3

Protection of Information Systems

Learning Objectives
• To understand the need for Protection of Information Systems;
• To know Information Security Policies, Procedures, related Standards and Guidelines;
• To understand the term 'Controls';
• To know about various types of Controls - IT General Controls, Logical Access Controls & Application Controls, Technologies and Security Management Features;
• To discuss the role of technology in Control Monitoring and Segregation of Duties; and
• To discuss Cyber Frauds.
Task Statements
• To understand the need of Information Security;
• To evaluate the Security Policy and its Components;
• To identify the Significant Security Aspects and Organization' need to look into it;
• To perform detailed analysis of the Controls that an Organization has put in place;
• To identify the nature of Controls put in place; and
• To identify the possibilities of Frauds relating to technology.
Knowledge Statements
• To know Information Security and its related concepts;
• To know various components of Information Security Policy;
• To know different controls and their related aspects; and
• To know various frauds that may hamper an organisation due to lack of controls.

3.1 Introduction

In the computerized information systems, most of the business processes are automated. Organizations are increasingly relying on Information Technology (IT) for information and transaction processing. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and generated need for reengineered business processes. IT

innovations such as hardware, software, networking technology, communication technology and ever-increasing bandwidth lead to completely new business models.

All these new business models and new methods assume that the information required by the business managers is available all the time; it is accurate, it is complete and no unauthorized disclosure of the same is made. Further, it is also presumed that the virtual business organization is up and running all the time on 24 × 7 basis. However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to information security threats than ever before. The Denial of Service (DoS) attacks on the websites of yahoo.com, amazon.com and lots of other web sites is a significant case. Those websites were down for several hours to a few days jeopardizing the business of those organizations. The virus threats are also in real. The horror stories of 'Melissa' and 'I love you' viruses are fresh in the minds of the IT professionals of those organizations, which were affected by them. Further, the hacking and cracking on the Internet is a real threat to virtual organizations, which are vulnerable to information theft and manipulations.

3.2 Need for Protection of Information Systems

In a global information society, where information travels through cyberspace on a routine basis, the significance of information is widely accepted. In addition, 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. Organizations depend on timely, accurate, complete, valid, consistent, relevant, and reliable information. Accordingly, executive management has a responsibility to ensure that the organization provides all users with a secure information processing environment.

It is clear from the instances cited above that there are not only many direct and indirect benefits from the use of information systems, there are also many direct and indirect risks relating to the information systems. 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, and regulatory requirements or technological developments.

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, among others, technical conditions (program bugs, disk crashes), natural disasters (fire, flood), environmental conditions (electrical surges), human factors (lack of training, errors, and omissions), unauthorized access (hacking), or viruses. In addition to these, other threats, such as business dependencies (reliance on third party communications carriers, outsourced operations, etc.) can potentially result in a loss of management control and oversight. Adequate measures for information security help to ensure the smooth functioning of information systems and protect the organization from loss or embarrassment caused by security failures.

3.3 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 understood and implemented by most of the organizations. However, security must be expanded to include logical and other technical safeguards such as user identifiers, passwords, firewalls, etc., which is not understood well by many organizations. In organizations, where a security breach has been experienced, the effectiveness of information security policy and procedures has to be reassessed.

This concept of information security applies to all information. In this context, the valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information is protected against harm from threats that will lead to its loss, inaccessibility, alteration, or wrongful disclosure. The protection is achieved through a layered series of technological and non-technological safeguards such as physical security and logical measures.

Information System 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:

- **Confidentiality:** Prevention of the unauthorized disclosure of information;
- **Integrity:** Prevention of the unauthorized modification of information; and
- **Availability:** Prevention of the unauthorized withholding of information.

The relative priority and significance of Confidentiality, Integrity and Availability (CIA) vary according to the data within the information system and the business context in which it is used.

3.3.1 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.

- **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 did the company discover that in all other geographic regions the competition for their product was intense. The result is that the company lost several million, rupees as its product sales faltered.

  Although, it might have been impossible for the company to completely prevent its intentions from being discovered, this situation does illustrate the real value of keeping strategic plans confidential. 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. Industry studies bear witness to this fact.

- **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 the organization. This is the case when one company can provide a service profitably at a lower price than the competitor. A company's client lists and the prices charged for various products and services can also be damaging in the hands of a competitor. While many organizations prohibit the sharing of such data, carelessness often results in its compromise. Such activity includes inadvertent storage of data on unauthorized systems, unprotected laptops, and failure to secure magnetic media.

- **Finances:** Financial information, such as salaries and wages, are very sensitive and should not be made public. While general salary ranges are known within industry, precise salary information can provide a competitive edge. 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. When competitors' costs are lower, they can either under-price the market or increase prices. In either case, the damage to an organization may be significant.

3.4 Information Security Policy

An **Information Security Policy** is the statement of intent by the management about how to protect a company's information assets. It is a formal statement of the rules, which give access to people to an organization's technology and information assets, and which they must abide. In its basic form, a information security policy is a document that describes an organization's information security controls and activities. The policy does not specify

technologies or specific solutions; it defines a specific set of intentions and conditions that help protect a company's information assets and its ability to conduct business.

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.

An information security policy should be in written form. It provides instructions to employees about 'what kinds of behavior or resource usage are required and acceptable', and about 'what is unacceptable'. An Information Security policy also provides direction to all employees about how to protect organization's information assets, and instructions regarding acceptable (and unacceptable) practices and behavior.

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

As policy is in the form of a broad general statement, organizations also develop standards, guidelines, and procedures that offer users, managers and others a clearer approach to implementing policy and meeting organizational goals.

Standards specify technologies and methodologies to be used to secure systems. Guidelines help in smooth implementation of information security policy. Procedures are more detailed steps to be followed to accomplish particular security related tasks. 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. Standardization of organization-wide identification badges is a typical example, providing ease of employee mobility and automation of entry/exit systems. Standards are compulsory within an organization. Guidelines assist users, systems personnel, and others in effectively securing their systems. Guidelines are often used to ensure that specific security measures are not overlooked, although they can be implemented, and correctly so, in more than one way.

Procedures normally 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 (e.g., preparing new user accounts and assigning appropriate privileges). Some organizations issue overall computer security manuals, regulations, handbooks, or similar documents.

An Information Security policy addresses many issues such as confidentiality, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls and who owns the information, and authority issues.

3.4.2 Issues to address

This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the 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 and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- 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. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most of the employees have some responsibilities for information security, and auditors should review any declarations to the contrary with care. The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

3.4.3 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.

Information security policies must always take into account business requirements. Business requirements are the principles and objectives adopted by an 6organization to support its operations and information processing. E-commerce security is an example of such business requirements. Furthermore, policies must consistently take into account the legal, statutory, regulatory and contractual requirements that the 6organization and its professional partners, suppliers and service providers must respect. The respect of intellectual property is a good example of such requirements.

3.4.4 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:

- **User Security Policies** – These include User Security Policy and Acceptable Usage Policy.

- **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.
- **Acceptable Usage Policy –** This sets out the policy for acceptable use of email, Internet services and other IT resources.

♦ **Organization Security Policies** – These include Organizational Information Security Policy, Network & System Security Policy and Information Classification Policy.

- **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. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document.
- **Network & System Security Policy –** This policy sets out detailed policy for system and network security and applies to IT department users.
- **Information Classification Policy –** This policy sets out the policy for the classification of information.

♦ **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.

The hierarchy of these policies is shown in the Fig. 3.4.1.

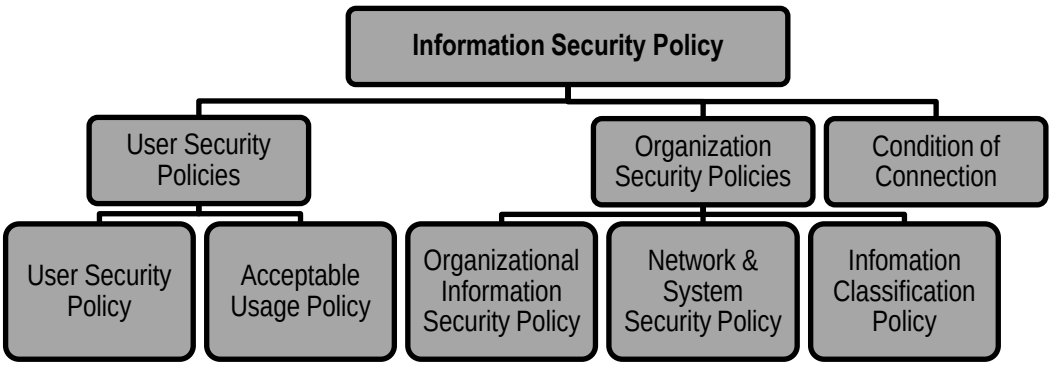

Fig 3.4.1: The Hierarchy of Information Security Policies

3.4.5 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.

