PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

*Question No. **1** is compulsory.*

*Candidates are required to answer any **four** questions*

*from the remaining **five** questions.*

Question 1

ABC Ltd. is planning to set-up an automated steel production plant. Steel plant is very labor intensive and coal is the major ingredient in steel manufacturing. After conducting thorough investigations and extensive cost-benefit analysis, the top-management of ABC Ltd. decided to set-up the plant at a location nearer to coal mines; where labor and coal is available at very cheap rates. It was also decided to perform the key business operations using IT. To accomplish, the performance of key business operations, the management decided to develop a new system using SDLC approach of system development. The vision of the company is to be profitable and also to demonstrate good corporate citizenship through environmental awareness, ethical behaviour and sound governance practices. Establishment of a sound internal control practice plays an important role in good corporate governance. A consultant was hired to do risk assessment and to identify and analyze the relevant risks related to the chosen location. After careful analysis of the location, the consultant submitted his report to the management pointing therein:

- *That the selected location is prone to earthquake exposure and suggested that to survive and to provide uninterrupted services, the management should plan in advance to deal with sudden disruptions on the happening of earthquake to ensure business continuity, and continuity of supply and logistics. The management was also advised to make an adequate provision for backup facilities in another geographical location.*
- *In addition to developing a test plan to ensure the effectiveness of disaster recovery/business resumption plan, it is also necessary to develop an audit procedure. The audit process ensures that the plan is adequate as well as current.*
- *Establish controls in system development activities to ensure that the system is developed according to established policies and procedures, well within the budget and budgeted time.*

Read the above carefully and answer the following questions:

(a) *System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process. Explain the six activities that deal with System Development Controls in IT setup.* ***(6 Marks)***

(b) *In a computerized environment, the goals of asset safeguarding, data integrity, system efficiency, and system effectiveness can be achieved only if an organization's management sets up a system of internal controls. Explain the five interrelated components of Internal Controls as specified by Committee of Sponsoring Organizations (COSO).* ***(5 Marks)***

(c) The objective of BCP audit is to assess the ability of the enterprise to continue all critical operations during a contingency and recover from a disaster within the defined critical recover time period. Explain any three aspects related to Administrative Procedures of the enterprise that should be reviewed by the BCP auditor. ***(3 Marks)***

Answer

(a) The activities that deal with System Development Controls in IT setup are as follows:

- **System Authorization Activities:** All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, system's authorization should be formal. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.
- **User Specification Activities:** Users must be actively involved in the systems development process. User involvement should not be ignored because of a high degree of technical complexity in the system. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals. However, it is most important that this document remains a statement of user needs. It should describe the user's view of the problem, not that of the systems professionals.
- **Technical Design Activities:** The technical design activities in the Systems Development Life Cycle (SDLC) translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design. The adequacy of these activities is measured by the quality of the documentation that emerges from each phase. Documentation is both a control and evidence of control and is critical to the system's long-term success.
- **Internal Auditor's Participation:** The internal auditor plays an important role in the control of systems development activities, particularly in organizations whose users lack technical expertise. The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. Auditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.
- **Program Testing:** All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors. Program testing is time-consuming, the principal task being the creation of meaningful test data. To facilitate the efficient implementation of audit objectives, test data prepared during the implementation phase must be preserved for future use. This will give the auditor a frame of reference for designing and evaluating future audit tests.

- **User Test and Acceptance Procedures:** Just before implementation, the individual modules of the system must be tested as a unified whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s). The formal test and acceptance of the system should consider being the most important control over the SDLC. It is imperative that user acceptance be documented. Before implementation, this is the last point at which the user can determine the system's adequacy and acceptability.

(b) The interrelated components of Internal Controls as specified by Committee of Sponsoring Organizations (COSO) are as follows:

- **Control Environment:** This includes the elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on. For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.
- **Risk Assessment:** This includes the elements that identify and analyze the risks faced by an organisation and the way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation. Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.
- **Control Activities:** This includes the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks are carried on performance and valuation of records. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives. Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.
- **Information and Communication:** These are the elements in which information is identified, captured, and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities. These are associated with control activities regarding information and communication systems of the entity that acts as one of the components of internal accounting system. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.

- **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions. This includes the elements that ensure internal controls operate reliably over time. The best internal controls are worthless if the company does not monitor them and make changes when they are not working.

(c) The aspects related to Administrative Procedures of the enterprise that should be reviewed by Business Continuity Planning auditor are as follows:

- Does the disaster recovery/ business resumption plan cover administrative and management aspects in addition to operations? Is there a management plan to maintain operations if the building is severely damaged or if access to the building is denied or limited for an extended period of time?
- Is there a designated emergency operations center where incident management teams can coordinate response and recovery?
- Determine if the disaster recovery/ business resumption plan covers procedures for disaster declaration, general shutdown, and migration of operations to the backup facility.
- Have essential records been identified? Do we have a duplicate set of essential records stored in a secure location?
- To facilitate retrieval, are essential records separated from those that will not be needed immediately?

