysts of the company are working in six different geographical locations and the financial data is stored on seven different systems, located world wide, therefore they are facing several problems. Few of them are as under :

- Missing the access to the same data as well as timely access to information.
- Dated budget and actual numbers for each business unit reside in seven different systems, separating critical components of the profit and loss account thus failing the financial analysts to assess results.
- The field analysts are not able to retrieve the data themselves from one universal place and therefore they have to rely upon the home office for the same.

It is therefore important that the company should buy new software for the solution of the problems as mentioned above.

As far as software is concerned, of course the company should select the one which could make same data available to all the financial analysts. One such software is

FINAL EXAMINATION : NOVEMBER, 2009

available from Oracle Corporation known as On Line Analytical Processing (OLAP) tool for better control over costs, analyze performance, evaluate opportunities, and formulate future directions. To improve the basis for making decisions quickly and accurately with real time, to provide consistent data which will improve cost control and to simplify and shorten the budgeting process, the software should be capable of the following:

- hands on ability to consolidate budgets, based on actual data in the process,
- enabling business units to make real-time, online decisions based on more accurate information,
- user friendly.

The company is expected to be benefited by significant financial saving and therefore it should reduce the length of the budgeting cycle and the number of people involved in the process, thus keeping the company financially competitive in a growing market. The system should provide online, real time access to the information.

- (b) The BS 7799 (ISO 17799) consists of 127 best security practices which companies can adopt to build their Security Infrastructure. The model helps the companies to maintain IT security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement. The benefits of an Information Security Management Systems (ISMS) tuned to the objective of the company are improved customer confidence, a competitive edge, better personnel motivation and involvement, and reduced incident impact leading to increased profitability.

The company can use BS 7799 for the following reasons:

- Reduced operational risk,
- Increased business efficiency, and
- Assurance that information security is being rationally applied.

This is achieved by ensuring that:

- Security controls are justified.
- Policies and procedures are appropriate.
- Security awareness is good amongst staff and managers.
- All security relevant information processing and supporting activities are auditable and are being audited.
- Internal audit, incident reporting / management mechanisms are being treated appropriately.
- Management actively focuses on information security and its effectiveness.

PAPER – 6 : INFORMATION SYSTEMS CONTROL & AUDIT

(c) The human resources involved in the systems and standards can be enriched by the following activities:

- **Training Personnel:** A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps in the successful implementation of information system and standards. Thus, training is a major component of systems implementation. When a new system is acquired which often involves new hardware and software, both users and computer experts need training organized by the vendor through hands-on learning techniques.
- **Training Systems Operators:** The effective implementation of new systems and standards also depend on the computer-centre personnel, who are responsible for keeping the equipment running as well as for providing the necessary support services. Their training must ensure that they are able to handle all possible operations, both routine and extra-ordinary. As part of their training, operators should be given a trouble shooting list that identifies possible problems and remedies for them. Training also involves familiarization with run procedures, which involve working through the sequence of activities needed to use a new system on an on-going basis.
- **User training:** User training deals with the operation of the system itself. Training in data coding emphasizes the methods to be followed in capturing data from transactions or preparing data for decision support activities. Users should be trained on data handling activities such as editing data, formulating inquiries (finding specific records or getting responses to questions) and deleting records of data. From time to time, users will have to prepare disks, load paper into printers, or change ribbons on printers. Some training time should be devoted to such system maintenance activities. If a micro computer or data entry system uses disks, users should be instructed in formatting and testing disks.

It is also required to have managers directly involved in evaluating the effectiveness of training activities because training deficiencies can translate into reduced user productivity level.

Question 2

(a) Identify and justify the type of each one of the following systems based on how they perform within an environment and/or certainty/ uncertainty:

- (i) Marketing system
- (ii) Communication system
- (iii) Manufacturing system
- (iv) Pricing system
- (v) Hardware-Software system.

(5 Marks)

(b) Explain the threats due to Cyber crimes.

