3. Protection of Information Systems

3.1 Need for Protection of Information Systems

- Information systems and communications that deliver the information are truly pervasive throughout organizations from the user's platform to local and wide area networks to servers.
- Executive management has a responsibility to ensure that the organization provides all users with a secure information processing environment.
- Information security failures may result in both financial losses and/or intangible losses such as unauthorized disclosure of competitive or sensitive information.
- Threats to information systems may arise from intentional or unintentional acts and may come from internal or external sources. The threats may emanate from technical conditions, natural disasters, environmental conditions, human factors, unauthorized access, or viruses.
- These risks have led to a gap between the need to protect systems and the degree of protection applied. This gap is caused by:
  - ✦ Widespread use of technology;
  - ✦ Interconnectivity of systems;
  - ✦ Elimination of distance, time, and space as constraints;
  - ✦ Unevenness of technological changes;
  - ✦ Devolution of management and control;
  - ✦ Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations; and
  - ✦ External factors such as legislative, legal & regulatory obligation or technological development

3.2 Information System Security

- Information security refers to the protection of valuable assets against loss, disclosure, or damage.
- Securing valuable assets from threats, sabotage, or natural disaster with physical safeguards such as locks, perimeter fences, and insurance is commonly implemented by most of the organizations.
- This concept of information security applies to all information. The protection is achieved through a layered series of technological and non-technological safeguards.
- **Information Security Objective –**
  - ✦ The objective of information system security is “the protection of the interests of those relying on information, and protect the information systems and communications that deliver the information from harm resulting from failures of confidentiality, integrity, and availability”.
- For any organization, **the security objective comprises three universally accepted attributes**:
  - **i). Confidentiality:** Prevention of the unauthorized disclosure of information;
  - **ii). Integrity:** Prevention of the unauthorized modification of information; and
  - **iii). Availability:** Prevention of the unauthorized withholding of information.

3.2.1 What Information is Sensitive?

- The following examples highlight some of the factors, necessary for an organization to succeed. The common aspect in each case is the critical information that each organization generates.

i). Strategic Plans –

- ✦ Most of the organizations readily acknowledge that strategic plans are crucial to the success of a company. But many of them fail to really make an effort to protect these plans.
- ✦ For example: a competitor learns that a company is testing a new product line in a specific geographic location. The competitor removes its product from that location, creating an illusionary demand for the product. When the positive results of the test marketing are provided to the company's executives, they decide to roll the product out nationwide. Only then company discover that in all other geographic regions the competition for their product was intense. The result is that company lost several million as its product sales faltered.
- ✦ In today's global environment, the search for competitive advantage has never been greater. The advantages of achieving insight into a competitor's intentions can be substantial.

ii). Business Operations –

- ✦ Business operations consist of an organization's process and procedures, most of which are deemed to be proprietary. As such, they may provide a market advantage to organization.
- ✦ This is the case when one company can provide a service profitably at a lower price than the competitor. While many organizations prohibit the sharing of such data, carelessness often results in its compromise.

iii). Finances –

- ✦ Financial information, such as salaries and wages, are very sensitive and should not be made public. This information if available can help competitive enterprises to understand and re-configure their salary structure accordingly.
- ✦ Similarly, availability of information about product pricing may also be used by competitive enterprises to price its products, competitively.

3.3 Information Security Policy

- An Information Security Policy is the statement of intent by the management about how to protect a company's information assets. An information security policy should be in written form.
- It provides instructions to employees about 'what kinds of behaviour or resource usage are required and acceptable', and about 'what is unacceptable'.
- In its basic form, an information security policy is a document that describes an organization's information security controls and activities.
- An Information Security Policy is the essential foundation for an effective and comprehensive information security program.
- It is the primary way in which management's information security concerns are translated into specific measurable and testable goals and objectives.
- It provides guidance to the people, who build, install, and maintain information systems.

- Information Security policy invariably includes rules intended to:
  - ✦ Preserve and protect information from any unauthorized modification, access or disclosure;
  - ✦ Limit or eliminate potential legal liability from employees or third parties; and
  - ✦ Prevent waste or inappropriate use of the resources of an organization.

3.3.1 Tools to Implement Policy: Standards, Guidelines, and Procedures

- Organizations develop standards, guidelines, and procedures that offer users, managers and others a clearer approach to implementing policy and meeting organizational goals.
- **Standards –**
  - ✦ Standards specify technologies and methodologies to be used to secure systems.
  - ✦ Standards, guidelines, and procedures should be promulgated throughout an organization through handbooks or manuals.
  - ✦ Organizational standards specify uniform use of specific technologies across the organization.
  - ✦ Standards are compulsory within an organization.
- **Guidelines** –
  - ✦ Guidelines help in smooth implementation of information security policy. Guidelines assist users, systems personnel, and others in effectively securing their systems.
  - ✦ Guidelines are used to ensure that specific security measures are not overlooked, although they can be implemented, and correctly so, in more than one way.
- **Procedures** –
  - ✦ Procedures are more detailed steps to be followed to accomplish particular security related tasks. Procedures assist in implementing applicable information security Policy.
  - ✦ These are detailed steps to be followed by users, system operations personnel, and others to accomplish a particular task.
  - ✦ Some organizations issue overall computer security manuals, regulations, handbooks, or similar documents.

3.3.2 Issues to address

- Information Security Policy does not need to be extremely extensive, but clearly state senior management's commitment to information security and be signed by appropriate senior manager.
- The policy should at least address the following issues:
  - ✦ A definition of information security,
  - ✦ Reasons why information security is important to the organization, and its goals & principles,
  - ✦ A brief explanation of the security policies, principles, standards and compliance requirement,
  - ✦ Definition of all relevant information security responsibilities; and
  - ✦ Reference to supporting documentation.
- The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents.

3.3.3 Members of Security Policy

- Security has to encompass managerial, technological and legal aspects.
- Security policy broadly comprises the following three groups of management:
  - ✦ Management members who have budget and policy authority,
  - ✦ Technical group who know what can and cannot be supported, and
  - ✦ Legal experts who know the legal ramifications of various policy charges.

3.3.4 Information Security Policies and their Hierarchy

- **Information Security Policy** –

  This policy provides a definition of Information Security, its overall objective and the importance that applies to all users.

- Various types of information security policies are:

i). User Security Policies –

- ✦ These include User Security Policy and Acceptable Usage Policy.

a) User Security Policy –

- This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.

b) Acceptable Usage Policy –

- This sets out the policy for acceptable use of email, Internet service & other IT resource.

ii). Organization Security Policies –

- ✦ These include Organizational Information Security Policy, Network & System Security Policy and Information Classification Policy.

a) Organizational Information Security Policy –

- This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information.

b) Network & System Security Policy –

- This policy sets out detailed policy for system and network security and applies to IT department users.

c) Information Classification Policy –

- This policy sets out the policy for the classification of information.

iii). Conditions of Connection –

- ✦ This policy sets out the Group policy for connecting to the network.
- ✦ It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.

3.3.5 Components of the Security Policy

- A good security policy should clearly state the following:
  - ✦ Purpose and Scope of the Document and the intended audience;

- ✦ The Security Infrastructure;
- ✦ Security policy document maintenance and compliance requirements;
- ✦ Incident response mechanism and incident reporting;
- ✦ Security organization Structure;
- ✦ Inventory and Classification of assets;
- ✦ Description of technologies and computing structure;
- ✦ Physical and Environmental Security;
- ✦ Identity Management and access control;
- ✦ IT Operations management;
- ✦ IT Communications;
- ✦ System Development and Maintenance Controls;
- ✦ Business Continuity Planning;
- ✦ Legal Compliances; and
- ✦ Monitoring and Auditing Requirements.

3.4 Information Systems Controls

- Control is defined as Policies, procedures, practices and enterprise structure that are designed to provide reasonable assurance that business objectives will be achieved and undesired events are prevented, detected and corrected.
- This is achieved by designing and effective information control framework, which comprise policies, procedures, practices, and organization structure.

3.4.1 Need for Controls in Information Systems

- Without adequate controls, anyone could look at the records and make amendments, some of which could remain undetected.
- The goals to reduce the probability of organizational costs of data loss, computer loss, computer abuse, incorrect decision making and to maintain the privacy; an organization's management must set up a system of internal controls.
- IS control procedure may include:
  - ✦ Strategy and direction,
  - ✦ General Organization and Management,
  - ✦ Access to IT resources, including data and programs,
  - ✦ System development methodologies and change control,
  - ✦ Operation procedures,
  - ✦ System Programming and technical support functions,
  - ✦ Quality Assurance Procedures,
  - ✦ Physical Access Controls,
  - ✦ BCP and DRP,

- ✦ Network and Communication,
- ✦ Database Administration, and
- ✦ Protective and detective mechanisms against internal and external attacks.

3.4.2 Objectives of Controls

- The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented, detected and corrected.
- The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss. Exposures are potential losses due to threats materializing.
- **Some categories of exposures are:**
  - ✦ Errors or omissions in data, procedure, processing, judgment and comparison;
  - ✦ Improper authorizations and improper accountability with regards to procedures, processing, judgment and comparison; and
  - ✦ Inefficient activity in procedures, processing and comparison.
- **Some of the critical control lacking in a computerized environment are:**
  - ✦ Lack of management understanding of IS risks and related controls;
  - ✦ Absence or inadequate IS control framework;
  - ✦ Absence of weak general controls and IS controls;
  - ✦ Lack of awareness and knowledge of IS risks and controls amongst business users and IT staff;
  - ✦ Complexity of implementation of controls in distributed computing environments and extended enterprises;
  - ✦ Lack of control features or their implementation in highly technology driven environments; and
  - ✦ Inappropriate technology implementations or inadequate security functionality in technologies implemented.
- **The control objectives serve two main purposes:**
  - ✦ Outline the policies of the organization as laid down by the management; and
  - ✦ A benchmark for evaluating whether control objectives are met.

3.4.3 Components of Internal Controls

- In a computerised environment, the goals of asset safeguarding, data integrity, system efficiency and system effectiveness can be achieved only if management sets up a system of internal control.
- Internal controls comprise of the following five interrelated components:

i). Control Environment –

- ✦ 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.

ii). Risk Assessment –

- ✦ 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.

iii). Control Activities –

- ✦ Elements that operate to ensure transaction are authorized, duties are segregated, adequate documents and records are maintained, assets & records are safeguarded and independent checks on performance and valuation of records. These are called accounting controls.

iv). Information and Communication –

- ✦ Elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.

v). Monitoring –

- ✦ The best internal controls are worthless if the company does not monitor them and make changes when they are not working.

