MOCK TEST PAPER – I

FINAL (OLD) COURSE: GROUP – II

PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT

ANSWERS

MULTIPLE CHOICE QUESTIONS

1. **(c)** Reciprocal Agreement

2. **(c)** (iii), (iv), (ii), (i)

3. **(c)** Makes decisions in solving complex problems on behalf of the managers.

4. **(d)** Transfer/Share the Risk

5. **(a)** Environmental

6. **(d)** How will the solution work?

7. **(a)** Legitimate

8. **(c)** The statutes or regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by subject organization.

9. **(b)** (i), (ii) and (iii)

10. **(b)** Expert System

11. **(b)** Piggybacking

12. **(d)** Review Report

13. **(d)** The cost of expansion, if developed

14. **(b)** Audit Hooks

15. **(b)** Section 43A

16. **(b)** Public Cloud

17. **(c)** Tolerate the risk

18. **(c)** Tax calculator is a physical system.

19. **(b)** Environmental Control

20. **(a)** Hot Site

21. **(c)** Pilot change-over

22. **(c)** Fieldwork

DESCRIPTIVE QUESTIONS

1. **(a)** The four categories of IT Strategy planning in an enterprise are as follows:

(i) **Enterprise Strategic Plan:** Business Planning determines the overall plan of the enterprise. The enterprise strategic plan provides the overall charter under which all units in the enterprise, including the information systems function must operate. It is the primary plan prepared by top management of the enterprise that guides the long run development of the enterprise. It includes a statement of mission, a specification of strategic objectives, an assessment of environmental and organization factors that affect the attainment of these objectives, a statement of strategies for achieving the objectives, a specification of constraints that apply, and a listing of priorities. In an IT environment, it is important to ensure that the IT plan is aligned with the enterprise plan.

(ii) **Information Systems Strategic Plan:** The IS strategic plan in an enterprise has to focus on striking an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment. This would require the enterprise to have a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals. Some of the enablers of the IS Strategic plan are-Enterprise business strategy, Definition of how IT supports the business objectives, Inventory of technological solutions and current infrastructure, Monitoring the technology markets, Timely feasibility studies and reality checks, Existing systems assessments, Enterprise position on risk, time-to-market, quality, and Need for senior management buy-in, support and critical review.

(iii) **Information Systems Requirements Plan:** Every enterprise needs to have clearly defined information architecture with the objective of optimizing the organization of the information systems. This requires creation and continuous maintenance of a business information model and also ensuring that appropriate systems are defined to optimize the use of this information. Based on the information architecture requirements of an enterprise, the Information Systems Requirements Plan has to be drawn up so as to meet the information requirements of the enterprise. Some of the key enablers of the information architecture are - Automated data repository and dictionary, Data syntax rules, Data ownership and criticality/security classification, an information model representing the business, and Enterprise information architectural standards.

The information system requirements plan defines information system architecture for the information systems department. The architecture specifies the major organization functions needed to support planning, control and operations activities and the data classes associated with each function. The business planning will determine the information needs of an enterprise. The information architecture will determine information needs and flow in an enterprise. Based on the information architecture, the organization structure is determined. This in turn will lead to specific information systems, which include the relevant IT and related processes. For example, depending on the business, information architecture and organization structure, the enterprise will decide whether to acquire or develop the solution and the relevant controls which are required to meet the business requirements.

(iv) **Information Systems Applications and Facilities Plan:** On the basis of the information systems architecture and its associated priorities, the information systems management can develop an information systems applications and facilities plan. This plan includes Specific application systems to be developed and an associated time schedule, Hardware and Software acquisition/development schedule, Facilities required, and Organization changes required.

Senior management is responsible for developing and implementing long and short-range plans that enable achievement of the enterprise mission and goals. Senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the enterprise's long- and short-range plans. IT long and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the enterprise. Strategic plan period could vary from 1 year to 3 years. It is important to ensure that the IT strategic plans are aligned with the business strategic plans as IT is ultimately used for achieving business objectives. Strategic planning could be done by the top management or by the steering committee. Strategic planning facilitates in putting organization objectives into time-bound plans and action. Comprehensive planning helps to ensure an effective and efficient enterprise. Strategic planning is time and project oriented, but must also address and help determine priorities to meet business needs.

(b) The various Operating System Access controls that may help in protecting the operating system installed in systems are as follows:

- **Automated terminal identification**

  This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.