3.5 Information Systems Controls

The increasing use of IT in organizations has made it imperative that appropriate information systems are implemented in an organization. IT should cover all key aspects of business processes of an enterprise and should have an impact on its strategic and competitive advantage for its success. The enterprise strategy outlines the approach, it wishes to formulate with relevant policies and procedures to achieve business objectives. 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. This is achieved by designing and effective information control framework, which comprise policies, procedures, practices, and organization structure that gives reasonable assurances that the business objectives will be achieved.

3.5.1 Need for Controls in Information Systems

Technology has impacted what can be done in business in terms of information as a business enabler. It has increased the ability to capture, store, analyze and process tremendous amounts of data and information by empowering the business decision maker. With the advent of affordable hardware, technology has become a critical component of business. IT department may store all financial records centrally. For example, a large multinational company with offices in many locations may store all its computer data in just one centralised data centre. In the past, the financial information would have been spread throughout the organisation in many filing cabinets. If a poorly controlled computer system is compared to a poorly controlled manual system, it would be akin to placing an organisation's financial records on a table in the street and placing a pen and a bottle of correction fluid nearby. Without adequate controls, anyone could look at the records and make amendments, some of which could remain undetected.

Today's dynamic global enterprises need information integrity, reliability and validity for timely flow of accurate information throughout the organization. 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. Safeguarding assets to maintain accurate data readily available and its integrity to achieve system effectiveness and efficiency is a significant control process.

A well designed information system should have controls built in for all its sensitive or critical sections. For example, the general procedure to ensure that adequate safeguards over access to assets and facilities can be translated into an IS-related set of control procedures, covering access safeguards over computer programs, data and any related equipment. 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; Qualify Assurance Procedures; Physical Access Controls; BCP and DRP; Network and Communication; Database Administration; Protective and detective mechanisms against internal/external attacks etc..

3.5.2 Objectives of 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. Thus, an information systems auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.

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. All exposures have causes. 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 as follows:

- 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 the business users and even 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.

3.5.3 Impact of Technology on Internal Controls

These are discussed as follows:

- **Competent and Trustworthy Personnel:** Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often vested in the errors responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations. Unfortunately, ensuring that an organization has competent and trustworthy information systems personnel is a difficult task.
- **Segregation of Duties:** Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions. 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. The irregularities are frauds due to various facts like 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 perpetrate irregularities like rounding down, salami etc.

  In a manual system, during the processing of a transaction, there are split between different people, such that one person does not process a transaction right from start to finish. However, in a computerised system, the critical factors that need to be considered 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 as follows:

  - 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 Information systems use; Data entry; Computer operation; Network management; System administration; Systems development and maintenance; Change management; Security administration, and Security audit.

- **Authorization Procedures:** In manual systems, auditors evaluate the adequacy of procedures for authorization of examining the work of employees. In computer systems, authorization procedures often are embedded within a computer program. For example: In some on-line transaction systems, written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).
- **Adequate Documents and Records:** This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.In a manual system, adequate documents and records are needed to provide an audit trail of activities within the system. In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions. Thus, no visible audit or management trail would be available tot trance the transactions in a computerized system. However, if the controls over the protection and storage of documents, transaction details, and audit trails etc. are placed properly, it will not be a problem for auditor.
- **Physical Control over Assets and Records:** Physical control over access and records is critical in both manual systems and computer systems. In the manual systems, protection from unauthorised access was through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs can all be maintained at a single site – namely the site where the computer is located. This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster. The nature and types of control available have changed to address these new risks.
- **Adequate Management Supervision:** This refers to review of specific work by a supervisor but this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them. This is an extremely difficult control to test after the fact because the auditor cannot judge the quality of the review unless he or she witnesses it, and, even then, the auditor cannot attest to what the supervisor did when the auditor was not watching.In a manual system, management supervision of employee activities is relatively straightforward as the managers and the employees are often at the same physical location. In computer system, however, data communication facilities can be used to enable employees to be closer to the customers they service. Thus supervision of employees might have to be carried our remotely. The Management's supervision and review helps to deter and detect both errors and fraud.
- **Independent Checks on Performance:** In manual systems, independent checks are carried out because employees are likely to forget procedures, make genuine mistakes, become careless, or intentionally fail to follow prescribed procedures. 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.

- **Comparing Recorded Accountability with Assets:** Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred. In a manual system, independent staff prepares the basic data used for comparison purposes. In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies o the data being prepared for comparison purposes.
- **Delegation of Authority and Responsibility:** A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users. Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

3.6 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. These categories have been represented in the Fig. 3.6.1:

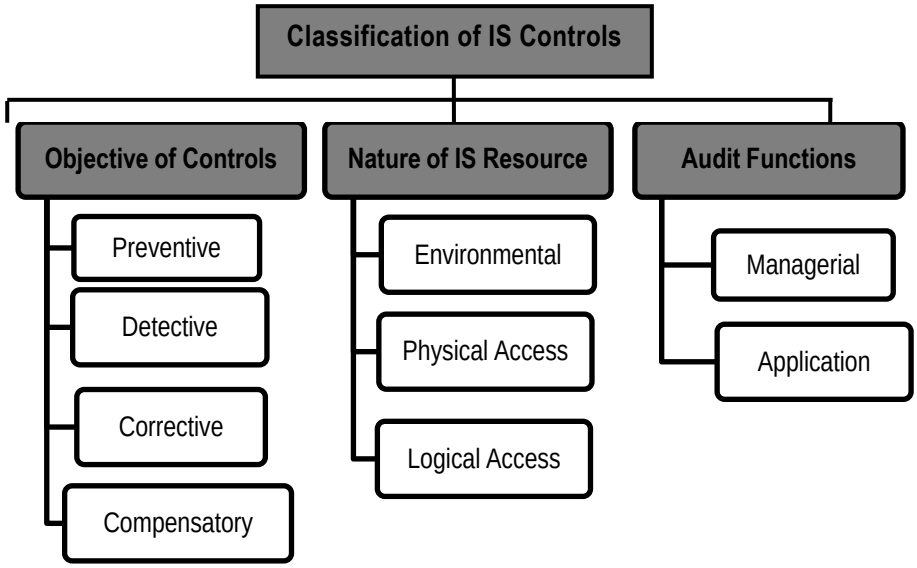

Fig. 3.6.1: Categories of Controls

3.6.1 Classification on the basis of "Objective of Controls"

The controls according to the time that they act, relative to a security incident can be classified as under:

(A) Preventive Controls: Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control

is the use of passwords to gain access to a financial system. The broad characteristics of preventive controls are as follows:

- A clear-cut understanding about the vulnerabilities of the asset;
- Understanding probable threats; and
- Provision of necessary controls for probable threats from materializing.

As discussed earlier, any control can be implemented in both manual and computerized environment for the same purpose. Only, the implementation methodology may differ from one environment to the other. Some of the examples of preventive controls can be Employing qualified personnel; Segregation of duties; Access control; Vaccination against diseases; Documentation; Prescribing appropriate books for a course; Training and retraining of staff; Authorization of transaction; Validation, edit checks in the application; Firewalls; Anti-virus software (sometimes this acts like a corrective control also), etc., and Passwords. The above list contains both of manual and computerized, preventive controls. The following Table 3.6.1 shows how the same purpose is achieved by using manual and computerized controls.

Table 3.6.1: Preventive Controls

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

(B) Detective Controls: These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend. The main characteristics of such 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 the appropriate person or group;
- 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.

(C) Corrective Controls: Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the 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.

Some of the Corrective Controls may be Contingency planning; Backup procedure; Rerun procedures; Change input value to an application system; and Investigate budget variance and report violations.

(D) 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."** Sometimes, while designing and implementing controls, organizations because of different constraints like financial, administrative or operational, may not be able to implement appropriate controls. In such a scenario, 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.

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

These are given as follows:

(A) Environmental Controls: These are the controls relating to IT environment such as power, air-conditioning, Un-interrupted Power Supply (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. However, with proper controls, exposures can be reduced. 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. Water damage is a risk, usually from broken water pipes, and Bomb threat/attack.

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):

- **Hardware and Media:** This includes Computing Equipment, Communication equipment, and Storage Media.
- **Information Systems Supporting Infrastructure or Facilities:** This typically includes 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).
- **Documentation:** Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.
- **Supplies:** The third party maintenance procedures viz. air-conditioning, fire safety, and civil contractors whose entry and assess with respect to their scope of work assigned are to be monitored and logged.
- **People:** The employees, contract 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). Training of employees and other stake holders on control procedures is a critical component.

(ii) Controls for Environmental Exposures

The Table 3.6.2 enlists all the environmental exposure and their controls.