3.4.4 Impact of Technology on Internal Controls

These are discussed as follows:

1) **Competent and Trustworthy Personnel –**
   - ✦ Personnel should have proper skill and knowledge to discharge their duties. But ensuring that an organization has competent and trustworthy information system personnel is a difficult task.
2) **Segregation of Duties –**
   - ✦ In a computerised system, the auditor should be concerned with the segregation of duties within the IT department. Segregation of duties prevents or detects errors or irregularities.
3) **Authorization Procedures –**
   - ✦ In computer systems, authorization procedures are embedded within a computer program. For example: In some on-line transaction systems, written evidence of individual data entry authorisation, may be replaced by computerised authorisation controls.
4) **Adequate Documents and Records –**
   - ✦ In computer systems, documents might not be used to support the initiation, execution and recording of some transaction. Thus, if the control over the protection & storage of documents, transaction details, and audit trails etc. are placed properly, it will not be a problem for auditor.
5) **Physical Control over Assets and Records –**
   - ✦ Physical control over access and records is critical in computer systems. Computerised financial systems have not changed the need to protect the data. The nature and types of control available have changed to address these new risks.
6) **Adequate Management Supervision –**
   - ✦ In computer system, data communication facilities can be used to enable employees to be closer to customers they service. So supervision of employees might have carried out remotely.

7) **Independent Checks on Performance –**

- ✦ If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.

8) **Comparing Recorded Accountability with Assets –**

- ✦ In a computer system, software is used to prepare the data. So, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.

9) **Delegation of Authority and Responsibility –**

- ✦ In a computer system, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users.

3.5 Classification of Information Systems Controls

- Internal controls can be classified into various categories to illustrate the interaction of various groups in the enterprise and their effect on information systems on different basis.

3.5.1 Classification on the basis of "Objective of Controls"

The controls can be classified as under:

1) **Preventive Controls –**

- Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring.
- Any control can be implemented in both manual and computerized environment for the same purpose.

- The broad **characteristics of preventive controls** are as follows:
  - ✦ A clear-cut understanding about the vulnerabilities of the asset;
  - ✦ Understanding probable threat; and
  - ✦ Provision of necessary controls for probable threats from materializing.
- **Example of preventive controls** are given as follows –
  - ✦ Employ qualified personal,
  - ✦ Segregation of duties
  - ✦ Access control
  - ✦ Vaccination against diseases
  - ✦ Documentation
  - ✦ Prescribing appropriate books for the course
  - ✦ Training and retraining of staff
  - ✦ Authorization of transaction
  - ✦ Validity, edit checks in the application
  - ✦ Firewalls
  - ✦ Passwords
  - ✦ Antivirus Software
- The following Table shows how the same purpose is achieved by using manual & computerized controls.

Purpose	Manual Control	Computerised Control
Restrict unauthorized entry into the premises	Build a gate and post a security guard.	Use access control software, smart card, biometrics, etc
Restrict unauthorized entry into the software applications	Keep the computer in a secured location and allow only authorised person to use the applications.	Use access control, viz. user id, password, smart card, etc.

2) Detective Controls –

- Detective controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence.
- The main **characteristics of detective controls** are given 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 appropriate person;
  - ✦ Interaction with the preventive control to prevent such acts from occurring; and
  - ✦ Surprise checks by supervisor.

- **Examples of detective controls** include:
  - ✦ Hash totals,
  - ✦ Check points in production jobs,
  - ✦ Echo control in telecommunications,
  - ✦ Error message over tape labels,
  - ✦ Duplicate checking of calculations,
  - ✦ Periodic performance reporting with variances,
  - ✦ Past-due accounts report,
  - ✦ The internal audit functions,
  - ✦ Intrusion detection system,
  - ✦ Cash counts and bank reconciliation, and
  - ✦ Monitoring expenditures against budgeted amount.

3) Corrective Controls –

- Corrective controls are designed to reduce impact or correct an error once it has been detected.
- Corrective controls may include use of default dates on invoices where an operator has tried to enter incorrect date. A Business Continuity Plan (BCP) is considered to be a corrective control.
- The main **characteristics of the corrective controls** are:
  - ✦ Minimizing the impact of the threat;
  - ✦ Identifying the cause of the problem;
  - ✦ Providing Remedy to the problems discovered by detective controls;
  - ✦ Getting feedback from preventive and detective controls;
  - ✦ Correcting error arising from a problem; and
  - ✦ Modifying the processing systems to minimize future occurrences of the incidents.
- **Examples of Corrective Controls** are given as follows:
  - ✦ Contingency planning,
  - ✦ Backup procedure,
  - ✦ Rerun procedures,
  - ✦ Change input value to an application system, and
  - ✦ Investigate budget variance and report violations.

4) Compensatory Controls –

- Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset.
- While designing the appropriate control one thing should be kept in mind - “The cost of the lock should not be more than the cost of the assets it protects.”
- There should be adequate compensatory measures, which may although not be as efficient as the appropriate control, but reduce the probability of loss to the assets. Such measures are called compensatory controls.

3.5.2 Classification on the basis of "Nature of Information System Resources"

These are given as follows:

1) **Environmental Controls –**

- These are the controls relating to IT environment such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc.
- This section deals with the external factors in the Information System and preventive measures to overcome these conflicts.

i). Environmental Issues and Exposures –

- Environmental exposures are primarily due to elements of nature.
- Common occurrences are Fire, Natural disasters-earthquake, volcano, hurricane, tornado, Power spike, Air conditioning failure, Electrical shock, Equipment failure, Water damage/flooding-even with facilities located on upper floors of high buildings.
- Other environmental issues and revelations include the following:
  - ✦ Is the power supply to the compiler equipment properly controlled so as to ensure that it remains within the manufacturer's specification?
  - ✦ Are the air conditioning, humidity and ventilation control systems protected against the effects of electricity using static rug or anti-static spray?
  - ✦ Is consumption of food, beverage and tobacco products prohibited, by policy, around computer equipment?
  - ✦ Are backup media protected from damage due to variation in temperatures or are they guarded against strong magnetic fields and water damage?
  - ✦ Is the computer equipment kept free from dust, smoke and other particulate matter?
- From the perspective of environmental exposures and controls, Information systems resources may be categorized as follows (with the primarily focus on facilities):

a) Hardware and Media –

- ✦ Includes Computing Equipment, Communication equipment, and Storage Media.

b) Information Systems Supporting Infrastructure or Facilities –

This typically includes the following:

- ✦ Physical Premises like Computer Rooms, Cabins, Server Rooms, Data Centre premises, Printer Rooms, Remote facilities, Staging Room, and Storage Areas,
- ✦ Communication Closets,
- ✦ Cabling ducts,
- ✦ Power Source, and
- ✦ Heating, Ventilation and Air Conditioning (HVAC).

c) Documentation –

- ✦ Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.

d) Supplies –

- The third party maintenance procedures and civil contractors whose entry and assess with respect to their scope of work assigned are to be monitored and logged.

e) People –

- The employees, visitors, supervisors and third party maintenance personnel are to be made responsible and accountable for environmental controls in their respective Information Processing Facility (IPF).

ii). Controls for Environmental Exposures

These are given as follows:

- **Water Detectors –**
  - In the computer room, water detectors should be placed under the raised floor and near drain holes. For easy identification, the location of the water detectors should be marked.
  - When activated, the detectors should produce an audible alarm that can be heard by security and control personnel.
- **Hand-Held Fire Extinguishers –**
  - Fire extinguishers should be in calculated locations throughout the area. They should be tagged for inspection and inspected at least annually.
- **Manual Fire Alarms –**
  - Hand-pull fire alarms should be purposefully placed throughout the facility. The resulting audible alarm should be linked to a monitored guard station.
- **Smoke Detectors –**
  - Smoke detectors are positioned at places above and below ceiling tiles. Upon activation, detectors should produce an audible alarm and must be linked to a monitored station.
- **Fire Suppression Systems –**
  - The alarms are activated when extensive heat is generated due to fire. The system should be segmented into zones so that fire in one part of facility does not activate entire system.
  - The fire suppression techniques vary upon situation but it is usually one of the following:

a) Dry-Pipe sprinkling systems –

- These are typically referred to as sprinkler systems.
- These pipes remain dry and upon activation by the electronic fire alarm water is sent through the pipe.
- Dry pipe systems have the advantage that any failure in the pipe will not result in water leaking into sensitive equipment.

b) Water based systems –

- These also function similar to the sprinkler systems.
- These systems are effective but also are unpopular because they damage equipment and property in the case of leakage or breakage of pipes facilities.

c) **Halon –**

- Halon systems contain pressurized Halon gases that remove oxygen from the air.
- Halon is preferred because of its inertness and does not damage equipment like water does. There should be an audible alarm and brief delay before discharge to permit personnel time to evacuate the area and disconnect system in case of false alarm.
- The drawback is, since Halon adversely affects the ozone layer, its usage is banned.

✦ **Strategically Locating the Computer Room –**

- To reduce the risk of flooding, the computer room should not be located in the basement or ground floor of a multi-storey building.

✦ **Regular Inspection by Fire Department –**

- An annual inspection by the fire department should be carried out to ensure that all fire detection systems act in accordance with building codes.

✦ **Fireproof Walls, Floors and Ceilings surrounding the Computer Room –**

- Information processing facility should be surrounded by walls that should control or block fire from spreading.

✦ **Electrical Surge Protectors –**

- The risk of damage due to power spikes can be reduced by using electrical surge protector.

✦ **Uninterruptible Power System (UPS)/Generator –**

- A UPS system consists of a battery or gasoline powered generator that interfaces between the main electrical power entering the facility and the electrical power supplied to the computer. The system cleanses the power to ensure wattage into computer is consistent.

✦ **Power Leads from Two Substations –**

- Electrical power lines that are exposed to many environmental dangers such as waters fire, lightning, cutting due to careless digging etc.

✦ **Emergency Power-Off Switch –**

- When there arise a necessity of immediate power shut down, an emergency power-off switch at the strategic locations would serve the purpose.

✦ **Wiring Placed in Electrical Panels and Conduit –**

- Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in the fire resistant panels and conduit.

✦ **Prohibitions against Eating, Drinking and Smoking within Information Processing Facility –**

- These activities should be prohibited from the information processing facility.

✦ **Fire Resistant Office Materials –**

- The materials used in the information processing facility such as Wastebaskets, curtains, desks, cabinets and other general office materials should be fire proof.

✦ **Documented and Tested Emergency Evacuation Plans –**

- Relocation plans should emphasize human safety, but should not leave information processing facilities physically unsecured.