(5 Marks)

FINAL EXAMINATION : NOVEMBER, 2009

- (c) Discuss 'Physical and Environmental Security with Control and Objectives' with respect to information Security Policy? (5 Marks)
- (d) How does the Information Technology Act, 2000 enable the authentication of records using digital signatures? (5 Marks)

Answer

(a)

System	System Type	Justification
(i) Marketing system	Open System	The marketing system plays a pivotal role in the running of a business in the competitive environment. The objective of the system is to maximize customer satisfaction by providing a free interactive environment. The system takes input/feedbacks and facilitates the outcomes as products of the company and to create new customers.
(ii) Communication System	Open System	The communication system in an organization is a point of contact to balance the external influence and render its services to the customers. The system interacts freely with its environment by taking input and returning output.
(iii) Manufacturing System	Closed System	This system is in place to meet a particular objective. It neither interacts with the environment nor changes with the change in the environment. A manufacturing unit is completely isolated from its environment for its operation.
(iv) Pricing System	Probabilistic and Open System	The system has a probable behavior and interacts freely with its environment by taking inputs and returning outputs. The pricing system is a dynamic one which influences the form of profit and goodwill of an organization.
(v) Hardware-Software System	Closed Deterministic System	The interaction among the various parts of the system is known with certainty and it does not interact with the environment and does not change with the change in the environment. Here the requirements of the hardware and software inventory are known with certainty. The operational state of these systems is predictable.

PAPER – 6 : INFORMATION SYSTEMS CONTROL & AUDIT

(b) Threats due to cyber crimes are given as follows:

- **Embezzlement:** It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted, for his/her own use or purpose.
- **Fraud:** It occurs on account of intentional misappropriation of information or identifies to deceive others, the unlawful use of credential card or ATM, or the use of electronic means to transmit deceptive information, to obtain either money or other valuable things. Fraudulent may be an employee of the company or outsider.
- **Theft of proprietary information:** It is the illegal capturing of other's documentation or information. Usually it is done by electronic copying. The things illegally copied may be in the form of design, plans, blue prints, codes, computer programs, formulas, trade secrets, graphics, copyrighted material, data, forms, files and personal or financial information etc.
- **Denial of service:** This is the disruption or degradation of external services. This is usually caused by events like ping attacks, port scanning probes and excessive amount of incoming data.
- **Vandalism or sabotage:** It is the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
- **Computer virus:** They are hidden computer codes. They are destruction programs. They propagate by inserting themselves or modifying other programs.
- **Others:** Threat includes several other cases such as intrusions, breaches and compromises of the respondent's computer networks.

(c) **Physical and Environmental Security:** This is the beginning point of any security plan. It is designed to prevent unauthorized access, damage and interference to business premises and information. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control.

Maintenance of the physical operating environment in a computer server room is as important as ensuring that paper records are not subject to damage by mould, fire or fading. Supporting equipments such as air conditioning plant etc. should be properly maintained. Physical controls may be difficult to manage as they rely to some extent on building structure, but good physical security can be very effective.

The detailed control and objectives for this type of security are:

- **Secure areas:** To prevent unauthorized access, damage and interference to business premises and information,
- **Equipment Security:** To prevent loss, damage or compromise of assets and interruption to business activities, and

FINAL EXAMINATION : NOVEMBER, 2009

- General Controls: To prevent compromise or theft of information and information processing facilities.
- (d) Chapter-II, Section 3 of IT Act, 2000 provides conditions subject to which an electronic record is authenticated by means of affixing digital signature.
- The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as “hash function” which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record.

Any tampering with the contents of the electronic record will immediately invalidate the digital signature.
 - Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the corresponding public key.

This will enable anybody to verify whether the electronic record is retained intact or has been tampered with; since it was fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

Question 3

- (a) What analysis should be done for understanding the degree of potential loss (such as reputation damage, regulation effects) of an organization? Enumerate the tasks to be undertaken in this analysis. In what ways the information can be obtained for this analysis? (10 Marks)
- (b) Describe Risk Management Process. (5 Marks)
- (c) Explain the term “Cryptosystems”. Briefly discuss Data Encryption Standard. (5 Marks)

Answer

- (a) Business Impact Analysis (BIA) should be done for assessing the potential impacts resulting from various events or incidents. It is intended to help in understanding the degree of potential loss which could occur. It covers not only financial loss but also other losses due to reputation damage, regulatory effects, etc.

For BIA, the following tasks are to be undertaken:

1. Identify organizational risks, and to minimize potential threats that may lead to a disaster.
2. Identify critical business processes.
3. Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
4. Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.

PAPER – 6 : INFORMATION SYSTEMS CONTROL & AUDIT

5. Identify the maximum allowable downtime for each business processes.
6. Identify the type and the quantity of resources required for recovery.
7. Determine the impact to the organisation in the event of a disaster, e.g. financial reputation etc.