Table 3.6.2: Controls for Environmental Exposures

Environmental Exposures	Controls for Environmental Exposures
Fire Damage It is a major threat to the physical security of a computer installation.	Some of the major ways of protecting the installation against fire damage are as follows: o Both automatic and manual fire alarms may be placed at strategic locations and a control panel may be installed to clearly indicate this. o Besides the control panel, master switches may be

	installed for power and automatic fire suppression system. Different fire suppression techniques like Dry-pipe sprinkling systems, water based systems, halon etc., depending upon the situation, may be used. o Manual fire extinguishers can be placed at strategic locations. o Fireproof Walls; Floors and Ceilings surrounding the Computer Room and Fire Resistant Office Materials such as wastebaskets, curtains, desks, and cabinets should be used. o Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station. o 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 / Fire Brigade Nos., Smoke detectors, and Carbon dioxide based fire extinguishers. o Less Wood and plastic should be in computer rooms. o Use a gas based fire suppression system; o To reduce the risk of firing, the location of the computer room should be strategically planned and should not be located in the basement or ground floor of a multi-storey building. o Regular Inspection by Fire Department should be conducted. o Fire repression systems should be supplemented and not replaced by smoke detectors. o **Smoke Detectors:** Smoke detectors are positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station (for example, a fire station). o **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. This conduit generally lies under the fire-resistant raised floor in the computer room.
Power Spikes This is caused due	Some of the major ways of protecting the installation against power spikes as follows: o The risk of damage due to power spikes can be reduced

to a very short pulse of energy in a power line.	to a great extent using Electrical Surge Protectors that are typically built into the Uninterruptible Power System (UPS). o **Uninterruptible Power System (UPS)/Generator:** In case of a power failure, the UPS provides the back up by providing electrical power from the battery to the computer for a certain span of time. Depending on the sophistication of the UPS, electrical power supply could continue to flow for days or for just a few minutes to permit an orderly computer shutdown. o **Power Supply Variation:** Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power. o **Emergency Power-Off Switch:** When the need arises for an immediate power shut down during situations like a computer room fire or an emergency evacuation, an emergency power-off switch at the strategic locations would serve the purpose. They should be easily accessible and yet secured from unauthorized people.
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.	o **Water Detectors:** These should be placed under the raised floor, near drain holes and near any unattended equipment storage facilities. o **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. Studies reveal that the computer room located in the top floors is less prone to the risk of fire, smoke and water. o Some of the other 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; • Water proofing; and • Water leakage Alarms.

Pollution Damage and others	o The major pollutant in a computer installation is dust. Dust caught between the surfaces of magnetic tape / disk and the reading and writing heads may cause either permanent damage to data or read/ write errors. o **Documented and Tested Emergency Evacuation Plans:** Relocation plans should emphasize human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation. In all circumstances saving human life should be given paramount importance. o **Power Leads from Two Substations:** Electrical power lines that are exposed to many environmental dangers such as water, fire, lightning, cutting due to careless digging etc. To avoid these types of events, redundant power links should feed into the facility. Interruption of one power supply does not adversely affect electrical supply. o **Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility:** These activities should be prohibited from the information processing facility. This prohibition should be clear, e.g. a sign on the entry door.

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

These controls are personnel; hardware and software related and include procedures exercised on access to IT resources by employees/outsiders. These controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy.

These Physical security and access controls should address supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to authorized individuals where IT resources are located in public areas, they should be appropriately protected to prevent or deter loss or damage from theft or vandalism. Further, IT management should ensure zero visibility.

This section enumerates the losses that are incurred as result of perpetrations, accidental or intentional violation of access paths. In addition, the section emphasizes on physical access issues and exposures along with appropriate physical access controls. Afterwards, various access control mechanisms are also discussed.

(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 (an act of dishonestly withholding assets for the purpose of conversion (theft) of such assets, by one or more persons to whom the assets were entrusted, either to be held or to be used for specific purposes);
- Damage, vandalism or theft to equipments or documents;
- Public disclosure of sensitive information; and
- Unauthorized entry.

(a) Possible perpetrators: Perpetrations may be because of employees, who are:

- o Accidental ignorant-someone who outrageously violates rules;
- o Addicted to a substance or gambling;
- o Discontented;
- o Experiencing financial or emotional problems;
- o Former employee;
- o Interested or informed outsiders, such as competitors, thieves, organized crime and hackers;
- o Notified for their termination;
- o On strike; and
- o Threatened by disciplinary action or dismissal.

Exposures to confidential matters may be in form the unaware, accidental or anonymous persons, although the greatest impact may be from those with malicious intent. Other areas of concern include the following:

- o How far the hardware facilities are controlled to reduce the risk of unauthorized access?
- o Are the hardware facilities protected against forced entry?
- o Are intelligent computer terminals locked or otherwise secured to prevent illegal removal of physical components like boards, chips and the computer itself?
- o 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 - Communication channels; Computer room; Control units and front-end processors; Dedicated telephones/telephone lines; Disposal sites; Input/Output devices; Local area networks; Micro computers 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 equipments.

Apart from the computer facility provided, there must be vulnerable access points within the organization, organizational restrictions, and external organization to ensure the effectiveness of the above-mentioned safeguards. Additionally, the IS Auditor has to confirm whether similar controls exist within service providers or other third parties.

(ii) Controls for Physical Access Exposures

Physical access controls are designed to protect the organization from unauthorized access or in other words, to prevent illegal entry. These controls should be designed in such a way that it allows access only to authorized persons. 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:

- **Cipher locks (Combination Door Locks)** - Cipher locks are used in low security situations or when a large number of entrances and exits must be usable all the time. To enter, a person presses a four digit number, and the door will unlock for a predetermined period of time, usually ten to thirty seconds.
- **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.
- **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.

The following are the advantages of electronic door locks over bolting and 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 and sensor devices. Restrictions can be assigned to particular doors or to particular hours of the day.
- Degree of duplication is reduced.

- Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen. If unauthorized entry is attempted silent or audible alarms can be automatically activated.
- An administrative process, which may deal with Issuing, accounting for and retrieving the card keys, are also parts of security. The card key becomes an important item to retrieve when an employee leaves the firm.
- 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 instances when extremely sensitive facilities must be protected, such as in the military.

(b) Physical Identification Medium: These are discussed below:

- **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. The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication. His/her entry will be matched with the PIN number available in the security database.
- **Plastic Cards:** These cards are used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands.
- **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. Sophisticated photo IDs can also be utilized as electronic card keys.

(c) Logging on Facilities: These are given as under:

- **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.
- **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:

- **Video Cameras:** Cameras should be placed at specific locations and monitored by security guards. Refined video cameras can be activated by motion. The video supervision recording must be retained for possible future play back.

- **Security Guards:** Extra security can be provided by appointing guards aided with CCTV feeds. Guards supplied by an external agency should be made to sign a bond to protect the organization from loss.
- **Controlled Visitor Access:** A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.
- **Bonded Personnel:** All service contract personnel, such as cleaning people and off-site storage services, should be asked to sign a bond. This may not be a measure to improve physical security but to a certain extent can limit the financial exposure of the organization.
- **Dead Man Doors:** These systems encompass a pair of doors that are typically 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.
- **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. Only the general location of the information processing facility should be identifiable.
- **Computer Terminal Locks:** These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.
- **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 the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.
- **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. Security personnel should be able to hear the alarm when activated.
- **Perimeter Fencing:** Fencing at boundary of the facility may also enhance the security mechanism.
- **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 the concerned officials frequently
- **Secured Report/Document Distribution Cart:** Secured carts, such as mail carts, must be covered and locked and should always be attended.

(C) Logical Access Controls: These are the controls relating to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc.

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. The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorization, authentication and incident handling, reporting and follow-up, virus prevention and detection, firewalls, centralized security administration, user training and tools for monitoring compliance, intrusion testing and reporting.

Logical access controls are the 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.

(i) Logical Access Paths

These are given as follows:

(a) 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 the 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.

(b) 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 (the one that the telecommunication device uses). 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. A dial back line ensures security by confirming the presence and exactness of the data sent.

(c) 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 (i.e., dedicated to one user) or public, security is provided in the same manner as it is applied to online terminals.

Each of these routes has to be subjected to appropriate means of security in order to secure it from the possible logical access exposures.

(ii) Logical Access Issues and Exposures

Controls that reduce the risk of misuse (intentional or unintentional), theft, alteration or destruction should be used to protect unauthorized and unnecessary access to computer files. Restricting and monitoring computer operator activities in a batch-processing environment provide this control. The opportunities of access in an online system, is more; hence, the level of control for this system must be more complex, as shown in Fig. 3.6.2.

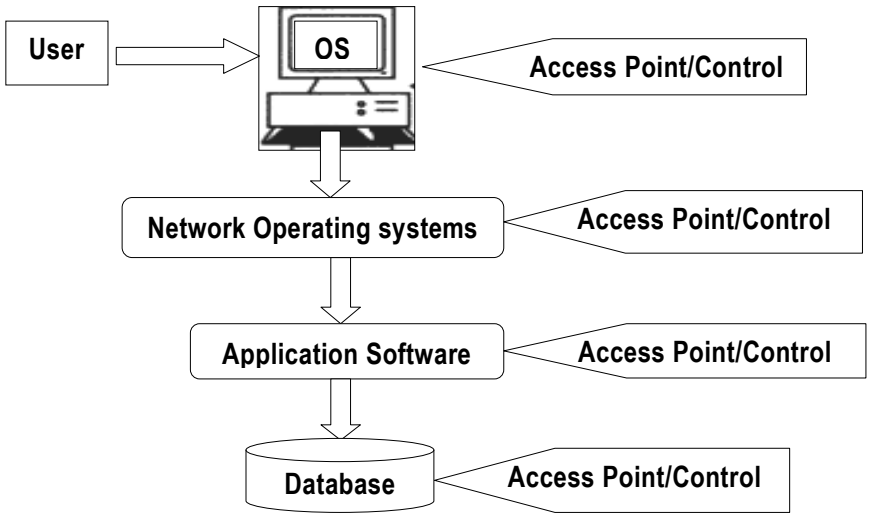

Fig. 3.6.2: Logical Access Paths in an Enterprise Information System

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 applications like - 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. These utilities should be properly secured to assure security to data.