Question 2

(a) The Reserve Bank of India is India's central banking institution, which formulates the monetary policy with regard to the Indian rupee. Primarily, RBI suggests that senior management and regulators need an assurance on the effectiveness of internal controls implemented. Explain any six requirements of Reserve Bank of India (RBI) for System Controls of Financial Institutions. ***(6 Marks)***

(b) Alternate processing arrangements are essential to business continuity and disaster recovery planning. Explain briefly the backup options available before security administrators in this regard. ***(5 Marks)***

(c) COBIT has a specific focus on compliance activities within the frame work and explains how they fit within the complete enterprise picture. Explain any three sample metrics for reviewing the process of evaluating and assessing compliance. ***(3 Marks)***

Answer

(a) The requirements of Reserve Bank of India (RBI) for System Controls of Financial Institutions are as follows:

- Duties of system programmer/designer should not be assigned to persons operating the system and there should be separate persons dedicated to system

programming/design. System person would only make modifications/improvements to programs and operating persons would only use such programs without having right to make any modifications.

- Contingency plans/procedures in case of failure of system should be introduced/ tested at periodic intervals. EDP auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.
- An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements.
- In order to bring about uniformity of software used by various branches/offices, there should be a formal method of incorporating change in standard software and it should be approved by senior management. Inspection and Audit Department should verify such changes from the viewpoint of control and for its implementation in other branches in order to maintain uniformity.
- Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively.
- There should also be annual review of IS Audit Policy or Charter to ensure its continued relevance and effectiveness.
- With a view to provide assurance to bank's management and regulators, banks are required to conduct a quality assurance at least once every three years, on the banks Internal Audit including IS Audit to validate the approach and practices adopted by them in the discharge of its responsibilities as laid out in the Audit Charter/Audit Policy.

(b) Security administrators should consider the following backup options as alternate processing facility arrangements to business continuity and disaster recovery planning:

- **Cold Site:** If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system - raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.
- **Hot Site:** If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data, and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.
- **Warm Site:** A warm site provides an intermediate level of backup. It has all cold-site facilities in addition to the hardware that might be difficult to obtain or install. For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

- **Reciprocal Agreement:** Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

(c) Sample metrics for reviewing the process of evaluating and assessing compliance are as follows:

- **Compliance with External Laws and Regulations:** These metrics are as follows:
  - Cost of IT non-compliance, including settlements and fines;
  - Number of IT related non-compliance issues reported to the board or causing public comment or embarrassment;
  - Number of non-compliance issues relating to contractual agreements with IT service providers; and
  - Coverage of compliance assessments.
- **IT Compliance with Internal Policies:** These metrics are as follows:
  - Number of incidents related to non-compliance to policy;
  - Percentage of stakeholders who understand policies;
  - Percentage of policies supported by effective standards and working practices; and
  - Frequency of policies' review and updates.

Question 3

(a) The main objective of Disaster Recovery Planning is to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster. Explain the areas that should be covered in Disaster Recovery Planning Document. ***(6 Marks)***

(b) Achieving the objectives of System Development is essential but many times, such objectives are not achieved as desired. Explain any five User Related and Developer Related issues due to which organizations fail to achieve their System Development objectives. ***(5 Marks)***

(c) Explain the provisions related to Protected Systems under Section 70 of IT Act, 2000.

(3 Marks)

Answer

(a) The Disaster Recovery Planning document may include the following areas:

- The conditions for activating the plans which describe the process to be followed before each plan are activated.
- Emergency procedures which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include

arrangements for public relations management and for effective liaisoning with appropriate public authorities e.g., police, fire, services and local government.

- Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations and to bring business process back into operation in the required time scale.
- Resumption procedures, which describe the actions to be taken to return to normal business operations.
- A maintenance schedule, which specifies 'how and when the plan will be tested', and the process for maintaining the plan.
- Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- Contingency plan document distribution list.
- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedure.
- List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- Checklist for inventory taking and updating the contingency plan on a regular basis.
- List of phone numbers of employees in the event of an emergency.
- Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- Medical procedure to be followed in case of injury.
- Back-up location contractual agreement, correspondences.
- Insurance papers and claim forms.
- Primary computer center hardware, software, peripheral equipment, and software configuration.
- Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- Alternate manual procedures to be followed such as preparation of invoices.
- Names of employees trained for emergency situation, first aid, and life saving techniques.
- Details of airlines, hotels, and transport arrangements.