2) Physical Access Controls –

- These are the controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media. Such controls include Access control doors, Security guards, door alarm, restricted entry to secure areas, visitor logged access, CCTV monitoring etc.

i). Physical Access Issues and Exposures

- The following points elaborate the results due to accidental or intentional violation of the access paths:
  - ✦ Abuse of data processing resources,
  - ✦ Blackmail,
  - ✦ Embezzlement,
  - ✦ Damage, vandalism or theft to equipments or documents,
  - ✦ Public disclosure of sensitive information, and
  - ✦ Unauthorized entry.
- **Possible perpetrators –**
  - ✦ Perpetrations may be because of employees, who are:
    - Accidental ignorant-someone who outrageously violates rules,
    - Addicted to a substance or gambling,
    - Discontented,
    - Experiencing financial or emotional problems,
    - Former employee,
    - Interested outsiders, such as competitors, thieves, organized crime and hackers,
    - Notified for their termination,
    - On strike, and
    - Threatened by disciplinary action or dismissal.
- **Exposures to confidential matters may be in form the unaware, accidental or anonymous persons. Other areas of concern include the following**:
  - ✦ How far the hardware facilities are controlled to reduce the risk of unauthorized access?
  - ✦ Are the hardware facilities protected against forced entry?
  - ✦ Are intelligent computer terminals locked or otherwise secured to prevent illegal removal of physical components like boards, chips and the computer itself?
  - ✦ When there is a need for the removal of computer equipment from its normal secure surroundings, are authorized equipment passes required for the removal?
- **The facilities that need to be protected from the auditor's perspective** are as follows:
  - ✦ Communication channels,
  - ✦ Computer room,
  - ✦ Control units and front-end processors,

- ✦ Dedicated telephones/telephone lines,
- ✦ Disposal sites,
- ✦ Input/output devices,
- ✦ Local area networks,
- ✦ Microcomputers and personal computers,
- ✦ Minicomputer establishments,
- ✦ Off-site backup file storage facility,
- ✦ On-site and remote printers,
- ✦ Operator consoles and terminals,
- ✦ Portable equipment,
- ✦ Power sources,
- ✦ Programming area,
- ✦ Storage rooms and supplies,
- ✦ Tape library, tapes, disks and all magnetic media, and
- ✦ Telecommunications equipment.

ii). Controls for Physical Access Exposures

- Physical access controls are designed to protect the organization from unauthorized access or to prevent illegal entry. The authorization given by the management should be explicit.
- Some of the more common access control techniques are discussed categorically as follows:

a) Locks on Doors –

These are given as follows:

i). Cipher locks (Combination Door Locks) –

- ✦ The cipher lock consists of a pushbutton panel that is mounted near the door outside of a secured area. To enter, a person presses a four digit number and the door will unlock for a predetermined period of time.
- ✦ Cipher locks are used in low security situations or when a large number of entrances and exits must be usable all the time.

ii). Biometric Door Locks –

- ✦ These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks.
- ✦ This system is used in extremely sensitive facilities to protect sensitive data.

iii). Bolting Door Locks –

- ✦ A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry the keys should be not be duplicated.

iv). Electronic Door Locks –

- ✦ A magnetic or embedded chip-based plastics card key or token may be entered into a reader to gain access in these systems.

b) Physical Identification Medium –

These are discussed below:

i). Personal Identification numbers (PIN) –

- A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual.

ii). Plastic Cards –

- These cards are used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands.

iii). Identification Badges –

- Special identification badges can be issued to personnel as well as visitors. For easy identification purposes, their colour of the badge can be changed.

c) Logging on Facilities –

These are given as under:

i). Manual Logging: All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see. Logging may happen at both fronts - reception and entrance to the computer room. A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before allowing entry inside the company.

ii). Electronic Logging: This feature is a combination of electronic and biometric security systems. The users logging can be monitored and the unsuccessful attempts being highlighted.

d) Other means of Controlling Physical Access –

Other important means of controlling physical access are given as follows:

(i) Video Cameras –

- Cameras should be placed at specific locations and monitored by security guards. The video supervision recording must be retained for possible future play back.

(ii) Security Guards –

- Extra security can be provided by appointing guards aided with CCTV feeds.

(iii) Controlled Visitor Access –

- A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.

(iv) Bonded Personnel –

- All service contract personnel, such as cleaning people and off-site storage services, should be asked to sign a bond.

(v) Dead Man Doors –

- These systems encompasses are a pair of doors that are found in entries to facilities such as computer rooms and document stations. The first entry door must close and lock, for the second door to operate, with the only one person permitted in the holding area.

(vi) Non–exposure of Sensitive Facilities –

- ✦ There should be no explicit indication such as presence of windows of directional signs hinting the presence of facilities such as computer rooms.

(vii) Computer Terminal Locks –

- ✦ These lock ensure that the device to desk is not turned on or cut off by unauthorized person

(viii) Controlled Single Entry Point –

- ✦ All incoming personnel can use controlled Single Entry Point. A controlled entry point is monitored by a receptionist. Multiple entry points increase chances of unauthorized entry.

(ix) Alarm System –

- ✦ Illegal entry can be avoided by linking alarm system to inactive entry point and the reverse flows of enter or exit only doors, so as to avoid illegal entry.

(x) Perimeter Fencing –

- ✦ Fencing at boundary of the facility may also enhance the security mechanism.

(xi) Control of out of hours of employee-employees –

- ✦ Employees who are out of office for a longer duration during the office hours should be monitored carefully. Their movements must be noted and reported to concerned officials.

(xii) Secured Report/Document Distribution Cart –

- ✦ Secured carts, such as mail carts, must be covered & locked and should always be attended.

- **The following are the advantages of electronic door locks over bolting & combinational locks**:
  - ✦ Through the special internal code, cards can be made to identity the correct individual.
  - ✦ Individuals access needs can be restricted through the special internal code & sensor devices.
  - ✦ Degree of duplication is reduced.
  - ✦ Card entry can be easily deactivated in the event an employee is terminated or a card is lost.
  - ✦ An administrative process, which may deal with Issuing, accounting for and retrieving the card keys, are also parts of security.

3) Logical Access Controls –

- Logical access controls are implemented to ensure that access to systems, data and programs is restricted to authorized users so as to safeguard information against unauthorized use, disclosure or modification, damage or loss.
- Logical access controls are system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.
- Assessing logical access controls involves evaluating the following critical procedures:
  - ✦ Logical access controls restrict users to authorized transactions and functions.
  - ✦ There are logical controls over network access.
  - ✦ There are controls implemented to protect the integrity of the application and the confidence of the public when the public accesses the system.

- **Logical Access Paths**

  These are given as follows:

  i). Online Terminals –

  - ✦ To access an online terminal, a user has to provide a valid login-ID and password. If additional authentication mechanisms are added along with password, it will strengthen the security.
  - ✦ Operator Console – The operator console is one of the crucial places where any intruders can play havoc. Hence, access to operator console must be restricted.
  - ✦ This can be done by:
    - Keeping the operator console at a place, which is visible, to all?
    - By keeping the operator console in a protected room accessible to selected personnel.

  ii). Dial-up Ports –

  - ✦ Using a dial up port, user at one location can connect remotely to another computer present at an unknown location via a telecommunication media.
  - ✦ A modem is a device, which can convert the digital data transmitted to analog data. Thus, the modem can act as an interface between remote terminal and the telephone line.
  - ✦ Security is achieved by providing a means of identifying the remote user to determine authorization to access.

  iii). Telecommunication Network –

  - ✦ In a Telecommunication network, a number of computer terminals, Personal Computers etc. are linked to the host computer through network or telecommunication lines.
  - ✦ Whether the telecommunication lines could be private or public, security is provided in the same manner as it is applied to online terminals.

- **Logical Access Issues and Exposures**
  - ✦ Controls that reduce the risk of misuse, theft, alteration or destruction should be used to protect unauthorized and unnecessary access to computer files.
  - ✦ Access control mechanisms should be applied not only to computer operators but also to end users programmers, security administrators, management or any other authorized user/s.
  - ✦ Access control mechanisms should provide security to the following applications:
    - Access control software,
    - Application software,
    - Data,
    - Data dictionary/directory,
    - Dial-up lines,
    - Libraries,
    - Logging files,
    - Operating systems Password library,
    - Procedure libraries,
    - Spool queues,

- System software,
- Tape files,
- Telecommunication lines,
- Temporary disk files, and Utilities.

- **Issues and Revelations related to Logical Access**

✦ Intentional or accidental exposures of logical access control encourage technical exposures and computer crimes. These are given as follows:

A. Technical Exposures –

✦ Technical exposures include unauthorized implementation or modification of data and software. Technical exposures include the following:

i). Data Diddling –

- Data diddling involves the change of data before or after they are entered into the system.
- A limited knowledge is required and it occurs before computer security can protect data.

ii). Bomb –

- Bomb is a piece of bad code deliberately planted by an insider or supplier of a program. An event, which is logical, triggers a bomb or time based.
- The bombs explode when the conditions of explosion get fulfilled causing the damage immediately. However, these programs cannot infect other programs.
- Bombs are generally of two types, which are given as follows:

a) Time Bomb –

- This name has been borrowed from its physical counterpart because of mechanism of activation. The computer time bomb causes a perverse activity, such as, disruption of computer system, modification or destruction of stored information etc. on a particular date and time for which it has been developed. The computer clock initiates it.

b) Logic Bomb –

- They resemble time bombs in their destruction activity. Logic bombs are activated by combination of events. These bombs can be set to go off at a future time or event.
- For example, a code like; “If a file named DELETENOT is deleted then destroy the memory contents by writing ones.” This code segment, on execution, may cause destruction of the contents of the memory on deleting a file named DELETENOT.

iii). Trojan Horse –

- Typically, a Trojan horse is an illicit coding contained in a legitimate program and causes an illegitimate action.
- A Trojan may:
  - Change or steal the password or
  - May modify records in protected files or
  - May allow illicit users to use the systems.

- Trojan Horses hide in a host and generally do not damage the host program. Trojans cannot copy themselves to other software in the same or other systems.
- The Trojans may get activated only if the illicit program is called explicitly. It can be transferred to other system only if an unsuspecting user copies the Trojan program.
- Christmas card is a well-known example of Trojan. It was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw the Christmas tree, but in addition, it will send copies of similar output to all other users connected to the network. Because of this message on other terminals, other users cannot save their half finished work.

iv). Worm –

- A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since, worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses.
- Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.

v). Rounding Down –

- This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.

vi). Salami Techniques –

- This involves slicing of small amounts of money from computerized transaction or account. Salami technique is slightly different from a rounding technique, as fix amount is deducted.

vii). Trap Doors –

- Trap doors allow insertion of specific logic, such as program interrupts that permit a review of data. They also permit insertion of unauthorized logic.

B. Computer Crime Exposures –

- ✦ Computer systems are used to steal money, goods, software or corporate information. Crimes are also committed when false data or unauthorized transaction is made.
- ✦ Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations.
- ✦ These are given as follows:

i). Financial Loss –

- Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.

ii). Legal Repercussions –

- An organization has to adhere to many laws while developing security policies and procedures. The organizations will be exposed to lawsuits from investors and insurers if there have no proper security measures.

iii). Loss of Credibility or Competitive Edge –

- In order to maintain competitive edge, companies needs credibility and public trust. This credibility will be shattered resulting in loss of business & prestige if security violation occur

iv). Blackmail/Industrial Espionage –

- By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.

v). Disclosure of Confidential, Sensitive or Embarrassing Information –

- These events can spoil the reputation of the organization. Legal or regulatory actions against the company may be also a result of disclosure.

vi). Sabotage –

- People, who may not be interested in financial gain but who want to spoil the credibility of the company or to will involve in such activities.

vii). Spoofing –

- A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique.
- Spoofing occurs only after a particular machine has been identified as vulnerable. A penetrator makes the user think that s/he is interacting with the operating system.