The information for this analysis can be obtained in many ways, including:

1. Questionnaires,
2. Workshops,
3. Interviews, and
4. Examination of documents.

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframe in which they must be recovered after interruption. The BIA Report should be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

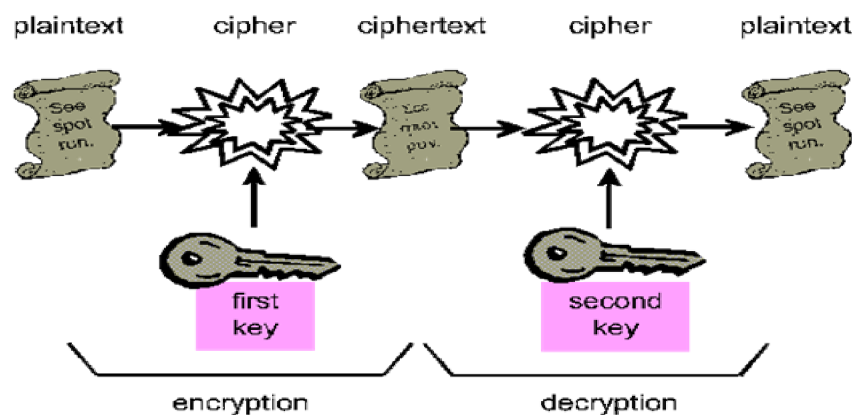
- (b) Risk Management Process: The broad Risk Management Process comprises of the following:
1. Identify the technology related risks under the gamut of operational risks.
 2. Assess the identified risks in terms of probability and exposure.
 3. Classify the risks as systematic and unsystematic.
 4. Identify various managerial actions that can reduce exposure to systematic risks and the cost of implementing the same.
 5. Look out for technological solutions available to mitigate unsystematic risks.
 6. Identify the contribution of the technology in reducing the overall risk exposure.
 7. Evaluate the technology risk premium on the available solutions and compare the same with the possible value of loss from the exposure.
 8. Match the analysis with the management policy on risk appetite and decide on induction of the same.
- (c) Cryptosystems: A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption. Typically, it consists of following three algorithms:
- Key Generation Algorithm,
 - Encryption Algorithm and
 - Decryption Algorithm.

The pair of algorithms of Encryption and Decryption is referred as Cipher or Cypher.

FINAL EXAMINATION : NOVEMBER, 2009

Data Encryption Standard (DES): It is a cipher. It is a mathematical algorithm for encrypting and decrypting binary coded information. Encrypting of data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. Encryption and Decryption operations are done by using a binary number called a key. A key consists of 64(bits) binary digits. Among these 64 bits, 56 bits are used for encryption/decryption and remaining 8 bits are used for error detection. Authorized users of the encrypted data must have the unique key that was used to encipher the data in order to decrypt it. Selection of a different key causes the cipher that is produced for any given set of inputs to be different. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

The encryption and decryption processes are depicted in the following diagram:



Some documentation distinguishes DES from its algorithms. It refers algorithms as DEA (Data Encryption Algorithm).

Question 4

- You have been asked to conduct an I.S. Audit for a bank. (i) How will you develop a documented audit program? (ii) What kind of working papers and documentation you will prepare? (10 Marks)
- Explain the basic types of Information Protection that an Organization can use. (5 Marks)
- Discuss the three processes of Access Control Mechanism, when an user requests for resources. (5 Marks)

Answer

- The documented audit program is developed with the help of following activities:
 - Documentation of the IS auditor's procedures for collecting, analysing, interpreting, and documenting information during the audit.

PAPER – 6 : INFORMATION SYSTEMS CONTROL & AUDIT

- Objectives of the audit.
- Scope, nature, and degree of testing required to achieve the audit objectives in each phase of the audit.
- Identification of technical aspects, risks, processes, and transactions which should be examined.
- Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.

(ii) Audit Working Papers and Documentation

Working papers should record the audit plan, the nature, timing and extent of auditing procedures performed, and the conclusions drawn from the evidence obtained. All significant matters which require the exercise of judgment, together with the auditor's conclusion thereon, should be included in the working papers. The form and content of the working papers are affected by matters such as:

- The nature of the engagement
- The form of the auditor's report
- The nature and complexity of client's business
- The nature and condition of client's records and degree of reliance on internal controls.

In case of recurring audits, some working paper files may be classified as permanent audit files which are updated currently with information of continuing importance to succeeding audits, as distinct from the current audit files which contain information relating primarily to audit of a single period.

The permanent audit file normally includes:

- The organization structure of the entity.
- The IS policies of the organization.
- The historical background of the information system in the organization.
- Extracts of copies of important legal documents relevant to audit.
- A record of the study and evaluation of the internal controls related to the information system.
- Copies of audit reports and observations of earlier years.
- Copies of management letters issued by the auditor, if any.

The current file normally includes:

- Correspondence relating to the acceptance of appointment and the scope of the work.
- Evidence of the planning process of the audit and audit programme.
- A record of the nature, timing, and extent of auditing procedures performed, and the results of such procedures.