(b) (i) Some of the **User related issues** due to which organizations fail to achieve their system development objectives are mentioned below:

- **Shifting User Needs:** User requirements for IT are constantly changing. As these changes accelerate, there will be more requests for Information systems development and more development projects. When these changes occur during a development process, the development team faces the challenge of developing systems whose very purpose might change since the development process began.
- **Resistance to Change:** People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the workplace. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure.
- **Lack of User Participation:** Users must participate in the development efforts to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps to reduce user resistance to change.
- **Inadequate Testing and User Training:** New systems must be tested before installation to determine that they operate correctly. Users must be trained adequately to effectively utilize the new system.

Some of the **Developer related issues** due to which organizations fail to achieve their system development objectives are mentioned below:

- **Lack of Standard Project Management and System Development Methodologies:** Some organizations do not formalize their project management and system development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
- **Overworked or Under-Trained Development Staff:** In many cases, system developers often lack sufficient educational background and requisite state of the art skills. Furthermore, many companies do a little to help their development personnel stay technically sound, and more so a training plan and training budget do not exist.

(c) The provisions related to Protected Systems under Section 70 of the Information Technology Act, 2000 is as follows:

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation -

For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

Question 4

(a) If Cloud Computing is used properly and to the extent necessary, working with data in the cloud can vastly benefit all types of businesses. Explain the major advantages of Cloud Computing. ***(6 Marks)***

(b) Financial Controls are generally defined as the procedures exercised by the system user personnel over source, or transaction origination, documents before system input. Explain any five Financial Control techniques. ***(5 Marks)***

(c) Explain any three advantages of System Development Life Cycle (SDLC) approach of System Development from the perspective of IS Audit. ***(3 Marks)***

Answer

(a) Major advantages of Cloud Computing are as follows:

- **Cost Efficiency:** Cloud computing is the most cost-efficient method to use, maintain and upgrade. Traditional desktop software costs companies a lot in terms of finance. Adding up the licensing fees for multiple users can prove to be very expensive for the establishment concerned. The cloud, on the other hand, is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.
- **Almost Unlimited Storage:** Storing information in the cloud gives users almost unlimited storage capacity. Hence, there is no need to worry about running out of storage space or increasing the current storage space availability.
- **Backup and Recovery:** Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Furthermore, most cloud service providers are usually competent enough to

handle recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.

- **Automatic Software Integration:** In the cloud, software integration is usually something that occurs automatically. This means that users do not need to take additional efforts to customize and integrate the applications as per their preferences. Cloud computing allows users to customize the options with great ease. Hence, users can handpick just those services and software applications that s/he thinks will best suit his/her particular enterprise.
- **Easy Access to Information:** Once registered in the cloud, users can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues.
- **Quick Deployment:** Cloud computing gives us the advantage of quick deployment. Once users opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes, though the amount of time taken will depend on the exact kind of technology that one needs for his/her business.

(b) Though the Financial Control techniques are numerous, some of them are highlighted below:

- **Authorization:** This entails obtaining the authority to perform some act like typically accessing to assets such as accounting or application entries.
- **Budgets:** These estimate the amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control. Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.
- **Cancellation of documents:** This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a "paid" or "processed" stamp or punching a hole in the document.
- **Dual control:** This entails having two people simultaneously accessing an asset. For example, the depositories of banks' 24-hour teller machines should be accessed and emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. For example - With teller-machines, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.
- **Input/Output verification:** This entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary events like dollar totals and item counts.

- **Safekeeping:** This entails physically securing assets, such as computer disks under lock and key, in a desk drawer, file cabinet storeroom, or vault.
- **Sequentially numbered documents:** These are working documents with pre-printed sequential numbers, which enables the detection of missing documents.

(c) The advantages of Systems Development Life Cycle (SDLC) approach from the perspective of the Information Systems (IS) Audit are as follows:

- The IS auditor can have clear understanding of various phases of the SDLC based on the basis of the detailed documentation created during each phase of the SDLC.
- The IS Auditor on the basis of his/her examination, can state in his/her report about the compliance by the IS management of the procedures, if any, set by the management.
- The IS Auditor, if has a technical knowledge and ability of different areas of SDLC, can be a guide during the various phases of SDLC.
- The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

Question 5

(a) Audit of Environmental Control should form a critical part of every IS Audit Plan. The Audit of Environmental Controls requires the IS Auditor to conduct physical inspection and observe practices. What should the Auditor verify for audit of Environmental Controls?