- **Terminal log-in procedures**

  A log-in procedure is the first line of defense against unauthorized access. The log-in procedure does not provide unnecessary help or information, which could be misused by an intruder. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorized. If password or user-id is entered incorrectly, then after a specified number of wrong attempts, the system should lock the user from the system.

- **Access Token**

  If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.

- **Access Control List**

  This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.

- **Discretionary Access Control**

  The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, in distributed systems, resources may be controlled by the end-user. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger.

- **User identification and authentication**

  The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.

- **Password management system**

  An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.

- **Use of system utilities**

  System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.

- **Duress alarm to safeguard users**

  If users are forced to execute some instruction under threat, the system should provide a

means to alert the authorities.

- **Terminal time out**

  Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.

- **Limitation of connection time**

  Define the available time slot. Do not allow any transaction beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m. - or on a Saturday or Sunday.

(c) **Control Risk** is the risk that could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level and will not be prevented or detected by the client's internal control system. This assessment includes an assessment of whether a client's internal controls are effective for preventing or detecting gaps and the auditor's intention to make that assessment at a level below the maximum (100 percent) as a part of the audit plan.

2. **(a)** Audit Trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines 'which events will be recorded in the log'. An effective audit policy will capture all significant events without cluttering the log with trivial activity.

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning. The accounting audit trail shows the source and nature of data and processes that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

The Audit Trail in Data Resource Management Controls are as follows:

- Auditors should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls.
- Auditors might employ test data to evaluate whether access controls and update controls are working.

The Audit Trail in Quality Assurance Management Controls are as follows:

- Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.
- Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.
- Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.

(b) Various aspects related to Business Continuity Planning (BCP) testing are as follows:

- A BCP has to be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become outdated as time passes and as the resources used to support critical functions change. Responsibility for keeping the plan updated has to be clearly defined in the BCP.

- A Business Continuity Management (BCM) testing should be consistent with the scope of the BCP(s), giving due regard to any relevant legislation and regulation. Testing may be based on a predetermined outcome, e.g. plan and scope in advance; or allow the enterprise to develop innovative solutions.
- An exercise program should lead to objective assurance that the BCP will work as anticipated when required. The BCP testing program should include testing of the technical, logistical, administrative, procedural and other operational systems, BCM arrangements and infrastructure (including roles, responsibilities, and any incident management locations and work areas, etc.) and technology and telecommunications recovery, including the availability and relocation of staff.
- The frequency of testing should depend upon both the enterprise's needs, the environment in which it operates, and stakeholder requirements. However, the testing program should be flexible, taking into account the rate of change within the enterprise, and the outcome of previous one. The above exercise methods can be employed for individual plan components, and single and multiple plans.
- Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include-Defining the test purpose/approach, Identifying test teams, Structuring the test, Conducting the test; Analyzing test results; and Modifying the plans as appropriate.
- The approach taken to test the plans depends largely on the recovery strategies selected to meet the recovery requirements of the organization. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

(c) The Control being implemented by company is **Detective Control.** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. The main characteristics of these controls are as follows:

- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc;
- An established mechanism to refer the reported unlawful activities to the appropriate person or group;
- Interaction with the preventive control to prevent such acts from occurring; and
- Surprise checks by supervisor.

3. (a) The categories of information required in an enterprise based on its requirement by management are as follows:

(i) Top Management: Top level management strives for the information that can help them in major policy decisions such as establishment of new plant, launching of new product etc. In other words, we can say that the top management requires strategic information that helps them in making strategy of an enterprise in terms of scope of products, targets of products i.e. customers, competition with market i.e. price, quality, long term planning etc. The information about the customers buying habits such as what combination of products and type of products they are likely to purchase together helps top managers to decide the launching of new products. e.g. if the information like a customer whose income is more than one lakh per month and working in IT sector and are in habit of buying latest model of laptops are more in a city where large number of IT companies are existing then it's better to launch notebook with latest operating system there. Such information can help top management of company to decide to work on new products as well as the location where it

has to be launched for maximum profit and sale which is one of the objectives and goals of the top management.

(ii) **Middle Management**: The middle managements require tactical information that helps in implementing decisions taken by the top management. For example - information of customers likely to purchase certain product in a particular location can help sales managers to fulfill their sales target efficiently. Tactical information is used for short term planning whereas strategy information is used for long term planning. For example, the offers of companies during festive seasons are a short term planning, which is done by having information about the customers buying capacity in that location.