C. Asynchronous Attacks –

- Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that is waiting to be transmitted are liable to unauthorized access called asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions.
- There are many forms of asynchronous attacks; some of them are given as follows:

i). Data Leakage –

- Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.

ii). Wire-tapping –

- This involves spying on information being transmitted over telecommunication network.

iii). Piggybacking –

- This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions.
- This involves intercepting communication between the operating system and the user and modifying them or substituting new messages. A special terminal is tapped into the communication for this purpose.

iv). Shutting Down of the Computer/Denial of Service –

- This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer. Individuals, who know the high-level systems log on-ID initiate shutting down process.

- The security measure will function effectively if there are appropriate access controls on the logging on through a telecommunication network. When overloading happens some systems have been proved to be vulnerable to shutting themselves.
- Hackers use this technique to shut down computer systems over the Internet.

D. Remote and distributed data processing applications can be controlled in many ways.

Some of these are given as follows:

- ✦ Remote access to computer and data files through the network should be implemented.
- ✦ Having a terminal lock can assure physical security to some extent.
- ✦ Applications that can be remotely accessed via modems and other devices should be controlled.
- ✦ Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
- ✦ In order to prevent the unauthorized user's access to the system, there should be proper control mechanisms over system documentation and manuals.
- ✦ Data transmission over remote locations should be controlled.
- ✦ When replicated copies of files exist at multiple locations it must be ensured that all are identical copies contain the same information.
- ✦ Logical Access Violators are often the same people who exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex.

  They are mainly:

  – Hackers;
  – Employees (authorized or unauthorized);
  – IS Personnel;
  – End Users;
  – Former Employees;
  – Interested or Educated Outsiders;
  – Competitors;
  – Foreigners;
  – Organized criminals;
  – Crackers;
  – Part-time and Temporary Personnel;
  – Vendors and consultants; and
  – Accidental Ignorant – Violation done unknowingly.

- **Logical Access Control across the System**
  - ✦ The purpose of logical access controls is to restrict access to information assets/resources.
  - ✦ They are expected to provide access to information resources on a need to know and need to do basis using principle of least privileges.

- ✦ The data, an information asset, can be:
  - Used by an application (Data at Process);
  - Stored in some medium (Back up) (Data at Rest);
  - Or it may be in transit (being transferred from one location to another).

3.5.3 Classification on the basis of "Functional Nature"

- When reviewing a client's control systems, the auditor will be able to identify three components of internal control. Each component is aimed at achieving different objectives.
- These controls are given as follows:

(i) Internal Accounting Controls –

- ✦ The Controls which are intended to safeguard the client's assets and ensure the reliability of the financial records are called internal accounting controls.

(ii) Operational Controls –

- ✦ These deals with the day-to-day operations, functions and activities to ensure that the operational activities are contributing to business objectives.

(iii)Administrative Controls –

- ✦ These are concerned with ensuring efficiency and compliance with management policies, including the operational controls.

3.5.4 Classification on the basis of "Audit Functions"

- Auditors have found two ways to be especially useful when conducting information systems audit. These are discussed below:

1) Managerial Controls –

- We shall examine controls over the managerial controls that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization.
- The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-today basis as discussed in Table.

Management Subsystem	Description of Subsystem
Top Management	Top management must ensure that information systems function is well managed. It is responsible primarily for long – run policy decisions on how Information Systems will be used in the organization.
Information Systems Management	IS management has overall responsibility for the planning and control of all information system activities. It also provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.
Programming Management	It is responsible for programming new system; maintain old systems and providing general systems support software.

Systems Development Management	Systems Development Management is responsible for the design, implementation, and maintenance of application systems.
Data Administration	Data administration is responsible for addressing planning and control issues in relation to use of an organization's data.
Quality Assurance Management	It is responsible for ensuring information system development, implementation, operation and maintenance to established quality standards.
Security Administration	It is responsible for access controls and physical security over the information systems function.
Operations Management	It is responsible for planning and control of the day-to-day operations of information systems.

2) Application Controls –

- These include the programmatic routines within the application program code.
- The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage.
- Any function or activity that works to ensure the processing accuracy of the application can be considered an application control.
- The categories of Application controls are listed below in the Table.

Application Subsystem	Description of Subsystem
Boundary	Comprises the components that establish the interface between user & system.
Input	Comprises the components that capture, prepare, and enter commands and data into the system.
Communication	Comprises the components that transmit data among subsystems and systems.
Processing	Comprises the components that perform decision making, computation, classification, ordering, and summarization of data in the system.
Database	Comprises components that define, add, access, modify & delete data in system.
Output	Comprises the components that retrieve and present data to users of the system.

3.6 Managerial Controls and their Categories

- The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to-day basis.

3.6.1 Top Management and Information Systems Management Controls

- The senior manager who take responsibility for IS function in an organization face many challenge.
- The major functions that a senior manager must perform are as follows:

i). Planning – determining the goals of the information systems function and the means of achieving these goals;

ii). Organizing – gathering, allocating, and coordinating the resources needed to accomplish goals;

iii). **Leading –** motivating, guiding, and communicating with personnel; and

iv). **Controlling –** comparing actual performance with planned performance as a basis for taking any corrective actions that are needed.

- Top management must prepare two types of information systems plans for information systems function: a Strategic plan and an Operational plan.
  - ✦ The strategic Plan is the long-run plan covering say next three to five years of operation whereas the Operational Plan is the short-plan covering, say next one to three years of operation.
  - ✦ Both the plans need to be reviewed regularly and updated as the need arises. The planning depends upon factors such as the importance of existing systems, the importance of proposed information systems, and the extent to which IT has been integrated into daily operations

3.6.2 Systems Development Management Controls

- Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems.
- Three different type of audits may be conducted during system development process as follows -

i). Concurrent Audit

- ✦ Auditors are members of the system development team. They assist the team in improving quality of systems development for the specific system they are building and implementing.

ii). Post implementation Audit

- ✦ Auditors seek to help an organization learn from its experiences in the development of a specific application system. They might be evaluating whether the system needs to be scrapped, continued, or modified in some way.

iii). General Audit

- ✦ Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions.

3.6.3 Programming Management Controls

- Primary objectives of this phase are to produce or acquire and to implement high-quality program.
- The purpose of control phase during software development or acquisition is to monitor progress against plan and to ensure software released for production use is authentic, accurate & complete.
- The program development life cycle comprises six major phases – Planning; Design; Control; Coding; Testing; and Operation and Maintenance.

Phases of Program Development Life Cycle

Phase	Controls
Planning	Techniques like Work Breakdown Structures, Gantt charts and PERT Charts can be used to monitor progress against plan.
Design	A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.

Coding	Programmers must choose a module implementation and integration strategy (like Top-down, bottom-up and Threads approach), a coding strategy (that follows the percepts of structured programming), and a documentation strategy (to ensure program code is easily readable and understandable).
Testing	These tests are to ensure that a developed or acquired program achieves its specified requirements. Three types of testing can be undertaken: • **Unit Testing** – which focuses on individual program modules; • **Integration Testing** – Which focuses in groups of program modules; and • **Whole-of-Program Testing** – which focuses on whole program.
Operation and Maintenance	Management establishes formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a timely basis. Three types of maintenance can be used – • **Repair Maintenance** – in which program errors are corrected; • **Adaptive Maintenance** – in which the program is modified to meet changing user requirements; and • **Perfective Maintenance** - in which the program is tuned to decrease the resource consumption.

3.6.4 Data Resource Management Controls

- Many organizations now recognize that data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented.
- For data to be managed better users must be able to share data, data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed.
- It must be controlled carefully, because the consequences are serious if the data definition is compromised or destroyed.
- Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities.

3.6.5 Quality Assurance Management Controls

- Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software.
- Organizations are undertaking more ambitious information systems projects that require more stringent quality requirements and are becoming more concerned about their liabilities if they produce and sell defective software.

3.6.6 Security Management Controls

- Information security administrators are responsible for ensuring that information systems assets are secure.

- Some of the major threats to the security of information systems and their controls are as follows:

Threat	Control
Fire	Well-designed, reliable fire-protection systems must be implemented.
Water	Facilities must be designed and sited to mitigate losses from water damage.
Energy Variations	Voltage regulator, circuit breaker, uninterruptible power supply can be used
Structural Damage	Facilities must be designed to withstand structural damage.
Pollution	Regular cleaning of facilities and equipment should occur.
Unauthorized Intrusion	Physical access controls can be used.
Viruses and Worms	Controls to prevent use of virus-infected programs and to close security loopholes that allow worms to propagate.
Misuse of software, data & services	Code of conduct to govern the actions of information systems employees.
Hackers	Strong, logical access control to mitigate losses from the activities of hackers.

3.6.7 Operations Management Controls

- Operations management is responsible for the daily running of hardware and software facilities.
- Operations management typically performs controls over the functions like Computer Operations, Communications Network Control, Data Preparation and Entry, Production control, File Library; Documentation and Program Library; Technical support; and Performance Monitoring.
- Operations management control must continuously monitor the performance of the hardware/ software platform to ensure that systems are executing efficiently, an acceptable response time or turnaround time is being achieved, and an acceptable level of uptime is occurring.

3.7 Application Controls and their Categories

- Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise.
- Different Application Controls are as follows:
  - ✦ Boundary Controls
  - ✦ Input Controls
  - ✦ Communication Controls
  - ✦ Processing Controls
  - ✦ Database Controls
  - ✦ Output Controls

3.7.1 Boundary Controls

- The major controls of the boundary system are the access control mechanisms. Access controls mechanism links the authentic users to the authorized resources, they are permitted to access.
- The access control mechanism has three steps of identification, authentication and authorization with respect to the access control policy implemented.
- The user can provide three factors of input information for the authentication process and gain access to his required resources, which are descried as below –

Class of information	Types of input
Personal Information	Name, Birth date, account number, password, PIN
Personal characteristics	Fingerprint, voice, hand size, signature, retinal pattern.
Personal objects	Identification cards, badge, key, finger ring.

- Major Boundary Control techniques are given as follows:

i). Cryptography –

- ✦ It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file.
- ✦ A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst.
- ✦ Three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).

ii). Passwords –

- ✦ User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control.

iii). Personal Identification Numbers (PIN) –

- ✦ PIN is similar to a password assigned to a user by an institution a random number stored in its database independent to a user identification details, or a customer selected number.

iv). Identification Cards –

- ✦ Identification cards are used to store information required in an authentication process.
- ✦ These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.

v). Biometric Devices –

- ✦ Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

3.7.2 Input Controls

- Input controls are responsible for ensuring the accuracy and completeness of data. Input controls are important since substantial time is spent on input of data, involve human intervention and are, therefore error and fraud prone.
- Input controls are divided into the following broad classes:
  - ✦ Source Document Control,
  - ✦ Data Coding Controls
  - ✦ Batch Controls, and
  - ✦ Validation Controls.