(6 Marks)

(b) Office Automation System (OAS) is the most rapidly expanding computer based information systems. Explain any five office activities that can be broadly grouped in Office Automation Systems. ***(5 Marks)***

(c) COBIT 5 has seven enablers. Explain any three of them. ***(3 Marks)***

Answer

(a) The Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. The Auditor should verify that:

- The IPF (Infrastructure Planning and Facilities) and the construction with regard to the type of materials used for construction;
- The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs;
- The location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers;
- Emergency procedures, evacuation plans and marking of fire exists. There should be half-yearly fire drill to test the preparedness;

- Documents for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors/auditors;
- Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment, and generators. Also, the power supply interruptions must be checked to test the effectiveness of the back-up power;
- For installation of environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc.
- Compliant logs and maintenance logs to assess if MTBF (Mean Time Between Failures) and MTTR (Mean Time to Repair) are within acceptable levels; and
- the identification of undesired activities such as smoking, consumption of eatables etc.

(b) Different office activities that can be broadly grouped in Office Automation Systems (OAS) are as follows:

- **Document Capture:** Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.
- **Document Creation:** This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.
- **Receipts and Distribution:** This basically includes distribution of correspondence to designated recipients.
- **Filling, Search, Retrieval and Follow up:** This is related to filling, indexing, searching of documents, which takes up significant time.
- **Calculations:** These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.
- **Recording Utilization of Resources:** This includes, where necessary, record keeping in respect to specific resources utilized by office personnel.

(c) The COBIT 5 framework describes seven categories of enablers are as follows:

- **Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- **Organizational structures** are the key decision-making entities in an enterprise.
- **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.

- **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **People, Skills and Competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

Question 6

(a) Audit Trail of Input Controls maintains the chronology of events from the time data and instructions are captured and entered into the application system until the time they are deemed valid and passed onto other subsystems within the application system. Explain the contents of Accounting Audit Trail for Input Controls. ***(6 Marks)***

(b) Corporate Governance is defined as the system by which a company or enterprise is directed and controlled; Explain any five best practices of Corporate Governance.

(5 Marks)

(c) Transaction Processing Systems (TPS) record and manipulate transaction data into useful information. Explain any three components of TPS. ***(3 Marks)***

OR

Explain three characteristics of Risk.

Answer

(a) The Accounting Audit Trail for Input Controls maintains a record of events within the subsystem. These are as follows:

- The identity of the person(organization) who was the source of the data;
- The identity of the person (organization) who entered the data into the system;
- The time and date when the data was captured;
- The identifier of the physical device used to enter the data into the system;
- The account or record to be updated by the transaction;
- The standing data to be updated by the transaction;
- The details of the transaction; and
- The number of the physical or logical batch to which the transaction belongs.

(b) Some of the best practices of Corporate Governance include the following:

- Clear assignment of responsibilities and decision-making authorities, incorporating a hierarchy of required approvals from individuals to the Board of Directors.
- Establishment of a mechanism for the interaction and cooperation among the Board of Directors, senior management, and the auditors.
- Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances.
- Special monitoring of risk exposures where conflicts of interest are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm (e.g. traders).
- Financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion, and other recognition.
- Appropriate information flows internally and to the public. For ensuring good corporate governance, the importance of overseeing the various aspects of the corporate functioning needs to be properly understood, appreciated, and implemented.

(c) The principal components of a Transaction Processing System (TPS) are as follows:

- **Inputs:** Source documents such as customer orders, sales, slips, invoices, purchase orders, and employee time-cards are the physical evidence of inputs into the Transaction Processing System. They serve several purposes like capturing data, facilitating operations by communicating data and authorizing another operation in the process, standardizing operations by indicating which data require recording and what actions need to be taken and providing a permanent file for future analysis, if the documents are retained etc.
- **Processing:** This involves the use of journals and registers to provide a permanent and chronological record of inputs. Journals are used to record financial accounting transactions, and registers are used to record other types of data not directly related to accounting. Some of the common journals are sales journal, purchase journal, cash receipts journal etc.
- **Storage:** Ledgers and files provide storage of data on both manual and computerized systems. The general ledger, the accounts/vouchers payable ledgers, and the accounts receivable ledger are the records of final account that provide summaries of a firm's financial accounting transactions.
- **Outputs:** Any document generated in the system is output. Some documents are both output and input. For example - a customer invoice is an output from the order-entry

application system and, also an input document to the customer. The trial balance lists the balances of all the accounts on the general ledger and tests the accuracy of the record keeping. Financial reports summarize the results of transaction processing and express these results in accordance with the principles of financial reporting.

OR

Risk has following characteristics:

- Loss potential that exists as the result of threat/vulnerability process;
- Uncertainty of loss expressed in terms of probability of such loss; and
- The probability/likelihood that a threat agent mounting a specific attack against a particular system.