(iii) Issues and Revelations related to Logical Access

Compromise or absence of logical access controls in the organizations may result in potential losses due to exposures that may lead to the total shutdown of the computer functions. 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:

- **Data Diddling:** Data diddling involves the change of data before or after they are entered into the system. A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect the data.
- **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. Since, these programs do not circulate by infecting other programs; chances of a widespread epidemic are relatively low.
- **Trojan Horse:** These are malicious programs that are hidden under any authorized program. Typically, a Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action. The concept of Trojan is similar to bombs but a computer clock or particular circumstances do not necessarily activate it. 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 Trojan 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 as expected, 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.
- **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. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive. Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.

- **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.
- **Salami Techniques:** This involves slicing of small amounts of money from a computerized transaction or account. A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted. For example, in the rounding off technique, ₹ 21,23,456.39 becomes ₹ 21,23,456.40, while in the Salami technique the transaction amount ₹ 21,23,456.39 is truncated to either ₹ 21,23,456.30 or ₹ 21,23,456.00, depending on the logic.
- **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: Computers can be utilized both constructively and destructively. Computer systems are used to steal money, goods, software or corporate information. Crimes are also committed when false data or unauthorized transaction is made. Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organization. Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations. These are given as follows:

- **Financial Loss:** Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.
- **Legal Repercussions:** An organization has to adhere to many laws while developing security policies and procedures. These laws protect both the perpetrator and organization from trial. The organizations will be exposed to lawsuits from investors and insurers if there have no proper security measures. The IS auditor should take legal counsel while reviewing the issues associated with computer security.
- **Loss of Credibility or Competitive Edge:** In order to maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs credibility and public trust. This credibility will be shattered resulting in loss of business and prestige if security violation occurs.
- **Blackmail/Industrial Espionage:** By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.

- **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.
- **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. They do it because of their dislike towards the organization or for their intemperance.
- **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. For example, a penetrator duplicates the login procedure, captures the user's password, attempts for a system crash and makes the user login again.

(c) Asynchronous Attacks: They occur in many environments where data can be moved asynchronously across telecommunication lines. 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:

- **Data Leakage:** Data is a critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.
- **Subversive Threats:** An intruder attempts to violate the integrity of some components in the sub-system. Subversive attacks can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages in many ways. 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 the data to be read only.
- **Wire-tapping:** This involves spying on information being transmitted over telecommunication network as shown in the Fig. 3.6.3.

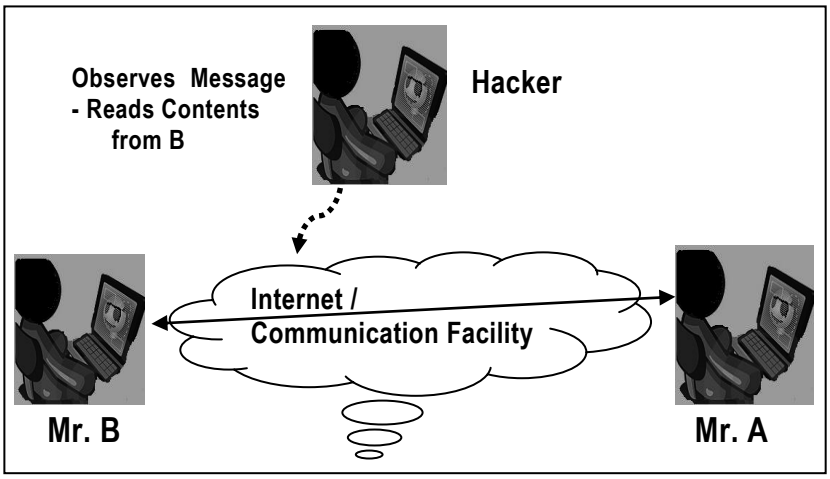

Fig. 3.6.3: Wire Tapping

- **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 he user and modifying them or substituting new messages. A special terminal is tapped into the communication for this purpose as shown in the Fig. 3.6.4.

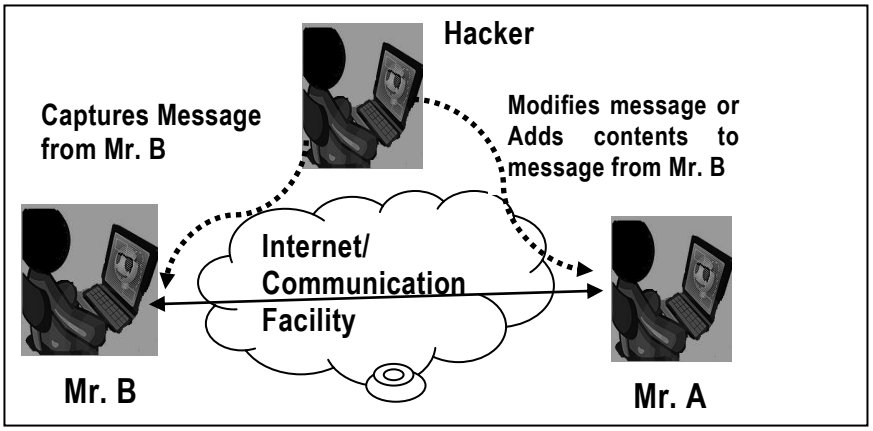

Fig. 3.6.4: Piggybacking

- **Shutting Down of the Computer/Denial of Service:** This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer. When a user establishes a connection on the Internet through TCP/IP, a three way handshake takes place between Synchronize (SYN) packets, SYN ACK (Acknowledgement) 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. 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, as shown in the Fig. 3.6.4.

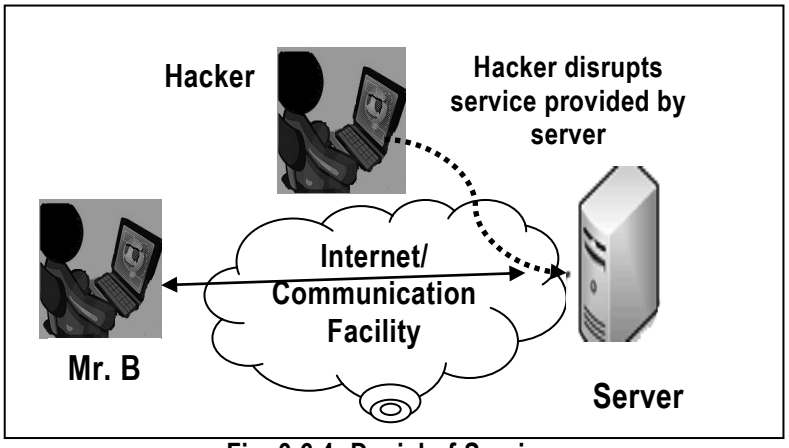

Fig. 3.6.4: Denial of Service

(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 appropriately.
- 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. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.
- When replicated copies of files exist at multiple locations it must be ensured that all are identical copies contain the same information and checks are also done to ensure that duplicate data does not exist.

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: Hackers try their best to overcome restrictions to prove their ability. Ethical hackers most likely never try to misuse the computer intentionally;
- Employees (authorized or unauthorized);
- IS Personnel: They have easiest to access to computerized information since they come across to information during discharging their duties. Segregation of duties and supervision help to reduce the logical access violations;
- Former Employees: should be cautious of former employees who have left the organization on unfavorable terms;
- End Users; Interested or Educated Outsiders; Competitors; Foreigners; Organized Criminals; Crackers; Part-time and Temporary Personnel; Vendors and consultants; and Accidental Ignorant – Violation done unknowingly.

(iv) Logical Access Control across the System

Logical access controls serve as one of the means of information security. 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. It means that the access should not be so restrictive that it makes the performance of business functions difficult or it should not be so liberal that it can be misused i.e. it should be just sufficient for one to perform one's duty without any problem or restraint. 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).

Logical access controls is all about protection of these assets wherever they reside. The details are given in the following Table 3.6.2:

Table 3.6.2: Logical Access Controls

User Access Management	**User Registration** Information about every user is documented. The following questions are to be answered: Why is the user granted the access?, Has the data owner approved the access?, and Has the user accepted the responsibility? etc. The de-registration process is also equally important.