The details of each aforementioned class are given as under:

1) Source Document Controls –

- In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments.
- Source document fraud can be used to remove assets from the organization.
- To control against this type of exposure, the organization must implement control procedures over source documents to account for each document, as described below:

i). Use pre-numbered source documents –

- ✦ Source documents should come pre-numbered from the printer with a unique sequential number on each document.
- ✦ Source document numbers enable accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.

ii). Use source documents in sequence –

- ✦ Source documents should be distributed to the users and used in sequence. This requires adequate physical security be maintained over the source document inventory at user site

iii). Periodically audit source documents –

- ✦ Missing source documents should be identified by reconciling document sequence numbers. Documents not accounted for should be reported to management.

2) Data Coding Controls –

- Two types of errors can corrupt a data code and cause processing errors. These are transcription and transposition errors, which are as discussed below:

i). Transcription Errors

These fall into three classes:

- ✦ **Addition errors** occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.
- ✦ **Truncation errors** occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.
- ✦ **Substitution errors** are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.

ii). Transposition Errors –

There are two types of transposition errors.

- ✦ **Single transposition errors** occur when two adjacent digits are reversed. For instance, 12345 are recorded as 21345.
- ✦ **Multiple transposition errors** occur when nonadjacent digits are transposed. For example, 12345 are recorded as 32154.

3) Batch Controls

- Batching is the process of grouping together transactions that bear some type of relationship to each other. Various controls can be exercises over the batch to prevent or detect errors.
- Two types of batch controls occur:

i). Physical Controls –

- ✦ These controls are groups of transactions that constitute a physical unit.
- ✦ For example – source documents might be obtained via the email, assembled into batches, spiked and tied together, and then given to a data-entry clerk to be entered into an application system at a terminal.

ii). Logical Controls –

- ✦ These are group of transactions bound together on some logical basis, rather than being physically contiguous.
- ✦ For example - different clerks might use the same terminal to enter transaction into an application system. Clerks keep control totals of transactions into an application system.

- To identify errors or irregularities in either a physical or logical batch, three types of control totals can be calculated as shown in Table.

Control Total Type	Explanation
Financial totals	Grand totals calculated for each field containing money amounts.
Hash totals	Grand totals calculated for any code on a document in the batch, e.g., the source document serial numbers can be totaled.
Document/Record Counts	Grand totals for the number of documents in record in the batch.

4) Validation Controls –

- Validation controls are intended to detect errors in the transaction data before data are processed
- There are three levels of input validation controls:
  - ✦ Field interrogation,
  - ✦ Record interrogation, and
  - ✦ File interrogation.

The details of the same are given as follows:

i). Field Interrogation –

- It involves programmed procedures that examine the characters of the data in the field.

- Various field checks used to ensure data integrity have been described below:

a) Limit Check –

- ✦ This is a basic test for data processing accuracy and may be applied to both the input and output data. The field is checked by the program against predefined limits to ensure that no input/output error has occurred or at least no input error has exceeding certain limits.

b) Picture Checks –

- ✦ These check against entry into processing of incorrect/invalid characters.

c) Valid Code Checks –

- ✦ Checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid.

d) Check Digit –

- ✦ A check digit is a control digit added to the code when it is originally assigned that allows the integrity of the code to be established during subsequent processing. The check digit can be located anywhere in the code, as a prefix, suffix or embedded someplace in middle.

e) Arithmetic Checks –

- ✦ Simple Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.

f) Cross Checks –

- ✦ It may be employed to verify fields appearing in different files to see that the result tally.

ii). Record Interrogation: These are discussed as follows:

a) Reasonableness Check –

- ✦ Whether the value specified in a field is reasonable for that particular field?

b) Valid Sign –

- ✦ The contents of one field may determine which sign is valid for a numeric field.

c) Sequence Check –

- ✦ If physical records follow a required order matching with logical records.

iii). File Interrogation –

These are discussed as follows:

a) Version Usage –

- ✦ Proper version of a file should be used for processing the data correctly.

b) Internal and External Labeling –

- ✦ Labeling of storage media is important to ensure that proper files are loaded for process.
- ✦ Where there is a manual process for loading files, external labeling is important. Where there is an automated tape loader system, internal labeling is more important.

c) Data File Security –

- ✦ Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability. These controls ensure that the correct file is used for processing.

d) Before and after Image and Logging –

- ✦ The application may provide for reporting of before and after images of transactions. These images combined with the logging of events enable re-constructing the data file back to its last state of integrity, after which the application can ensure that the incremental transactions are rolled back or forward.

e) File Updating and Maintenance Authorization –

- ✦ Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected.

f) Parity Check –

- ✦ When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.

3.7.3 Communication Controls

- Three major types of exposure arise in the communication subsystem:
  - ✦ Transmission impairments can cause difference between the data sent and the data received;
  - ✦ Data can be lost or corrupted through component failure; and
  - ✦ A hostile party could seek to subvert data that is transmitted through the subsystem.
- Communication controls are of following types –
  - **a)** Physical Component Controls
  - **b)** Line Error Controls
  - **c)** Flow Controls
  - **d)** Link Controls
  - **e)** Topological Controls
  - **f)** Channel Access Controls
  - **g)** Internet Working Controls

1) Physical Component Controls –

- These controls incorporate features that mitigate the possible effects of exposures.
- An overview of how physical components can affect communication subsystem reliability are –

i). Transmission Media

- ✦ It is a physical path along which a signal can be transmitted between a sender and a receiver. It is of two types:
  - **Guided/Bound Media** in which the signals are transported along an enclosed physical path like – Twisted pair, coaxial cable, and optical fiber.
  - In **Unguided Media**, the signals propagate via free-space emission like – satellite microwave, radio frequency and infrared.

ii). Communication Lines

- ✦ The reliability of data transmission can be improved by choosing a private (leased) communication line rather than a public communication line.

iii). Modem

- ✦ Increases the speed with which data can be transmitted over a communication line.
- ✦ Reduces the number of line errors that arise through distortion if they use equalization.
- ✦ Reduces the number of line errors that arise through noise.

iv). Port Protection Devices

- ✦ Used to mitigate exposures associated with dial-up access to a computer system. The port-protection device performs various security functions to authenticate users.

v). Multiplexers And Concentrators

- ✦ These allow the band width or capacity of a communication line to be used more effectively.
- ✦ These share the use of a high-cost transmission line among many messages that arrive at the multiplexer or concentration point from multiple low cost source lines.

2) Line Error Control –

- Whenever data is transmitted over a communication line, recall that it can be received in error because of attenuation distortion or noise that occurs on the line. These errors must be detected and corrected.
  - ✦ **Error Detection –**
    - The errors can be detected by either using a loop (echo) check or building some form of redundancy into the message transmitted.
  - ✦ **Error Correction –**
    - When line errors have been detected, they must then be corrected using either forward error correcting codes or backward error correcting codes.

3) Flow Controls –

- Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data.
- For example, a main frame can transmit data to a microcomputer terminal. The microcomputer cannot display data on its screen at the same rate the data arrives from the main frame.
- Flow controls will be used to prevent the mainframe swamping the microcomputer and, as a result, data is lost.

4) Link Controls –

- The link management components mainly use two common protocols HDLC (Higher Level Data Link control) and SDLC (Synchronous Data Link Control).

5) Topological Controls –

- A communication network topology specifies the location of nodes within a network, ways in which these nodes will be linked and the data transmission capabilities of links between nodes.

a) Local Area Network Topologies –

- ✦ Local Area Networks tend to have three characteristics:
  - They are privately owned networks;
  - They provide high-speed communication among nodes; and

- They are confined to limited geographic areas.

✦ Local Area Networks are implemented using four basic types of topologies –
(1) Bus topology, (2) Tree topology, (3) Ring topology, and (4) Star topology.

✦ Hybrid topologies like the star-ring topology and the star-bus topology are also used.

b) Wide Area Network Topologies –

✦ Wide Area Networks have the following characteristics:

- They often encompass components that are owned by other parties;
- They provide relatively low-speed communication among nodes; and
- They span large geographic areas With the exception of the bus topology, all other topologies that are used to implement LANs can also be used to implement WANs.

6) Channel Access Controls –

- Two different nodes in a network can compete to use a communication channel. Whenever the possibility of contention for the channel exists, some type of channel access control technique must be used.
- These techniques fall into two classes: Polling methods and Contention methods.

a) Polling:

✦ Polling techniques establish an order in which a node can gain access to channel capacity.

b) Contention Methods:

✦ Using contention methods, nodes in a network must compete with each other to gain access to a channel. Each node is given immediate right of access to the channel.

✦ Whether the node can use the channel successfully, depends on the actions of other nodes connected to the channel.

7) Internetworking Controls –

- Internetworking is the process of connecting two or more communication net-works together to allow the users of one network to communicate with the users of other networks.
- Three types of devices are used to connect sub-networks in an internet as follows –

a) Bridge –

✦ A bridge connects similar local area networks.

b) Router –

✦ A router performs all the functions of a bridge. In addition, it can connect heterogeneous local area networks and direct network traffic over the fastest channel between two nodes that reside in different sub-networks.

c) Gateway –

✦ Gateways are the most complex of the three network connection devices.

✦ Their primary function is to perform protocol conversion to allow different types of communication architectures to communicate with one another.

✦ The gateway maps functions performed in an application on one computer to the function performed by a different application with similar functions on another computer.

3.7.4 Processing Controls

- The processing subsystem is responsible for computing, sorting, classifying, and summarizing data.
- Its major components are
  - the Central Processor in which programs are executed,
  - the real or virtual memory in which program instructions and data are stored,
  - the operating system that manages system resources, and
  - the application programs that execute instructions to achieve specific user requirements.

1) Processor Controls –

- The processor has three components:
  - **a)** A Control unit, which fetches programs from memory and determines their type;
  - **b)** An Arithmetic and Logical Unit, which performs operations; and
  - **c)** Registers that are used to store temporary results and control information.
- Four types of controls that can be used to reduce expected losses from errors and irregularities associated with Central processors are explained below –

i). Error Detection and Correction Controls

- ✦ Occasionally, processors might malfunction. The causes could be design error, damage, manufacturing defects, fatigue, electromagnetic interference, and ionizing radiation.

ii). Multiple Execution States Controls

- ✦ It is important to determine the number of and nature of the execution states enforced by the processor. This helps auditors to determine which user processes will be able to carry out unauthorized activities.

iii). Timing Controls

- ✦ An operating system might get stuck in an infinite loop. In absence of any control, program will retain use of processor & prevent other program from undertaking their work.

iv). Component Replication Controls

- ✦ In some cases, processor failure can result in significant losses. If processor failure is permanent in multicomputer or multiprocessor architecture, the system might reconfigure itself to isolate the failed processor.