FINAL EXAMINATION : NOVEMBER, 2009

- Copies of letters and notes concerning audit matters communicated to or discussed with the client, including material weaknesses in relevant internal controls.
- Letters of representation and confirmation received from the client.
- Conclusions reached by the auditor concerning significant aspects of the audit, including the manner in which the exceptions and unusual matters, if any, disclosed by the auditor's procedures were resolved and treated.
- Copies on the data and system being reported on and the related audit reports.

Working papers are the property of the auditor. The auditor may, at his discretion, make portions of, or extracts from his working papers available to the client. The auditor should adopt reasonable procedures for custody and confidentiality of his working papers and should retain them for a period of time sufficient to meet the needs of his practice and satisfy any pertinent legal and professional requirements of record retention.

(b) Types of Information Protection: The two basic types of information protection that an organization can use are given as follows:

1. Preventative Information Protection, and
2. Restorative Information Protection.

Preventative Information Protection: It is based on use of security controls, which itself is a group of three types of controls such as Physical, Logical, and Administrative.

Physical controls deal with Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems,

Logical controls deal with Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems, and

Administrative controls deal with Security Awareness, User Account Revocation, and Policy.

Restorative Information Protection: If an organization cannot recover or recreate critical information systems in an acceptable time period, the organization will suffer and possibly have to go out of business. Hence, the key requirement of any restorative information system protection plan is that the information systems can be recovered. The claim of back program to backup data automatically cannot be reliable. It has so many problems. The restorative information protection program must address the following:

- Whether the recovery process has been evaluated and tested recently?
- The time taken for restoration,
- The quantum of productivity loss,
- The strict adherence of plan, and
- The time needed to input the data changes since the last backup.

PAPER – 6 : INFORMATION SYSTEMS CONTROL & AUDIT

- (c) Access control mechanism processes the user request for resources in three steps. They are:

- Identification
- Authentication
- Authorization

The access control mechanisms operate in the following sequence:

1. The users have to identify themselves, thereby indicating their intent to request the usage of system resources,
2. The users must authenticate themselves and the mechanism must authenticate itself, and
3. The users request for specific resources, their need for those resources and their areas of usage of these resources.

The mechanism accesses

- (a) previously stored information about users,
- (b) the resources they can access, and
- (c) the action privileges they have with respect to these resources.

The mechanism verifies this information against the user entries and it then permits or denies the request.

Identification and Authentication: Users identify themselves to the access control mechanism by providing information such as a name, account number, badge, plastic card, finger print, voice print or a signature. To validate the user, his entry is matched with the entry in the authentication file. The authentication process then proceeds on the basis of information contained in the entry, the user having to indicate prior knowledge of the information.

Authorization: There are two approaches to implementing the authorization module in an access control mechanism:

- **Ticket oriented:** In this approach the access control mechanism assigns the users a ticket for each resource they are permitted to access. Ticket oriented approach operates via a row in the matrix. Each row along with the user resources holds the action privileges specific to that user
- **List oriented:** In this approach, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource.

Question 5

- (a) How does the Information Technology Act, 2000 enable the objective of the Government in spreading e-governance? (5 Marks)

FINAL EXAMINATION : NOVEMBER, 2009

- (b) Briefly discuss Black Box Testing. (5 Marks)
- (c) Discuss anti-virus software and its types. (5 Marks)
- (d) ABC Limited has recently migrated to real-time Integrated ERP System. As an IS Auditor, advice the company as to what kinds of businesses risks it can face? (5 Marks)

Answer

- (a) In Information Technology Act 2000, chapter III is related with the objective of the government in spreading e-governance. It deals with the procedures to be followed for sending and receiving of electronic records. This chapter contains sections 4 to 10.

Section 4 - This section provides the legal recognition of electronic records.

Section 5 - This section provides the legal recognition of Digital Signatures.

Section 6 – It lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.

Section 7 – This section provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained in the electronic form with the following conditions:

- (i) the information therein remains accessible so as to be usable subsequently,
- (ii) it is retained in its original format ,
- (iii) the details such as origin, destination, dates and time of dispatch or receipt of such electronic record.

Section 8- It provides for the publication of rules, regulations and notifications in the Electronic Gazette.

- (b) Black box testing: Black box testing attempts to derive sets of inputs that will fully exercise all the functional requirements of a system. It is not an alternative to white box testing. This type of testing attempts to find errors in the following categories:

- incorrect or missing functions,
- interface errors,
- errors in data structures or external database access,
- performance errors, and
- initialization and termination errors.