	Privilege management Access privileges are to be aligned with job requirements and responsibilities. For example, an operator at the order counter shall have direct access to order processing activity of the application system. S/he will be provided higher access privileges than others. However, misuse of such privileges could endanger the organization's information security. These privileges are to be minimal with respect to their job functions. **User password management** Passwords are usually the default screening point for access to systems. Allocations, storage, revocation, and reissue of password are password management functions. Educating users is a critical component about passwords, and making them responsible for their password. **Review of user access rights** A user's need for accessing information changes with time and requires a periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.
User Responsibilities	User awareness and responsibility is also an important factor: **Password use** Mandatory use of strong passwords to maintain confidentiality. **Unattended user equipment** Users should ensure that none of the equipment under their responsibility is ever left unprotected. They should also secure their PCs with a password, and should not leave it accessible to others.
Network Access Control	An Internet connection exposes an organization to the entire world. This brings up the issue of benefits the organization should derive along with the precaution against harmful elements. This can be achieved through the following means: **Policy on use of network services** An enterprise wide policy applicable to internet service requirements aligned with the business need for using the Internet services is the first step. Selection of appropriate services and approval to access them should be part of this policy. **Enforced path** Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; e.g., internet access by employees will be routed through a firewall and proxy. **Segregation of networks** Based on the sensitive information handling function; say a VPN

	connection between a branch office and the head-office, this network is to be isolated from the internet usage service **Network connection and routing control** The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility. **Security of network services** The techniques of authentication and authorization policy should be implemented across the organization's network. **Firewall** Organizations connected to the Internet and Intranet often implements an electronic firewall to insulate their network from intrude. A Firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the external network and the organization's Intranet must pass through the firewall. Only authorized traffic between the organization and the outside is allowed to pass through the 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. **Encryption** Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm and the original message called the 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. **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 the 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 or telephone numbers and prevents an intruder masquerading as a legitimate user. This also helps to avoid the call forwarding and man-in-the middle attack. **Recording of Transaction Log:** An intruder may penetrate the

	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.
Operating System Access Control	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. Major tasks of O/S are Scheduling Jobs; Managing Hardware and Software Resources; Maintaining System Security; Enabling Multiple User Resource Sharing; Handling Interrupts and Maintaining Usage Records. 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'. Operating system provides the platform for an application to use various IS resources and perform the specific business function. If an intruder is able to bypass the network perimeter security controls, the operating system is the last barrier to be conquered for unlimited access to all the resources. The major control objectives are to protect itself from user; protect user from each other; protect user from themselves; protect the operating system from itself; and to protect it from its environment. Hence, protecting operating system access is extremely crucial. **Automated terminal identification** This will help to ensure that a particular session could only be initiated from a particular location or computer terminal. **Terminal log-in procedures** A log-in procedure is the first line of defense against unauthorized access. The log-in procedure does not provide unnecessary help or information, which could be misused by an intruder. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorized. If password or user-id is entered incorrectly, then after a specified number of wrong attempts, the system should lock the user from the system. **Access Token** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to

	the user. The information in the access token is used to approve all actions attempted by the user during the session. **Access Control List** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access. **Discretionary Access Control** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, in distributed systems, resources may be controlled by the end-user. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger. **User identification and authentication** The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed. **Password management system** An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users. **Use of system utilities** System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged. **Duress alarm to safeguard users** If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities. **Terminal time out** Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user. **Limitation of connection time** Define the available time slot. Do not allow any transaction

	beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m. - or on a Saturday or Sunday.
Application and Monitoring System Access Control	**Information access restriction** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user is allowed to access only to those items, s/he is authorized to access. Controls are implemented on the access rights of users, For example, read, write, delete, and execute. And ensure that sensitive output is sent only to authorized terminals and locations. **Sensitive system isolation** Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment. Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities. **Event logging** In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly. An intruder may penetrate the 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. **Monitor system use** Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs. **Clock synchronization** Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.
Mobile Computing	In today's organizations, computing facility is not restricted to a particular data centre alone. Ease of access on the move provides efficiency and results in additional responsibility on the management to maintain information security.

	Mobile Computing Theft of data carried on the disk drives of portable computers is a high risk factor. Both physical and logical access to these systems is critical. Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features.

3.6.3 Classification on the basis of "Audit Functions"

Auditors might choose to factor systems in several different ways. Auditors have found two ways to be especially useful when conducting information systems audits. These are discussed below:

(A) Managerial Controls: In this part, 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-to-day basis as discussed in Table 3.6.3.

Table 3.6.3: Types of Management Subsystem and their description

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.
Systems Development Management	Systems Development Management is responsible for the design, implementation, and maintenance of application systems.
Programming Management	It is responsible for programming new system; maintain old systems and providing general systems support software.
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 systems development; implementation, operation, and maintenance conform to established quality standards.
Security	It is responsible for access controls and physical security over the

Administration	information systems function.
Operations Management	It is responsible for planning and control of the day-to-day operations of information systems.

(B) 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. The specific controls could include form design, source document controls, input, processing and output controls, media identification, movement and library management, data back-up and recovery, authentication and integrity, legal and regulatory requirements. Any function or activity that works to ensure the processing accuracy of the application can be considered an application control. Necessary controls belonging to this category are discussed in separate headings.

The categories of Application controls are listed below in the Table 3.6.4.

Table 3.6.4: Types of Application Subsystem and their description

Application Subsystem	Description of Subsystem
Boundary	Comprises the components that establish the interface between the user and the 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 the components that define, add, access, modify, and delete data in the system.
Output	Comprises the components that retrieve and present data to users of the system.

We shall study Managerial and Application Controls in detail now.

3.7 Managerial Controls and their Categories

In this part, we shall examine controls over the managerial functions 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-to-day basis.

3.7.1 Top Management and Information Systems 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 scope of control here includes framing high level IT policies, procedures and standards on a holistic view and in establishing a sound internal controls framework within the organization. The high level policies establish a framework on which the controls for lower hierarchy of the enterprise. The controls flow from the top of an organization to down; the responsibility still lies with the senior management. ***Top management is responsible for preparing a master plan for the information systems function.*** The senior managers who take responsibility for IS function in an organization face many challenges. The major functions that a senior manager must perform are as follows:

(a) Planning – This includes determining the goals of the information systems function and the means of achieving these goals.

- ***Preparing the plan:*** ***This involves the following tasks:***
  - ***Recognizing opportunities and problems that confront the organization in which Information technology and Information systems can be applied cost effectively;***
  - ***Identifying the resources needed to provide the required information technology and information systems; and***
  - ***Formulating strategies and tactics for acquiring the needed resources.***
- ***Types of Plans:*** Top management must prepare two types of information systems plans for the information systems function: a **Strategic plan** and an **Operational plan**. 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.
  - ***Strategic Plan: The Strategic Plan is the long-run plan covering, say, the next three to five years of operations;***
  - ***Operation Plan: It is the short-plan covering, say, next one to three years of operations.***
- ***Role of a 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. ***The ultimate responsibility for information systems planning should be vested in an information systems steering committee. The steering committee should assume overall responsibility for the activities of the information systems function.*** Here the responsibility lies beyond just the accounting and financial systems; for example,

the telecommunications system (phone lines, video-conferencing) office automation, and manufacturing processing systems.

(b) Organizing – There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions.This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during Planning function.

- ***Resourcing the Information Systems Function: A major responsibility of top management is to acquire the resources needed to accomplish the goals and objectives set out in the information systems plan. These resources include hardware, software, personnel, finances and facilities. Adequate funding should be provided to support the acquisition and development of resources when and where they are needed. Further, Auditors should question whether top managers have a good understanding of the role the information systems function should play in their organization.***
- ***Staffing the Information systems Function: Staffing the Information systems function involves three major activities - Acquisition of information systems personnel, Development of information systems personnel; and Termination of information systems personnel.***

(c) Leading – This includes motivating, guiding, and communicating with personnel. ***The purpose of leading is to achieve the harmony of objectives; i.e. a person's or group's objectives must not conflict with the organization's objectives. The process of leading requires managers to motivate subordinates, direct them and communicate with them.***

- ***Motivating and Leading Information Systems Personnel: Though many theories exist, however there is no one best way of motivating and guiding all people and thus the strategies for motivating/leading people need to change depending upon particular characteristics of an individual person and his/her environment.***
- ***Communicating with IS Personnel: Effective communications are also essential to promoting good relationships and a sense of trust among work colleagues. For example - Due to failure in understanding the directions given by the top management, a serious error is made in the system design; the effect of which is for long-term.***

(d) Controlling – This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed. ***This involves determining when the actual activities of the information system's functions deviate from the planned activities.***

- ***Overall Control of IS function: When top managers seek to exercise overall control of the information systems function, two questions arise:***

- ***How much the organization should be spending on the information systems function?***
- ***Is the organization getting value for the money from its information systems function?***

- ***Control of Information System Activities: Top managers should seek to control the activities on the basis of Policies and Procedures; where Policies provide broad, general guidelines for behavior whereas Standards provide specific guidelines for behavior. New and existing staff must be made aware of the policies and procedures that govern their work.***
- ***Control over Information System Services: For each service level, estimates must be made of the expected benefits and resource consumption and finally the review committee must establish priorities.***

3.7.2 Systems Development Management Controls

Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems. System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process. It includes controls at controlling new system development activities. The six activities discussed below deal with system development controls in IT setup. These are given as follows:

- **System Authorization Activities:** All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, system's authorization should be formal. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.
- **User Specification Activities:** Users must be actively involved in the systems development process. User involvement should not be ignored because of a high degree of technical complexity in the system. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals. However, it is most important that this document remains a statement of user needs. It should describe the user's view of the problem, not that of the systems professionals.
- **Technical Design Activities:** The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design. The adequacy of these activities is measured by the quality of the documentation that emerges from each phase. Documentation is both a control and evidence of control and is critical to the system's long term success.