2) Real Memory Controls –

- This comprises the fixed amount of primary storage in which programs or data must reside for them to be executed or referenced by the central processor.
- Real memory controls seek to detect and correct errors that occur in memory cells and to protect areas of memory assigned to a program from illegal access by another program.

3) Virtual Memory Controls –

- Virtual Memory exists when the addressable storage space is larger than the available real memory space. To achieve this outcome, a control mechanism must be in place that maps virtual memory addresses into real memory addresses.

4) Data Processing Controls –

- These perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed. Normally, the processing controls are enforced through database management system that stores the data.
- Various processing controls are given as follows:

i). Run-to-run Totals –

- ✦ These help in verifying data that is subject to process through different stages. A specific record probably the last record can be used to maintain the control total.

ii). Reasonableness Verification –

- ✦ Two or more fields can be compared and cross verified to ensure their correctness.

iii). Edit Checks –

- ✦ Edit checks can used at the processing stage to verify accuracy and completeness of data.

iv). Field Initialization –

- ✦ Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing it.

v). Exception Reports –

- ✦ Exception reports are generated to identify errors in the data processed. Such exception reports give the transaction code and why a particular transaction was not processed or what is the error in processing the transaction.

❖ **Access Control Mechanisms:**

- An Access Control Mechanism is associated with identified, authorized users the resources they are allowed to access and action privileges.
- The mechanism processes the users request for Real time Memory and Virtual Memory resources in three steps:

i). Identification –

- ✦ First and foremost, the users have to identify themselves.

ii). Authentication –

- ✦ Secondly, the users must authenticate themselves and the mechanism must authenticate itself. The mechanism accesses previously stored information about users, the resources they can access and the action privileges they have; then it permits or denies the request.
- ✦ Users may provide four factor of authentication information as described below –
  - **Remembered information** – Name, Account number, passwords
  - **Objects Possessed by the user** – Badge, plastic card, key
  - **Personal characteristics** – Finger print, voice print, signature
  - **Dialog** – Through/around computer

iii). Authorization –

- ✦ Third, the users request for specific resources, their need for those resources and their areas of usage of these resources.

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

a) Ticket oriented approach

- In a ticket-oriented approach to authorization, the access control mechanism assigns 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.
- The primary advantage of the ticket oriented or capability system is its run-time efficiency. When a user process is executing, its capability list can be stored in some fast memory device. When the process seeks access to a resource, the access control mechanism simply looks up the capability list to determine if the resource is present in the list and whether if the user is permitted to take the desired action.

b) List oriented approach

- In a list-oriented 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. This mechanism operates via a column in the matrix.
- The major advantage of list-oriented system is that it allows efficient administration of capabilities. Each user process has a pointer to the access control list for a resource. Thus, the capabilities for a resource can be controlled since they are stored in one place.

3.7.5 Database Controls

- Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called update controls and report controls.
- **Major update controls** are given as follows:

a) Sequence Check between Transaction and Master Files –

- Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updation, insertion or deletion of records in the master file with respect to the transaction records. .

b) Ensure All Records on Files are processed –

- While processing, the transaction file records mapped to the respective master file, and the end-of-file of the transaction file with respect to the end-of-file of master file is to be ensured

c) Process multiple transactions for a single record in the correct order –

- Multiple transactions can occur based on a single master record (e.g. dispatch of a product to different distribution centers).

d) Maintain a suspense account –

- When mapping between the master record to transaction record results in a mismatch due to failure in the corresponding record entry in the master record; then these transactions are maintained in a suspense account.

- **Major Report controls** are given as follows:

  a) Standing Data –

  - ✦ Application programs use many internal tables to perform various functions like gross pay calculation, billing calculation based on a price table, bank interest calculation etc. Periodic monitoring of these internal tables by means of manual check or by calculating a control total is mandatory.

  b) Print-Run-to Run control Totals –

  - ✦ Run-to-Run control totals help in identifying errors like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.

  c) Print Suspense Account Entries –

  - ✦ The suspense account entries are to be periodically monitors with the respective error file and action taken on time.

  d) Existence/Recovery Controls –

  - ✦ The back-up strategies are implemented using prior version and logs of transactions or changes to the database.
  - ✦ Recovery strategies involve roll-forward (current state database from a previous version) or the roll-back (previous state database from the current version) methods.

3.7.6 Output Controls

- Output controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner.
- Whatever the type of output, it should be ensured that the confidentiality and integrity of the output is maintained. Output controls have to be enforced both in batch-processing environment as well as in an online environment.
- Various Output Controls are given as follows:

  i). Storage and logging of sensitive, critical forms –

  - ✦ Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies.

  ii). Logging of output program executions –

  - ✦ When programs used for output of data are executed, these should be logged & monitored; otherwise confidentiality/integrity of the data may be compromised.

  iii). Spooling/queuing –

  - ✦ “Spool” is an acronym for “Simultaneous Peripherals Operations Online”.
  - ✦ This is a process used to ensure that the user is able to continue working, while the print operation is getting completed. When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is then “spooled” to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification.
  - ✦ A queue is the list of documents waiting to be printed on a particular printer; this should not be subject to unauthorized modifications.

iv). Controls over printing –

- ✦ Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place.

v). Report distribution and collection controls –

- ✦ Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data.
- ✦ A log should be maintained for reports that were generated and to whom these were distributed. Uncollected reports should be stored securely.

vi). Retention controls –

- ✦ Retention controls consider the duration for which outputs should be retained before being destroyed. Various factors ranging from the need of the output, use of the output, to legislative requirements would affect the retention period.

3.8 General Controls

- Some of the general controls that are quite commonly used are as follows –
  - **a)** Organisational Controls
  - **b)** Management Controls
  - **c)** Financial Controls
  - **d)** BCP Controls
  - **e)** Operating System Controls
  - **f)** Data Management Controls
  - **g)** System Development Controls
  - **h)** Computer Centre Security Controls
  - **i)** Internet and Intranet Controls
  - **j)** Personal Computer Controls

3.8.1 Organizational Controls

- These controls are concerned with the decision-making processes that lead to management authorization of transactions.
- In manual environment, the task may be segregated in the following manner:
  - ✦ Segregate the task of transaction authorization from transaction processing;
  - ✦ Segregate record keeping from asset custody; and
  - ✦ Divide transaction-processing tasks among individuals.
- In a Computer Based Information System (CBIS), segregation is done at the following functional levels, to adhere the following principles of internal controls:
  - ✦ Segregating the maker / creator from checker;
  - ✦ Segregating the asset record keeper from physical asset keeper; and
  - ✦ Regular checking of effectiveness of internal controls.

- **To save from compromises that occur due to above, it is required that following must be done:**
  - ✦ Documentation is improved because the maintenance group requires documentation to perform its maintenance duties.
  - ✦ The programmer is denied the access to the production environment, to mitigate the programmed frauds.
  - ✦ Companies with large data processing facilities separate data processing from business units to provide control over its costly hardware, software, and human resources.
  - ✦ Organizational control techniques include documentation of the following:
    - **a)** Reporting responsibility and authority of each function,
    - **b)** Definition of responsibilities and objectives of each functions,
    - **c)** Policies and procedures,
    - **d)** Job descriptions, and
    - **e)** Segregation of duties.

  These are discussed as follows:

1) Responsibilities and objectives –

- Each IS function must be clearly defined and documented including systems software, application programming and system development, database administration, and operations.
- The senior manager and managers of the individual groups make up the IS management team responsible for the effective and efficient utilization of IS resources.
- Their responsibilities include:
  - ✦ Providing information to senior management on the IS resources, to enable senior management to meet strategic objectives;
  - ✦ Planning for expansion of IS resources;
  - ✦ Controlling the use of IS resources; and
  - ✦ Implementing activities and functions that support accomplishment of company's strategic plan.

2) Policies, standards, procedures and practices –

- Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. These are the standards and instructions that all IS personnel must follows.
- Procedures establish the instructions that individuals must follow to compete their daily assigned tasks.
- Documented policies should exist in IS for:
  - ✦ Use of IS resources,
  - ✦ Physical security,
  - ✦ Data security
  - ✦ On-line security,

- ✦ Use of Information systems,
- ✦ Reviewing, evaluating, and purchasing hardware and software,
- ✦ System development methodology, and
- ✦ Application program changes.

- Documented procedures should exist for all data processing activities.

3) Job descriptions –

- These communicate management's specific expectations for job performance. Job procedures establish instructions on how to do the job and policies define the authority of the employee.
- Job descriptions establish responsibility and the accountability of the employee's actions.

4) Segregation of duties –

- Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only duties stipulated for their respective job & position.
- The main purpose is to prevent or detect errors or irregularities by applying suitable controls. It reduces the likelihood of errors and wrongful acts going undetected because the activities of one group or individual will serve as a check on the activities of the other.
- It is the responsibility of senior management to implement a division of role & responsibilities, which should exclude the possibility for a single individual to subvert a critical process.
- The irregularities are frauds due to various facts e.g.:
  - ✦ Theft of assets like funds, IT equipment, the data and programs;
  - ✦ Modification of the data leading to misstated and inaccurate financial statements; and
  - ✦ Modification of programs in order to enact irregularities like rounding down, salami etc.
- The critical factors to be considered in segregation of duties in a computerized information system are:
  - ✦ Nature of business operations;
  - ✦ Managerial policy;
  - ✦ Organization structure with job description; and
  - ✦ IT resources deployed such as: Operating system, Networking, Database, Application software, Technical staff available, IT services provided in-house or outsourced, Centralized or decentralized IT operations.

❖ **Examples of segregation of duties are:**

- ✦ Systems software programming group from the application programming group;
- ✦ Database administration group from other data processing activities;
- ✦ Computer hardware operations from the other groups;
- ✦ Systems analyst function from the programming function;
- ✦ Physical, data, and online security group(s) from the other IS functions; and
- ✦ IS Audit from business operations groups.

- **From a functional perspective, segregation of duties should be maintained between the following functions:**
  - Information systems use,
  - Data entry,
  - Computer operation,
  - Network management,
  - System administration,
  - Systems development and maintenance,
  - Change management,
  - Security administration, and
  - Security audit.
- **There are various general guidelines, with reference to 'Segregation of Duties', which may be followed in addition with concepts like, the maker should not be the checker**:
  - Separate those, who can run live programs e.g. operations department, from those who can change programs e.g. programmers. This is required in order to ensure that unauthorized programs are prevented from running.
  - Separate those, who can access the data e.g. data entry and the DBA, from those who can run programs e.g. computer operators. This is required in order to ensure that unauthorized data entry cannot take place.
  - Separate those, who can input data e.g. data entry, from those, who can reconcile or approve data e.g. data authorization persons. This is required in order to ensure that unauthorized data entry cannot take place.
  - Separate those, who can test programs e.g. users, quality assurance and security, from those, who can develop programs e.g. application programmers. This is required in order to ensure that unauthorized programs cannot be allowed to run.
  - Separate those, who can enter errors in a log e.g. data entry operator, who transfer the data to an error log, from those who can correct the errors like the end user departments. This is required in order to ensure that unauthorized data entry cannot take place.
  - Separate those, who can enter data e.g. data entry personnel, from those who can access the database e.g. the DBA. This is required in order to ensure that unauthorized data entry or data modification cannot take place.