Tests are designed to answer the following questions:

- How is the function's validity tested?
- What classes of input will make good test cases?
- Is the system particularly sensitive to certain input values?

PAPER – 6 : INFORMATION SYSTEMS CONTROL & AUDIT

- How are the boundaries of a data class isolated?
- What data rates and data volume can the system tolerate?
- What effect will specific combinations of data have on system operation?

Some of the methods used for test cases are as follows:

- **Equivalence Partitioning:** This method divides the input domain of a program into classes of data from which test cases can be derived. Equivalence partitioning strives to define a test case that uncovers classes of errors and thereby reduces the number of test cases needed. It is based on an evaluation of equivalence classes for an input condition. An equivalence class represents a set of valid or invalid states for input conditions.
 - **Boundary Value Analysis (BVA):** This method leads to a selection of test cases that exercise boundary values. It complements equivalence partitioning since it selects test cases at the edges of a class. Rather than focusing on input conditions solely, BVA derives test cases from the output domain also.
 - **Cause-Effect Graphing Techniques:** This technique provides a concise representation of logical conditions and corresponding actions. Causes (input conditions) and effects (actions) are listed for a module and represented in a cause-effect graph. This graph is converted to a decision table rules which are used to derive test cases.
- (c) **Anti-virus Software:** It is a program that is used to detect viruses, and prevent their further propagation and harm.
- Three types of anti-virus software are briefly discussed below:
- Scanners:** Scanners for a sequence of bits called virus signatures that are characteristic of virus codes. They check memory, disk boot sectors, executables and systems files to find matching bit patterns. As new viruses emerge frequently, it is necessary to frequently update the scanners with the data on virus code patterns for the scanners to be reasonably effective.
- Active Monitor and Heuristic Scanner:** This looks for critical interrupt calls and critical operating systems functions such as OS calls and BIOS calls, which resemble virus action.
- Integrity Checkers:** These can detect any unauthorized changes to files on the system. These can detect any unauthorized changes to the files on the system. The software performs a “take stock” of all files resident on the system and computes a binary check data called the Cyclic Redundancy Check (CRC). When a program is called for execution, the software computes the CRC again and checks with the parameter stored on the disk.
- (d) The company, ABC Limited may face several new business risks when they migrate to real-time, integrated ERP systems. These risks include the following:
1. **Single point of failure** – All input data of an organization and transaction processing is within one application system.

FINAL EXAMINATION : NOVEMBER, 2009

2. Structural Changes - Significant personnel and organizational structural changes associate with reengineering or redesigning business processes.
3. Job Role Changes - Traditional roles of users are changed to empowered-based role. They have more chances to access enterprise information in real-time. This point of control shifts from the back-end financial processes to the front-end point of creation.
4. Online Real-Time – This environment requires a continuous business interaction. This warrants the capabilities of utilizing the ERP application and responds quickly to any problem that requires a re-entry of information (e.g., if field personnel are unable to transmit orders from handheld terminals, customer service staff may need the skills to enter orders into the ERP system correctly so the production and distribution operations will not be adversely impacted).
5. Change Management - It is challenging to bring together a highly integrated environment when different business processes have existed among business units for long. The level of user acceptance of the system has a significant influence on its success. Training and awareness of users is mandatory, to understand that their actions or inaction have a direct impact upon other users and in the performance of their day-to-day duties.
6. Distributed Computing Experience - Inexperience with implementing and managing this kind of environment may pose significant challenges.
7. Broad System Accessibility – Increased remote access by users and outsiders and high integration among application functions allow increased access to the application and data.
8. Dependency on External Assistance – Organization accustomed to in-house legacy systems may find that they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to a greater risk.
9. Program Interfaces and Data Conversions - Extensive interfaces and data conversions from legacy systems and other commercial software are necessary. The exposures of data integrity, security and capacity requirements for ERP are much higher.
10. Audit Expertise – Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialization such that each specialist may know only a relatively small fraction of the entire ERP's functionality in a particular core module, e.g. FI auditors, who are required to audit the entire organization's business processes, have to maintain a good grasp of all the core modules to function effectively.
11. Single sign on - It reduces the security administration efforts associated with administering web-based access to multiple systems, but simultaneously introduces additional risks in that an incorrect assignment of access may result in inappropriate access to multiple systems.
12. Data content quality - As enterprise applications are opened to external suppliers and customers, the need for integrity in enterprise data becomes paramount.
13. Privacy and confidentiality - Regularity and governance issues surrounding the increased capture and visibility of personal information, i.e. spending habits.