- **Internal Auditor's Participation:** The internal auditor plays an important role in the control of systems development activities, particularly in organizations whose users lack technical expertise. The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. Auditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.
- **Program Testing:** All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors. Program testing is time-consuming, the principal task being the creation of meaningful test data. To facilitate the efficient implementation of audit objectives, test data prepared during the implementation phase must be preserved for future use. This will give the auditor a frame of reference for designing and evaluating future audit tests. For example, if a program has undergone no maintenance changes since its implementation, the test results from the audit should be identical to the original test results. Having a basis for comparison, the auditor can thus quickly verify the integrity of the program code. On the other hand, if changes have occurred, the original test data can provide evidence regarding these changes. The auditor can thus focus attention upon those areas.
- **User Test and Acceptance Procedures:** Just before implementation, the individual modules of the system must be tested as a unified whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s). The formal test and acceptance of the system should consider being the most important control over the SDLC. It is imperative that user acceptance be documented. Before implementation, this is the last point at which the user can determine the system's adequacy and acceptability. Although discovering a major flaw at this juncture is costly, discovering the flaw during the production operations may be devastating.

3.7.3 Programming Management Controls

Program development and implementation is a major phase within the systems development life cycle. The primary objectives of this phase are to produce or acquire and to implement high-quality programs. The program development life cycle comprises six major phases – Planning; Design; Control; Coding; Testing; and Operation and Maintenance with Control phase running in parallel for all other phases as shown in the Table 3.7.1. The purpose of the control phase during software development or acquisition is to monitor progress against plan and to ensure software released for production use is authentic, accurate, and complete.

Table 3.7.1: Phases of Program Development Life Cycle

Phase	Controls
Planning	Techniques like Work Breakdown Structures (WBS), Gantt charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.

Control	***The Control phase has two major purposes:*** • ***Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations.*** • ***Control over software development, acquisition, and implantation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete.***
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	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. These tests are to ensure that a developed or acquired program achieves its specified requirements.
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 are as follows: • **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.

3.7.4 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. Further it must be possible to modify data fairly easily and the integrity of the data be preserved. If data repository system is used properly, it can enhance data and application system reliability. It must be controlled carefully, however, 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.

The control activities involved in maintaining the integrity of the database is as under:

(a) Definition Controls: These controls are placed to ensure that the database always corresponds and comply with its definition standards.

(b) Existence/Backup Controls: These ensure the existence of the database by establishing backup and recovery procedures. 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. 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 files and databases. Various backup strategies are given as follows:

- **Dual recording of data***:* Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.
- **Periodic dumping of data**: This strategy involves taking a periodic dump of all or part of the database onto some backup storage medium – magnetic tape, removable disk, Optical disk etc. The dump may be scheduled.
- **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.
- **Logging changes to the data***:* This involves copying a record each time it is changed by an update action.

(c) 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:

- User Access Controls through passwords, tokens and biometric Controls; and
- Data Encryption: Keeping the data in database in encrypted form.

(d) Update Controls: These controls restrict update of the database to authorized users in two ways:

- ***By permitting only addition of data to the database; and***
- ***Allowing users to change or delete existing data.***

(e) Concurrency Controls: These controls provide solutions, agreed-upon schedules and strategies to overcome the data integrity problems that may arise when two update processes access the same data item at the same time.

(f) Quality Controls: These controls ensure the accuracy, completeness, and consistency of data maintained in the database. This may include traditional measures such as program validation of input data and batch controls over data in transit through the organization.

3.7.5 Quality Assurance Management Controls

Quality Assurance management is concerned with ensuring that the –

- ***Information systems produced by the information systems function achieve certain quality goals; and***
- ***Development, implementation, operation and maintenance of Information systems comply with a set of quality standards.***

The reasons for the emergence of Quality assurance in many organizations are as follows:

- ***Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software they employ to undertake their work.***
- ***Organizations are undertaking more ambitious projects when they build software.***
- ***Users are becoming more demanding in terms of their expectations about the quality of software they employ to undertake their work,***
- ***Organizations are becoming more concerned about their liabilities if they produce and sell defective software.***
- ***Poor quality control over the production, implementation, operation, and maintenance of software can be costly in terms of missed deadlines, dissatisfied users and customer, lower morale among IS staff, higher maintenance and strategic projects that must be abandoned.***
- ***Improving the quality of Information Systems is a part of a worldwide trend among organizations to improve the quality of the goods and services they sell.***

Quality Assurance (QA) personnel should work to improve the quality of information systems produced, implemented, operated, and maintained in an organization. They perform a monitoring role for management to ensure that –

- ***Quality goals are established and understood clearly by all stakeholders; and***
- ***Compliance occurs with the standards that are in place to attain quality information systems.***

3.7.6 Security Management Controls

Information security administrators are responsible for ensuring that information systems assets ***categorized under Personnel, Hardware, Facilities, Documentation, Supplies Data, Application Software and System Software*** are secure. Assets are secure when the expected losses that will occur over some time, are at an acceptable level. ***The control's classification on the basis of "Nature of Information System Resources – Environmental Controls, Physical Controls and Logical Access Controls (discussed under Section 3.6.2)" are all security measures against the possible threats.***

Threat Identification: A threat is some action or event that can lead to a loss. During the threat-identification phase, security administrators attempt to flesh out all material threats that can eventuate and result in information systems assets being exposed, removed either temporarily or permanently, lost, damaged, destroyed or used for

unauthorized purposes. Some of the major threats and to the security of information systems and their controls are as discussed in the Table 3.7.2:

Table 3.7.2: Major Security threats and their control measures

Threat	Controls
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 regulators, circuit breakers, and uninterruptible power supplies can be used.
Structural Damage	Facilities like BCP, DRP, Insurance etc. must be adapted to withstand structural damages that may occur due to earthquake, snow, wind, avalanche etc.
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 and services	Code of conduct to govern the actions of information systems employees.
Hackers	Strong, logical access controls to mitigate losses from the activities of hackers.

However, in spite of the controls on place, there could be a possibility that a control might fail. When disaster strikes, it still must be possible to recover operations and mitigate losses using the last resort controls - A Disaster Recovery Plan (DRP) and Insurance.

- ***DRP: A comprehensive DRP comprise four parts – an Emergency Plan, a Backup Plan, a Recovery Plan and a Test Plan. The plan lays down the policies, guidelines, and procedures for all Information System personnel.*** BCP (Business Continuity Planning) 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 on business in the event of a major disruption. The controls include Critical Classification, alternative procedures, Back-up and 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.

- ***Insurance:*** ***Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations. Policies usually can be obtained to cover the resources like – Equipment, Facilities, Storage Media, Valuable Papers and Records etc.***

3.7.7 Operations Management Controls

Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the functions as below:

(a) Computer Operations: The controls over computer operations govern the activities that directly support the day-to-day execution of either test or production systems on the hardware/software platform available. Three types of controls fall under this category:

- ***Operation controls: These controls prescribe the functions that either human operators or automated operations facilities must perform.***
- ***Scheduling controls: These controls prescribe how jobs are to be scheduled on a hardware/software platform.***
- ***Maintenance controls: These controls prescribe how hardware is to be maintained in good operating order.***

(b) Network Operations: This includes the proper functioning of network operations and monitoring the performance of network communication channels, network devices, and network programs and files. 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 cables, fiber optics, microwave and 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.

(c) Data Preparation and Entry: Irrespective of whether the data is obtained indirectly from source documents or directly from, say, customers, keyboard environments and facilities should be designed to promote speed and accuracy and to maintain the well being of keyboard operators.

(d) Production Control: This includes the major functions like- receipt and dispatch of input and output; job scheduling; management of service-level agreements with users; transfer pricing/charge-out control; and acquisition of computer consumables.

(e) File Library: This includes the management of an organization's machine-readable storage media like magnetic tapes, cartridges, and optical disks.

(f) Documentation and Program Library: This involves that documentation librarians ensure that documentation is stored securely; that only authorized personnel gain access to documentation; that documentation is kept up-to-date and that adequate backup exists for documentation. The documentation may include reporting of responsibility and authority of each function; Definition of responsibilities and objectives of each functions; Reporting responsibility and authority of each function; Policies and procedures; Job descriptions and Segregation of duties.

- *Each IS function must be clearly defined and documented including system software, application software, database administration etc.*
- *Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. Procedures establish the instructions that individuals must follow to compete their daily assigned tasks.*
- *Documented policies should exist in IS for use of IS resource; 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.*
- *Job descriptions 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.*
- *Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions.*

(g) Help Desk/Technical support: This assists end-users to employ end-user hardware and software such as micro-computers, spreadsheet packages, database management packages etc. and also provides the technical support for production systems by assisting with problem resolution.