3.8.2 Management Controls

- The controls adapted by the management of an enterprise are to ensure that the information systems function correctly and they meet the strategic business objectives.
- The management has the responsibility to determine whether the controls that the enterprise system has put in place are sufficient to ensure that the IT activities are adequately controlled.
- The controls flow from the top of an organization to down; the responsibility still lies with the senior management.

- The controls considerations while reviewing management controls in an IS system shall include:

i). Responsibility –

- ✦ The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.

ii). An IT Organization Structure –

- ✦ There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions.

iii). An IT Steering Committee –

- ✦ The steering committee shall comprise of representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. Here the responsibility lies beyond just the accounting and financial systems; for example, the telecommunications system (phone lines, videoconferencing) office automation, and manufacturing processing systems.

3.8.3 Financial Controls

- These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input.
- These areas exercise control over transactions processing using reports generated by computer applications to reflect un-posted item, non-monetary change, item count & amount of transaction for settlement of transactions processed and reconciliation of applications to general ledger.
- The financial control techniques are numerous and are highlighted here:

1) Authorization –

- ✦ This entails obtaining the authority to perform some act typically accessing to such assets as accounting or application entries.

2) Budgets –

- ✦ These estimates of the amount of time or money expected to be spent during a particular period, project, or event. Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.

3) 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 document.

4) Documentation –

- ✦ This includes written or typed explanations of actions taken on specific transactions.

5) Dual control –

- ✦ This entails having two people simultaneously access an asset. Dual access divides the access function between two people: once access is achieved, only one person handles the asset.

6) 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.

7) **Safekeeping –**
   - ✦ This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.

8) **Sequentially numbered documents –**
   - ✦ These are working documents with preprinted sequential numbers, which enables the detection of missing documents.

9) **Supervisory review –**
   - ✦ This refers to review of specific work by a supervisor but this control requires a sign-off on documents by supervisor, in order to provide evidence that supervisor at least handled them.

3.8.4 BCP (Business Continuity Planning) Controls

- These controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements so as to make sure IT services are available as required and to ensure a minimum impact in event of major disruption.
- The controls include Critical Classification, alternative procedure, Back-up & Recovery, Systematic and Regular Testing and Training, Monitoring and Escalation Processes, Internal and External Organizational Responsibilities, Business Continuity Activation, Fallback and Resumption plans, Risk Management Activities, Assessment of Single Points of Failure and Problem Management.

3.9.5 Operating System Controls

- Operating System is the computer control program. It allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers.
- Operating system performs the following major tasks:

i). Scheduling Jobs –
   - ✦ They can determine the sequence in which jobs are executed, using priorities established.

ii). Managing Hardware and Software Resources –
   - ✦ They can first cause the user's application program to be executed by loading it into primary storage and then cause the various hardware units to perform as specified by the application.

iii). Maintaining System Security –
   - ✦ They may require users to enter a password - a group of characters that identifies users as being authorized to have access to the system.

iv). Enabling Multiple User Resource Sharing –
   - ✦ They can handle the scheduling and execution of the application programs for many users at the same time, a feature called multiprogramming.

v). Handling Interrupts –
   - ✦ An interrupt is a technique used by the operating system to temporarily suspend the processing of one program in order to allow another program to be executed.

vi). Maintaining Usage Records –
   - ✦ They can keep track of the amount of time used by each user for each system unit - the CPU, secondary storage, and input and output devices.

- **Control Objectives –**
  - ✦ Operating Systems being one of most critical software of any computer need to work in a well-controlled environment. Following are the major control objectives:
    - Protect itself from user;
    - Protect user from each other;
    - Protect user from themselves;
    - The operating system must be protected from itself; and
    - The operating system must be protected from its environment.
- **Operating System Security –**
  - ✦ Operating system security involves policy, procedure and controls that determine, 'who can access the operating system,' 'which resources they can access' and 'what action they can take'.
  - ✦ The following security components are found in secure operating system:

    i). Log-in Procedure –
    - A log-in procedure is the first line of defense against unauthorized access.
    - 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, else the system should lock the user from the system.

    ii). 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.

    iii). Access Control List –
    - This list contains information that defines the access privilege for all valid user of 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.

    iv). Discretionary Access Control –
    - The system administrator usually determines; who is granted access to specific resources and maintains the access control list.
- **Remedy from destructive programs –**
  - ✦ The following can be used as remedies from destructive programs like viruses, worms etc.:
    - Purchase software from reputed vendor;
    - Examine all software before implementation;
    - Establish educational program for user awareness;
    - Install all new application on a standalone computer and thoroughly test them;
    - Make back up copy of key file; and
    - Always use updated anti-virus software.

3.8.6 Data Management Controls

- These Controls fall in two categories:
  - ✦ Access Control, and
  - ✦ Backup Control.

1) Access Controls –

- ✦ Access controls are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data.
- ✦ Controls are established in the following manner:
  - **a)** User Access Controls through passwords, tokens and biometric Controls; and
  - **b)** Data Encryption: Keeping the data in database in encrypted form.

2) Back-up Controls –

- ✦ Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its file & database.
- ✦ Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss.
- ✦ Various backup strategies are given as follows:

i). Dual recording of data –

- Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.

ii). Periodic dumping of data –

- This strategy involves taking a periodic dump of all or part of the database.
- The database is saved at a point in time by copying it onto some backup storage medium – magnetic tape, removable disk, Optical disk. The dump may be scheduled.

iii). Logging input transactions –

- This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump.
- In case of complete database failure, the last dump is loaded and reprocessing of the transactions are carried out which were logged since the last dump.

iv). Logging changes to the data –

- This involves copying a record each time it is changed by an update action. The changed record can be logged immediately before the update action changes the record, immediately after, or both.

3.8.7 System Development Controls

- System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process.

- The six activities that deals with system development controls in IT setup are given as follows:

i). 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).

ii). 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.
- ✦ The creation of a user specification document often involves the joint efforts of the user and systems professionals. It should describe the user's view of the problem, not that of the systems professionals.

iii). Technical Design Activities –

- ✦ The technical design activities in the 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.

iv). 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.

v). Program Testing –

- ✦ All program modules must be thoroughly tested before implementation. The results of tests are then compared against predetermined results to identify programming and logic errors.
- ✦ Program testing is time-consuming, the principal task being 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.

vi). 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).

3.8.8 Computer Centre Security and Controls

- These are of the following types:
  - ✦ Physical Security,
  - ✦ Software & Data Security, and
  - ✦ Data Communication Security.

1) Physical Security –

- The security required for computer system can be categorized as security from accidental breach and incidental breach.
- Accidental breach of security due to such natural calamities as fire, flood and earthquake etc. may cause total destruction of important data and information.
- Incidental or fraudulent modification or tampering of financial records maintained by the organization can cause considerable amount of money to be disbursed to fraudulent personnel.
- Physical security includes arrangements for:
  - ✦ Fire detection and fire suppression systems,
  - ✦ Security from water damage,
  - ✦ Safeguards from power variation, and
  - ✦ Pollution and unauthorized intrusion.

  These are discussed as follows:

a) Fire Damage –

- ✦ It is a major threat to the physical security of a computer installation.
- ✦ Some of the major features of a well-designed fire protection system are given below:
  - – Both automatic and manual fire alarms are placed at strategic locations.
  - – A control panel may be installed which shows where in the location an automatic or manual alarm has been triggered.
  - – Master switches may be installed for power and automatic fire suppression system.
  - – Manual fire extinguishers can be placed at strategic locations.
  - – Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station.
  - – All staff members should know how to use the system. The procedures to be followed during an emergency should be properly documented are: Fire Alarms, Extinguishers, Sprinklers, Instructions, Smoke detectors and Carbon dioxide based fire extinguishers.
  - – Less Wood and plastic should be in computer rooms.

b) Water Damage –

- ✦ Water damage to a computer installation can be the outcome of water pipes burst. Water damage may also result from other resources such as cyclones, tornadoes, floods etc.
- ✦ Some of the major ways of protecting the installation against water damage are as follows:
  - – Wherever possible have waterproof ceilings, walls and floors;

- Ensure an adequate positive drainage system exists;
- Install alarms at strategic points within the installation;
- In flood areas have the installation above the upper floors but not at the top floor;
- Use a gas based fire suppression system;
- Water proofing; and
- Water leakage Alarms.

c) Power Supply Variation –

- ✦ Voltage regulator and circuit breaker protect hardware from temporary increase or decrease of power. UPS Battery back-up can be provided in case a temporary loss of power occurs.
- ✦ A generator is needed for sustained losses in power for extended period.

d) Pollution Damage –

- ✦ The major pollutant in a computer is dust. Dust caught between surfaces of magnetic tape and reading/ writing heads may cause either permanent damage to data or read/ write error.
- ✦ Regular cleaning of walls, floors and equipment etc. is essential. Only such materials and finishing may be used inside the room, which enables it to remain dust free. These are:
  - Air conditions,
  - Dust protection, and
  - Regular cleaning.

e) Unauthorized Intrusion –

- ✦ Unauthorized intrusion takes two forms.
  - First, the intruder by physically entering the room may steal assets or carry out sabotage.
  - Alternatively, the intruder may eavesdrop on the installation by wiretapping, installing an electronic bug or using a receiver that picks up electro-magnetic signals.
- ✦ Various devices are available to detect the presence of bugs by the intruder; these are:
  - Physically or Electronically logging,
  - Guard, dogs,
  - Entry in computer area restricted,
  - Log books,
  - Alarms,
  - Preventing wiretapping,
  - Physical Intrusion detectors, and
  - Security of Documents, data & storage media.

2) Software & Data Security –

- Software and Data Security can be implemented through the following controls –
  - ✦ Authorization of persons to use data,
  - ✦ Passwords & PINs,
  - ✦ Monitoring after office hours activity,

- ✦ Segregation, check & control over critical information,
- ✦ Frequent audits,
- ✦ Screening and background checks before recruitment,
- ✦ Encryption of data – Viewing & recognition of data only by PINs & passwords,
- ✦ Security software,
- ✦ Management checks,
- ✦ Back up of data/information, and
- ✦ Antivirus software.

3) Data Communication Security –

- Data Communication Security can be implemented through the following controls:
  - ✦ Audit trails of crucial network activities,
  - ✦ Sign on user identifier,
  - ✦ Passwords to gain access,
  - ✦ Terminal locks,
  - ✦ Sender & receiver authentications,
  - ✦ Check over access from unauthorized terminals,
  - ✦ Encryption of data / information,
  - ✦ Proper network administration,
  - ✦ Hardware & system software built in control,
  - ✦ Use of approved networks protocols,
  - ✦ Network administrations, and
  - ✦ Internally coded device identifier.