(iii) **Lower Management:** The lower management requires operational information, which is required in day-to-day activities. The operational information mainly comprises of information about stock on hand, information about customer order pending, information about bill payable by customer etc. These are essential for smooth running of the daily activities of a business at primary level. For example, if a regular customer demands for a product other than the daily purchase then this information is important for salesman because it will help him in providing better service.

(b) The **advantages** of continuous audit techniques are as follows:

- **Timely, Comprehensive and Detailed Auditing** – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability** – As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives** - Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users** – Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

The **limitations** of the continuous audit techniques are as follows:

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

(c) (i) "**Computer Network**" means the interconnection of one or more Computers or Computer systems or Communication device through-

(a) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(b) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

(ii) "**Intermediary**" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes;

4. (a) The major security issues related to cloud computing are as follows:

- **Confidentiality:** Prevention of the unauthorized disclosure of the data is referred as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential the unauthorized entities. With the use of encryption and physical isolation, data can be kept secret. The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of TC3 (Total Claim Capture & Control).
- **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secure. It should be insured that the data is not changed after being moved to the cloud. It is important to verify if one's data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Methods like digital signature, Redundant Array of Independent Disks (RAID) strategies etc. are some ways to preserve integrity in Cloud computing. The most direct way to enforce the integrity control is to employ cryptographic hash function. For example, a solution is developed as underlying data structure using hash tree for authenticated network storage.
- **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). In addition, Availability also ensures that they meet the organization's continuity and contingency planning requirements. Availability can be affected temporarily or permanently, and a loss can be partial or complete from Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure, and natural calamities are all threats to availability. One of the major Cloud service provider, AWS had a breakdown for several hours, which lead to data loss and access issues with multiple Web 2.0 services.
- **Governance:** Due to the lack of control over the employees and services, it creates problems relating to design, implementation, testing and deployment. So, there is a need of governance model, which controls the standards, procedures and policies of the organization. The organization gains computational resources as capital expenditures. These actions should be looked by the organization under governance through legal regulation, policies, privacy and security. Auditing and risk management programs are some way to verify the policy, which can shift the risk landscape.
- **Trust:** Deployment model provided a trust to the Cloud environment. An organization has direct control over security aspects as well as the federal agencies even have responsibility to protect the information system from the risk. Trust is an important issue in Cloud. Various clients' oriented studies reveal that Cloud has still failed to build trust between the client and service provider. Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time.

- **Legal Issues and Compliance:** There are various requirements relating to legal, privacy and data security laws that need to be studied in Cloud system. One of the major troubles with laws is that they vary from place to place, and users have no assurance of where the data is located physically. There is a need to understand various types of laws and regulations that impose security and privacy duties on the organization and potentially impact Cloud computing initiatives such as demanding privacy, data location and security controls, records management, and E-discovery requirements. An approach to monitor and compliance that helps to prepare Cloud Service Provider (CSP) and users to address emerging requirements and the evolution of Cloud models. To achieve efficiency, risk management, and compliance; CSPs need to implement an internal control monitoring function coupled with external audit process. To increase the comfort of Cloud activities, Cloud user define control requirements, internal control monitoring processes, examine applicable external audit reports, and accomplish their responsibilities as CSP users. It is the responsibility of the cloud suppliers that they are protecting the data and supplying to the customer in a very secure and legal way.
- **Privacy:** Privacy is also considered as one of the important issues in Cloud. The privacy issues are embedded in each phase of the Cloud design. It should include both the legal compliance and trusting maturity. The Cloud should be designed in such a way that it decreases the privacy risk.
- **Audit:** Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'. Its security is stronger than the one built in software and application. But, still it consumes more time, insistent across customers, pricy and motivational debilitate for everyone. The context of use of Cloud, time consuming audits seriously detains a key gain of Cloud agility.
- **Data Stealing:** In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. In such cases, an issue arises as data stealing. Some of the Cloud providers do not use their own server, instead. They use server/s from other service providers. In that case, there is a probability that the data is less secure and is more prone to the loss from external server. If the external server is shut down due to any legal problem, financial crisis, natural disaster, and fire creates loss for the user. In that case, data protection is an important mechanism to secure the data. Back up policies such as Continuous Data Protection (CDP) should be implemented in order to avoid issues with data recovery in case of a sudden attack.
- **Architecture:** In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The architecture of the Cloud is based on a specific service model. Its reliable and scalable infrastructure is dependent on the design and implementation to support the overall framework.
- **Identity Management and Access control:** The key critical success factor for Cloud providers is to have a robust federated identity management architecture and strategy internal in the organization. Using Cloud-based "Identity as a Service" providers may be a useful tool for outsourcing some identity management capabilities and facilitating federated identity management with Cloud providers. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public Cloud and extending or changing the existing framework to support Cloud services may prove difficult. Identity Management and Access control provides a secure authentication and authorization to an organization. The identity management provides a trust and shares the digital attributes between the Cloud provider and organization ensuring the protection against attackers.