(h) Capacity Planning and Performance Monitoring: Regular performance monitoring facilitates the capacity planning wherein the resource deficiencies must be identified well in time so that they can be made available when they are needed.

(i) Management of Outsourced Operations: This has the responsibility for carrying out day-to-day monitoring of the outsourcing contract.

3.8 Application Controls and their Categories

Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise. Applications represent the interface between the user and the business functions. For example, a counter clerk at a bank is required to perform various business activities as part of his/her job description and assigned responsibilities. S/he is able to relate to the advantages of technology when he is able to

interact with the computer system from the perspective of meeting his job objectives. From the point of view of users, it is the applications that drive the business logic. Different Application Controls are as follows:

3.8.1 Boundary Controls

(i) 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 as shown in the Fig. 3.8.1.

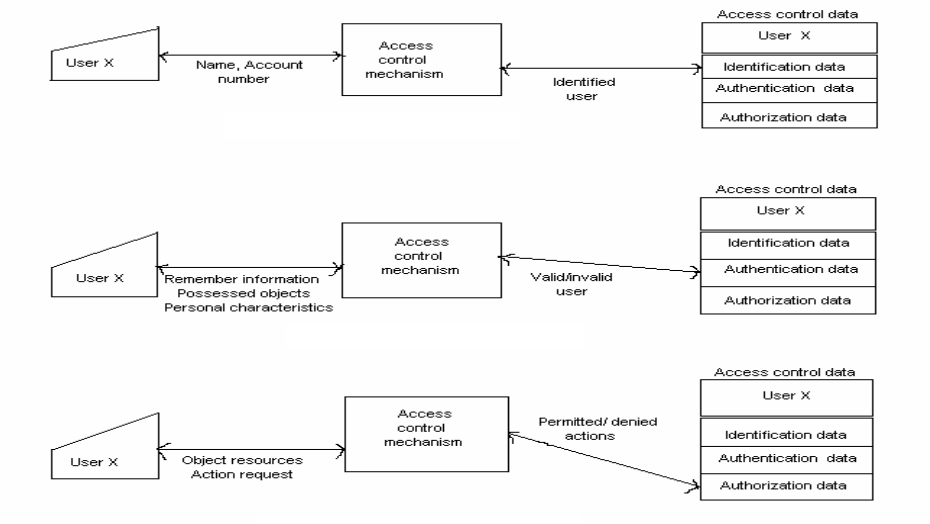

Fig. 3.8.1: Identification/Authentication /Authorization Process

The user can provide three factors of input information for the authentication process and gain access to his required resources. The three factors of information with respect to the corresponding input to the boundary control are summarized in the Table 3.8.1.

Table 3.8.1: Authentic Information

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:

- **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). A pictorial representation of the same is given in Fig. 3.8.2.

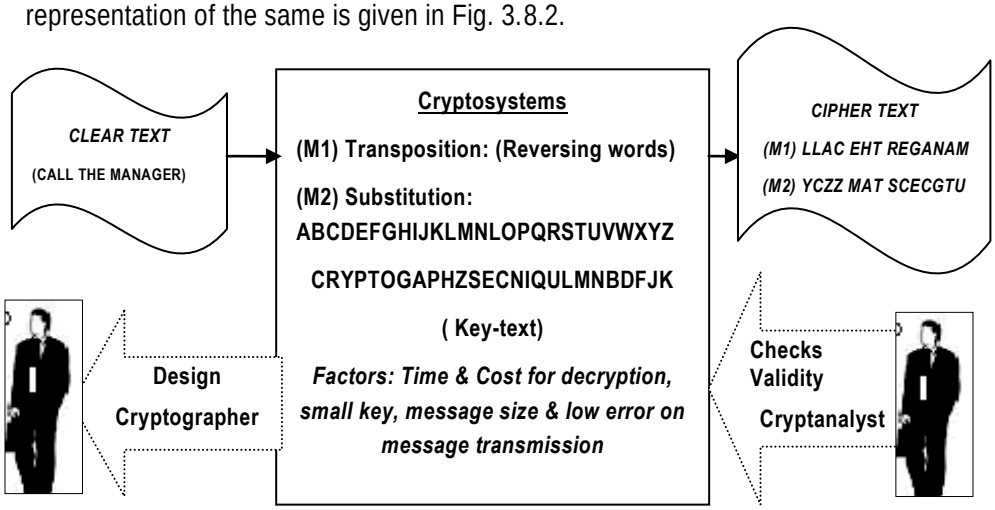

Fig. 3.8.2: Cryptography Techniques

- **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. A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, hashing of passwords and number of entry attempts.
- **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. Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
- **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.
- **Biometric Devices:** Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

3.8.2 Input Controls

These controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input controls are important since substantial time is spent on input of data, involve human intervention and are, therefore error and fraud prone.

Controls relating to data input are critical. It might be necessary to reprocess input data in the event, master files are lost, corrupted, or destroyed. Controls relating to instructions are often in the form of changes to data, which are recorded in the audit trail. Thus, source documents

or transaction listings are to be stored securely for longer periods for reasons – compliance with statutory requirements. Input controls are divided into the following broad classes:

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:

(a) 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. For example, an individual with access to purchase orders and receiving reports could fabricate a purchase transaction to a non-existent supplier. If these documents were entered into the data processing stream along with a fictitious vendor's invoice, the system could process these documents as if a legitimate transaction had taken place. In the absence of other compensating controls to detect this type of fraud, the system would create an account payable and subsequently write a cheque for payment.

To control against this type of exposure, the organization must implement control procedures over source documents to account for each document, as described below:

- **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.
- **Use source documents in sequence:** Source documents should be distributed to the users and used in sequence. This requires the adequate physical security be maintained over the source document inventory at the user site. When not in use, documents should be kept under lock and key and access to source documents should be limited to authorized persons.
- **Periodically audit source documents:** Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors. Documents not accounted for should be reported to management.

(b) 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:

- **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.

- **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.

Any of these errors can cause serious problems in data processing if they go undetected. For example, a sales order for customer 987654 that is transposed into 897654 will be posted to the wrong customer's account. A similar error in an inventory item code on a purchase order could result in ordering unneeded inventory and failing to order inventory that is needed. These simple errors can severely disrupt operations.

(c) 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 or irregularities. Two types of batches occur:

- **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.
- **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 the 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 3.8.2.

Table 3.8.2: Control Totals on Logical / Physical Batch

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, eg., the source document serial numbers can be totaled.
Document/Record Counts	Grand totals for the number of documents in record in the batch.

In case of Physical Controls, these totals can be written on the batch cover sheet and keyed into the application system prior to the key entry of the transactions in the batch. The input program then computes the batch totals as the transactions are entered. When keying of all

the transactions in the batch has been completed, it compares the computed total against the entered total and signals any discrepancy.

In case of logical batch, the person responsible for keying data must keep an independent record of transactions entered into the application system. Periodically, the batch totals calculated by the input program must then be compared against the batch totals calculated on the basis of these independent records.

(d) Validation Controls: Input validation controls are intended to detect errors in the transaction data before the data are processed. There are three levels of input validation controls:

- **Field Interrogation:** It involves programmed procedures that examine the characters of the data in the field. The following are some common types of field interrogation. Various field checks used to ensure data integrity have been described below:
  - **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 exceeding certain pre-established limits has occurred.
  - **Picture Checks:** These check against entry into processing of incorrect/invalid characters.
  - **Valid Code Checks:** Checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid. The predetermined codes or tables may either be embedded in the programs or stored in (direct access) files.
  - **Check Digit:** One method for detecting data coding errors is a check digit. A check digit is a control digit (or digits) 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, a suffix, or embedded someplace in the middle.
  - **Arithmetic Checks:** Simple Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.

    Example: The discounted amount for ₹ 4,000 at 5% discounted may be computed twice by the following different ways:

    4,000 – 4,000 × 5/100 = 3,800 or

    Next time again at

    (3800/(100-5))*100.
  - **Cross Checks:** may be employed to verify fields appearing in different files to see that the result tally.
- **Record Interrogation:** These are discussed as follows:
  - **Reasonableness Check:** Whether the value specified in a field is reasonable for that particular field?

- **Valid Sign:** The contents of one field may determine which sign is valid for a numeric field.
- **Sequence Check:** If physical records follow a required order matching with logical records.

- **File Interrogation:** These are discussed as follows:
  - **Version Usage***:* Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file be processed.
  - **Internal and External Labeling:** Labeling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process for loading files, external labeling is important to ensure that the correct file is being processed. Where there is an automated tape loader system, internal labeling is more important.
  - **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.
  - **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/events are rolled back or forward.
  - **File Updating and Maintenance Authorization:** Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or of the overall system access restrictions.
  - **Parity Check:** When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.

3.8.3 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.

These controls discusses exposures in the communication subsystem, controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.

(a) Physical Component Controls: These controls incorporate features that mitigate the possible effects of exposures. The Table 3.8.3 below gives an overview of how physical components can affect communication subsystem reliability.