3.8.9 Internet and Intranet Controls

- Major exposures in the communication sub-system including Internet & Intranet are as follows:

i). Component Failure –

- ✦ Data may be lost or corrupted through component failure.
- ✦ The primary components in the communication sub-systems are given as follows:
  - Communication lines viz. twisted pair, coaxial cable, fiber optics, microwave & satellite etc.
  - Hardware – ports, modems, multiplexers, switches and concentrators etc.
  - Software – Packet switching software, polling software, data compression software etc.
  - Due to component failure, transmission between sender and receiver may be disrupted, destroyed or corrupted in the communication system.

ii). Subversive Threats –

- ✦ An intruder attempts to violate the integrity of some components in the sub-system.
- ✦ An intruder attempts to violate the integrity of some components in the sub-system by:
  - **Invasive tap**: By installing it on communication line, s/he may read and modify data.
  - **Inductive tap**: It monitors electromagnetic transmissions and allows data to be read only.

- **Denial of Service**: When a user establishes a connection on Internet through TCP/IP, a three way handshake takes place between Synchronize (SYN) packets, SYN ACK packets and ACK packets. Computer hacker transmits hundreds of SYN packets to the receiver but never responds with an ACK to complete the connection. As a result, the ports of the receiver's server are clogged with incomplete communication requests and legitimate requests are prevented from access. This is known as Connection Flooding.

- **Controls for Subversive Threats**

  a) Firewall –

  - A Firewall is a system that enforce access control between two networks. To do this, all traffic between the external network and the organization's Intranet must pass through firewall.
  - The firewall must be immune to penetrate from both outside and inside the organization. In addition to insulating the organization's network from external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access also.

  b) Encryption –

  - Encryption is the conversion of data into a secret code for storage in databases and transmission over networks.
  - Sender uses an encryption algorithm and the original message called clear text is converted into cipher text. This is decrypted at the receiving end. The encryption algorithm uses a key. The more bits in the key, the stronger are the encryption algorithms. Two general approaches are used for encryption viz. private key and public key encryption.

  c) Recording of Transaction Log –

  - An intruder may penetrate system by trying different passwords and user ID combinations.
  - All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.

  d) Call Back Devices –

  - It is based on the principle that the key to network security is to keep the intruder off the Intranet rather than imposing security measure after the criminal has connected to intranet.
  - The call- back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials the caller's number to establish a new connection.
  - This limits access only from authorized terminals and prevents an intruder masquerading as a legitimate user. This also helps to avoid the call forwarding and man-in-the middle attack.

3.8.10 Personal Computers Controls

- Related risks are given as follows:
  - Personal computers are small in size and easy to connect and disconnect, they are likely to be shifted from one location to another or even taken outside organization for theft of information
  - Pen drives can be very conveniently transported from one place to another, as a result of which data theft may occur. Even hard disks can be ported easily these days.

- ✦ Segregation of duty is not possible, owing to limited number of staff.
- ✦ PC is basically a single user oriented machine and hence, does not provide inherent data safeguards. Problems can be caused by computer viruses and pirated software.
- ✦ Due to vast number of installations, the staff mobility is higher and hence becomes a source of leakage of information.
- ✦ The operating staff may not be adequately trained.
- ✦ Weak access control.

- The Security Measures that could be exercised to overcome above risks are given as follows:
  - ✦ Physically locking the system;
  - ✦ Proper logging of equipment shifting must be done;
  - ✦ Centralized purchase of hardware and software;
  - ✦ Standards set for developing, testing and documenting;
  - ✦ Uses of antimalware software;
  - ✦ The use of personal computer and their peripheral must have controls; and
  - ✦ Use of disc locks that prevent unauthorized access to the floppy disk or pen drive of a computer.

3.9 Controls over Data Integrity and Security

- The classification of information and documents is essential if one has to differentiate between that which is of little value, and that which is highly sensitive and confidential.
- For many organizations, a simple 5 scale grade will suffice as follows:

i). Top Secret –

- ✦ Highly sensitive internal information e.g. pending mergers or acquisitions; investment strategies; plans or designs; that could seriously damage the organization if made public.
- ✦ Information classified as Top Secret information has very restricted distribution and must be protected at all times. Security at this level should be the highest possible.

ii). Highly Confidential –

- ✦ Information that, if made public or even shared around the organization, could seriously impede the organization's operations and is considered critical to its ongoing operations.
- ✦ Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants etc.
- ✦ Such information should not be copied or removed from the organization's operational control without specific authority. Security at this level should be very high.

iii). Proprietary –

- ✦ Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates.
- ✦ Such information is used to authorized personnel only. Security at this level should be high.

iv). Internal Use only –

- ✦ Information not approved for general circulation outside organization where its loss would inconvenience the management but where disclosure is unlikely to result in financial loss.

- ✦ Security at this level should controlled but normal.
- ✦ Examples would include, internal memos, minutes of meetings, internal project reports.

v). Public Documents –

- ✦ Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level should minimal.

3.9.1 Data Integrity

- Data integrity is a reflection of the accuracy, correctness, validity, and currency of the data.
- The primary objective of data integrity control techniques is to ensure the integrity of a specific application's inputs, stored data, programs, data transmissions, and outputs.
- Data integrity controls protect data from accidental or malicious alteration or destruction and provide assurance to the user that information meets expectations about its quality and integrity.
- Assessing data integrity involves evaluating the following critical procedures:
  - ✦ Virus detection and elimination software is installed and activated.
  - ✦ Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended.
- An auditor should be concerned with the testing of user-developed systems; changes or the release of data, unknown to the user, could occur because of design flaw.

3.9.2 Data Integrity Policies

Major data integrity policies are given as under:

i). Virus-Signature Updating –

- ✦ Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.

ii). Software Testing –

- ✦ All software must be tested in a suitable test environment before installation on systems.

iii). Division of Environments –

- ✦ The division of environment into Development, Test & Production is required for critical system.

iv). Offsite Backup Storage –

- ✦ Backups older than one month must be sent offsite for permanent storage.

v). Quarter-End and Year-End Backups –

- ✦ Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes.

vi). Disaster Recovery –

- ✦ A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

3.9.3 Data Security

- Data security encompasses the protection of data against accidental or intentional disclosure to unauthorized persons as well as the prevention of unauthorized modification and deletion of data.
- An IS auditor is liable to evaluate the following while reviewing adequacy of data security controls:

- ✦ Who is responsible for the accuracy of the data?
- ✦ Who is permitted to update data?
- ✦ Who is permitted to read and use the data?
- ✦ Who is responsible for determining who can read and update the data?
- ✦ Who controls the security of the data?
- ✦ If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
- ✦ Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
- ✦ The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.

3.10 Cyber Frauds

- Fraud has been defined as "Intentional Error". Cyber Fraud shall mean frauds committed by use of technology. Cyber fraud refers to any type of deliberate deception for unfair or unlawful gain that occurs online. The most common form is online credit card theft.
- One of the major reasons behind the rise of cyber frauds are:

  i). Failure of internal control system,

  ii). Failure of organizations to update themselves to new set of risk, and

  iii). Smart fraudsters: These are people who are able to target the weaknesses in system, lacunae's in internal controls, even before the organization realizes that such gaps are there.
- On the basis of the functionality, these are of two types:

  a) Pure Cyber Frauds –

  - ✦ Frauds, which exists only in cyber world. They are borne out of use of technology. For example: Website hacking.

  b) Cyber Enabled Frauds –

  - ✦ Frauds, which can be committed in physical world also but with use of technology; the size, scale and location of frauds changes. For example: Withdrawal of money from bank account by stealing PIN numbers.

3.10.1 Cyber Attacks

Major cyber-attacks are discussed as follows:

i). Phishing –

- ✦ It is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.
- ✦ Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.

ii). Network Scanning –

- ✦ It is a process to identify active hosts of a system, for purpose of getting information about IP addresses etc.

iii). Virus/Malicious Code –

- As per Section 43 of Information Technology Act, 2000, "Computer Virus" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed in that computer resource;

iv). Spam –

- E-mailing same message to everyone on one or more Usenet News Group is termed as spam.

v). Website Compromise/Malware Propagation –

- It includes website defacements. Hosting malware on websites in an unauthorized manner.

vi). Others –

a) Cracking –

- Crackers are hackers with malicious intentions.

b) Eavesdropping –

- It refers to the listening of the private voice or data transmissions, often using a wiretap.

c) E-mail Forgery –

- Sending e-mail messages that look as if someone else sent it is termed as E-mail forgery.

d) E-mail Threats –

- Sending a threatening message to try and get recipient to do something that would make it possible to defraud him is termed as E-mail threats.

e) Scavenging –

- This is gaining access to confidential information by searching corporate records.

3.11.2 Impact of Cyber Frauds on Enterprises

The impact of cyber frauds on enterprises can be viewed under the following dimensions:

i). Financial Loss –

- Cyber frauds lead to actual cash loss to target company/organization.

ii). Legal Repercussions –

- Entities hit by cyber frauds are caught in legal liabilities to their customers.
- Section 43A of the Information Technology Act, 2000, fixes liability for organizations having secured data of customers. These entities need to ensure that such data is well protected.

iii). Loss of credibility or Competitive Edge –

- News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility.

iv). Disclosure of Confidential, Sensitive or Embarrassing Information –

- Cyber-attack may expose critical information in public domain.

v). Sabotage –

- The above situation may lead to misuse of such information by enemy country.

3.10.3 Techniques to Commit Cyber Frauds

Following are the major techniques to commit cyber frauds:

1. **Hacking –**
   - ✦ It refers to unauthorized access and use of computer systems, by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.
2. **Cracking –**
   - ✦ Crackers are hackers with malicious intentions. Hacking is general term, with two nomenclature namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking.
3. **Data Diddling –**
   - ✦ Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data is referred as data diddling.
4. **Data Leakage –**
   - ✦ It refers to the unauthorized copying of company data such as computer files.
5. **Denial of Service (DoS) Attack –**
   - ✦ It refers to an action or series of actions that prevents access to a system by its authorized users; causes delay of its time-critical operations; or prevents any part of the system from functioning.
6. **Internet Terrorism –**
   - ✦ It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.
7. **Logic Time Bombs –**
   - ✦ These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotage the system by destroying programs, data or both.
8. **Masquerading or Impersonation –**
   - ✦ In this case, perpetrator gains access to the system by pretending to be an authorized user
9. **Password Cracking –**
   - ✦ Intruder penetrates a system's defense, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.
10. **Piggybacking –**
    - ✦ It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
11. **Round Down –**
    - ✦ Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
12. **Scavenging or Dumpster Diving –**
    - ✦ It refers to the gaining access to confidential information by searching corporate records.
13. **Social Engineering Techniques –**
    - ✦ Perpetrator tricks an employee into giving out the information needed to get into the system.
14. **Super Zapping –**
    - ✦ It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.
15. **Trap Door –**
    - ✦ In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.