- **Incident Response:** It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. Affected networks measures, determined systems, and applications, exposed intrusion vector helps to understand an incident response and the activities carried out must be re-modeled.
- **Software Isolation:** Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi-tenant software architecture, and evaluate the risks required for the organization.
- **Application Security:** Security issues relating to application security still apply when applications move to a cloud platform. To prevent Cloud computing; service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. Infected applications need to be monitored and recovered by the Cloud security drivers.

(b) The threats and their corresponding control mechanisms associated with each category of Data Integrity Controls are given below:

Control Category	Threats/Risks	Controls
Source data control	Invalid, incomplete, or inaccurate source data input	Forms design; sequentially pre-numbered forms, turnaround documents; cancellation and storage of documents, review for appropriate authorization; segregation of duties, visual scanning; check-digit verification; and key verification.
Input validation routines	Invalid or inaccurate data in computer-processed transaction files	As transaction files are processed, edit programs check key data fields using these edit checks, sequence, field, sign, validity, limit, range, reasonableness, redundant data, and capacity checks. Enter exceptions in an error log; investigate, correct, and resubmit them on time; re-edit them, and prepare a summary error report.
On-line data entry controls	Invalid or inaccurate transaction input entered through on-line terminals	Field, limit, range, reasonableness, sign, validity, and redundant data checks; user-ids and passwords; compatibility tests; automatic system date entry; prompting operators during data entry, pre-formatting, completeness test; closed-loop verification; a transaction log maintained by the system; clear error messages, and data retention sufficient to satisfy legal requirements.
Data processing and storage controls	Inaccurate or incomplete data in computer-processed master files	Policies and procedures (governing the activities of data processing and storage personnel; data security and confidentiality, audit trails, and confidentiality agreements); monitoring and expediting data entry by data control personnel; reconciliation of system updates with control accounts or reports; reconciliation of database totals with externally maintained totals; exception reporting, data currency checks, default values, data marching; data security

		(data library and librarian, backup copies of data files stored at a secure off-site location, protection against conditions that could harm stored data); use of file labels and write protection mechanisms, database protection mechanisms (data wise administrators, data dictionaries, and concurrent update controls); and data conversion controls.
Output controls	Inaccurate or incomplete computer output	Procedures to ensure that system outputs conform to the organization's integrity objectives, policies, and standards, visual review of computer output, reconciliation of batch totals; proper distribution of output; confidential outputs being delivered are protected from unauthorized access, modification, and misrouting; sensitive or confidential out-put stored in a secure area; review of user of computer output for completeness and accuracy, shredding of confidential output no longer needed; error and exception reports.
Data transmission controls	Unauthorized access to data being transmitted or to the system itself; system failures; errors in data transmission	Monitor network to detect week points, backup components, design network to handle peak processing, multiple communication paths between network components, preventive maintenance, data encryption, routing verification (header labels, mutual authentication schemes, callback systems), parity checking; and message acknowledgement procedures (echo checks, trailer labels, numbered batches).

(c) **Recovery Plan:** The backup plan is intended to restore operations quickly so that information system function can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Members of a recovery committee must understand their responsibilities. Again, the problem is that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur. If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

5. (a) The **Section 69A** of IT Act,2000 is related to the situation, wherein sovereignty and integrity of India may be compromised, which is given as follows:

[Section 69A] Power to issue directions for blocking for public access of any information through any computer resource

(1) Where the Central Government or any of its officers specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states

or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

(b) The issues which affect evidence collection and understanding the reliability of controls in financial audit are as follows:

- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transactions on the computer system. For example, the client's computer system may save data on detachable storage device by summarising transactions into monthly, weekly or period end balances.
- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of Electronic Data Interchange (EDI) will result in less paperwork being available for audit examination.
- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- **Lack of availability of printed output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output, it may be necessary for an auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.
- **Audit evidence:** Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalised) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.
- **Legal issues:** The use of computers to carry out trading activities is also increasing. More organisations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and are the parties to the contract.

(c) The various system change-over strategies that may be executed in ABC Ltd. are as follows:

- **Direct Implementation / Abrupt Change-Over:** This is achieved through an abrupt takeover – an all or no approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go. Direct Implementation, which usually takes place on a set date, often after a break in production or a holiday period so that time can be used to get the hardware and software for the new system installed without causing too much disruption.
- **Phased Changeover:** With this strategy, implementation can be staged with conversion to the new system taking place gradually. For example, some new files may be converted and used by employees whilst other files continue to be used on the old system i.e. the new is brought in stages (phases). If a phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one.
- **Pilot Changeover:** With this strategy, the new system replaces the old one in one operation but only on a small scale. Any errors can be rectified or further beneficial changes can be introduced and replicated throughout the whole system in good time with the least disruption. For example - it might be tried out in one branch of the company or in one location. If successful then the pilot is extended until it eventually replaces the old system completely.
- **Parallel Changeover:** This is considered the most secure method with both systems running in parallel over an introductory period. The old system remains fully operational while the new systems come online. With this strategy, the old and the new system are both used alongside each other, both being able to operate independently. If all goes well, the old system is stopped and new system carries on as the only system.

6. (a) **Identification of Problem:** The first step in an application development is to define the problem clearly and precisely, which is done only after the critical study of the existing system and several rounds of discussions with the user group. Then its prevalence within the organization has to be assessed. A problem that has a considerable impact on the organization is likely to receive immediate management attention. User involvement will also be high, if they are convinced that the proposed solution will resolve the problem.

For instance, personnel in a functional area may feel that an existing system is outdated or a manager might want access to specific new information that s/he claims will lead to better decisions. Shifting business requirements, changing organizational environments, and evolving information technology may render systems ineffective or inefficient. Whatever may be the reason, managers and users may feel compelled to submit a request for a new system to the IS department. If the need seems genuine, a system analyst is assigned to perform preliminary investigation who submits all proposals to the steering committee for evaluation to identify those projects that are most beneficial to the organization.

Thus, it can be concluded that the purpose of the preliminary investigation is to evaluate the project request feasibility. It is neither a designed study nor it includes the collection of details to completely describe the business system. Rather it relates to collection of information that permits committee members to evaluate the merits of the project request and make an informed judgment about the feasibility of the proposed project.

The analyst working on the preliminary investigation should accomplish the following objectives:

- Clarify and understand the project request;

- Determine the size of the project;
- Determine the technical and operational feasibility of alternative approaches;
- Assess costs and benefits of alternative approaches; and
- Report findings to the management with recommendation outlining the acceptance or rejection of the proposal.

(b) (i) Asset: Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees. Irrespective the nature of the assets themselves, they all have one or more of the following characteristics:

- They are recognized to be of value to the organization.
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form a part of the organization's corporate identity, without which, the organization may be threatened.
- Their Data Classification would normally be Proprietary, Highly confidential or even Top Secret.

It is the purpose of Information Security Personnel to identify the threats against the risks and the associated potential damage to, and the safeguarding of Information Assets.

(ii) Threat: Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat. A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization.

Threat has capability to attack on a system with intent to harm. It is often to start threat modeling with a list of known threats and vulnerabilities found in similar systems. Every system has a data, which is considered as a fuel to drive a system, data is nothing but assets. Assets and threats are closely correlated. A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets.

(iii) Vulnerability: Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records. Some examples of vulnerabilities are given as follows:

- Leaving the front door unlocked makes the house vulnerable to unwanted visitors.
- Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.

Missing safeguards often determine the level of vulnerability. Determining vulnerabilities involves a security evaluation of the system including inspection of safeguards, testing, and penetration analysis.

Vulnerability can be referred as the weakness of the software, which can be exploited by the attackers. Vulnerabilities can originate from flaws on the software's design, defects in its implementation, or problems in its operation. Some experts also define 'vulnerability' as opening doors for attackers. Normally, vulnerability is a state in a computing system (or set

of systems), which must have at least one condition, out of the following:

- 'Allows an attacker to execute commands as another user' or
- 'Allows an attacker to access data that is contrary to the specified access restrictions for that data' or
- 'Allows an attacker to pose as another entity' or
- 'Allows an attacker to conduct a denial of service'.

(c) The **Section 72A** of Information Technology Act, 2000 describes the punishment for Disclosure of information in breach of lawful contract, which is given as follows:

[Section 72A] Punishment for Disclosure of information in breach of lawful contract

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the Information Technology Regulatory Issues 7.23

intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.