Table 3.8.3: Physical Components affecting reliability of Communication subsystem

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.
Communication Lines	The reliability of data transmission can be improved by choosing a private (leased) communication line rather than a public communication line.
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 a process called equalization. • Reduces the number of line errors that arise through noise.
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.
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.

(b) 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.

(c) 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 can not display data on its screen at the same rate the data arrives from the main frame. Moreover, the microcomputer will have limited buffer space. Thus, it cannot continue to receive data from the

mainframe and to store the data in its buffer pending display of the data on its screen. Flow controls will be used, therefore, to prevent the mainframe swamping the microcomputer and, as a result, data is lost.

(d) Link Controls: In WANs, line error control and flow control are important functions in the component that manages the link between two nodes in a network. The link management components mainly use two common protocols HDLC (Higher Level Data Link control) and SDLC (Synchronous Data Link Control).

(e) Topological Controls: A communication network topology specifies the location of nodes within a network, the ways in which these nodes will be linked, and the data transmission capabilities of the links between the nodes. Specifying the optimum topology for a network can be a problem of immense complexity.

- **Local Area Network Topologies:** Local Area Networks tend to have three characteristics: (1) they are privately owned networks; (2) they provide high-speed communication among nodes; and (3) they are confined to limited geographic areas (for example, a single floor or building or locations within a few kilometers of each other). They 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.
- **Wide Area Network Topologies:** Wide Area Networks have the following characteristics:
  - o they often encompass components that are owned by other parties (e.g. a telephone company);
  - o they provide relatively low-speed communication among nodes; and
  - o 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.

(f) 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.

- **Polling:** Polling (non contention) techniques establish an order in which a node can gain access to channel capacity.
- **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, however, depends on the actions of other nodes connected to the channel.

(g) 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. The networks connected to each other might or might not employ the

same underlying hardware-software platform. Three types of devices are used to connect sub-networks in an internet as shown in Table 3.8.4.

Table 3.8.4: Internetworking Devices

Device	Functions
Bridge	A bridge connects similar local area networks (e.g. one token ring network to another token ring network).
Router	A router performs all the functions of a bridge. In addition, it can connect heterogeneous Local Area Networks (e.g. a bus network to a token ring network) and direct network traffic over the fastest channel between two nodes that reside in different sub-networks (e.g. by examining traffic patterns within a network and between different networks to determine channel availability.)
Gateway	Gateway is the most complex of the three network connection devices. The primary function is to perform protocol conversion to allow different types of communication architectures to communicate with one another. The gateway maps the functions performed in an application on one computer to the functions performed by a different application with similar functions on another computer.

3.8.4 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.

(i) 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 in the Table 3.8.5.

Table 3.8.5: Operating System Control

Control	Explanation
Error Detection and Correction	Occasionally, processors might malfunction. The causes could be design errors, manufacturing defects, damage, fatigue, electromagnetic interference, and ionizing radiation. Various types of error detection and correction strategies must be used.
Multiple Execution States	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, such as gaining access to sensitive data

	maintained in memory regions assigned to the operating system or other user processes.
Timing Controls	An operating system might get stuck in an infinite loop. In the absence of any control, the program will retain use of processor and prevent other programs from undertaking their work.
Component Replication	In some cases, processor failure can result in significant losses. Redundant processors allow errors to be detected and corrected. If processor failure is permanent in multicomputer or multiprocessor architectures, the system might reconfigure itself to isolate the failed processor.

(ii) 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.

(iii) Virtual Memory Controls: Virtual Memory exists when the addressable storage space is larger that 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.

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:

- **Identification:** First and foremost, the users have to identify themselves.
- **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 with respect to these resources; it then permits or denies the request. Users may provide four factor of authentication information as described in Table 3.8.6.

Table 3.8.6: Classes of Authentication

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

- **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”, and
  - a “list oriented approach”.

Considering the authorization function in terms of a matrix where rows represent the users and columns represent the resources and the element represents the users privilege on the resources, we can see the distinction between these two approaches.

- 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.
- 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 Table 3.8.7 given below illustrates the authorization matrix in an access control mechanism.

Table 3.8.7: Authorization Matrix

User	File A	Editor	File B	Program
User P	Read	Enter		
User Q	Statistical Read only	Enter		Enter
User R		Enter	Append only	
User S		Enter		Read Resource Code only

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.

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. It is enough to examine the access control list just to know who has access over the resource and similarly to revoke access to a resource, a user's entry in the access control list simply needs to be deleted.

(iv) 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. However, adequate controls should be enforced through the front end application system also to have consistency in the control process. Various processing controls are given as follows:

- **Run-to-run Totals:** These help in verifying data that is subject to process through different stages. If the current balance of an invoice ledger is ₹ 150,000 and the additional invoices for the period total ₹ 20,000 then the total sales value should be ₹

170,000. A specific record probably the last record can be used to maintain the control total.

- **Reasonableness Verification:** Two or more fields can be compared and cross verified to ensure their correctness. For example, the statutory percentage of provident fund can be calculated on the gross pay amount to verify if the provident fund contribution deducted is accurate.
- **Edit Checks:** Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.
- **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, i.e. setting all values to zero/blank before inserting the field or record.
- **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. For example, while processing a journal entry if only debit entry was updated and the credit entry was not updated due to the absence of one of the important fields, then the exception report would detail the transaction code, and why it was not updated in the database.

3.8.5 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:

- **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 updating, insertion or deletion of records in the master file with respect to the transaction records. If errors, in this stage are overlooked, it leads to corruption of the critical data.
- **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 the master file is to be ensured.
- **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). Here, the order in which transactions are processed against the product master record must be done based on a sorted transaction codes.
- **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. A non-zero balance of the suspense accounts reflects the errors to be corrected.

Major Report controls are given as follows:

- **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. Maintaining integrity of the pay rate table, price table and interest table is critical within an organization. Any changes or errors in these tables would have an adverse effect on the organizations basic functions. Periodic monitoring of these internal tables by means of manual check or by calculating a control total is mandatory.
- **Print-Run-to Run control Totals:** Run-to-Run control totals help in identifying errors or irregularities like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.
- **Print Suspense Account Entries:** Similar to the update controls, the suspense account entries are to be periodically monitors with the respective error file and action taken on time.
- **Existence/Recovery Controls:** The back-up and recovery strategies together encompass the controls required to restore failure in a database. Backup 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.

3.8.6 Output Controls

These controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Output can be in any form, it can either be a printed data report or a database file in a removable media such as a CD-ROM or it can be a Word document on the computer's hard disk. Whatever the type of output, it should be ensured that the confidentiality and integrity of the output is maintained and that the output is consistent. Output controls have to be enforced both in a batch-processing environment as well as in an online environment. Various Output Controls are given as follows:

- **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 such as security forms, negotiable instruments, etc.
- **Logging of output program executions:** When programs used for output of data are executed, these should be logged and monitored; otherwise confidentiality/integrity of the data may be compromised.
- **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.

- **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. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.
- **Report distribution and collection controls:** Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. A log should be maintained for reports that were generated and to whom these were distributed. Where users have to collect reports the user should be responsible for timely collection of the report, especially if it is printed in a public area. A log should be maintained about reports that were printed and collected. Uncollected reports should be stored securely.
- **Retention controls:** Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced. Various factors ranging from the need of the output, use of the output, to legislative requirements would affect the retention period.

3.9 Information Technology General Controls

Information Technology General Controls (ITGC) are the basic policies and procedures that ensure that an organization's information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions. IT General Controls are the foundation for the overall IT control environment as they provide the assurance that systems operate as intended and that output is reliable. Failure to ensure these controls are designed and operating effectively means that there will not be any assurance over the IT Application Controls.

ITGCs may also be referred to as General Computer Controls (GCC) which are defined as: Controls, other than application controls, which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.

General Controls are those that control the design, security, and use of computer programs and the security of data files in general throughout an organization. On the

whole, General Controls apply to all computerized applications and consist of a combination of system software and manual procedures that create an overall control environment.

Examples of primary objectives for general controls are to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the entity-wide, system, and business process application levels. The effectiveness of general controls at the entity-wide and system levels is a significant factor in determining the effectiveness of business process controls at the application level. Without effective general controls at the entity-wide and system levels, business process controls generally can be rendered ineffective by circumvention or modification. The most common ITGCs are as follows:

- ***Logical access controls over infrastructure, applications, and data.***
- ***System development life cycle controls.***
- ***Program change management controls.***
- ***Data center physical security controls.***
- ***System and data backup and recovery controls.***
- ***Computer operation controls.***

These General controls have already been covered in earlier topics.

3.10 Controls over Data Integrity and Security

Before discussing the controls relating to Data Integrity, it is important to understand the concept of information classified. The classification of information and documents is essential if one has to differentiate between that which is of little (if any) value, and that which is highly sensitive and confidential. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level. For many organizations, a simple 5 scale grade will suffice as follows:

- **Top Secret:** Highly sensitive internal information e.g. pending mergers or acquisitions; investment strategies; plans or designs; that could seriously damage the organization if such information were lost or 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.
- **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., patient's medical records and similar highly sensitive data. 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.

- **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 normally for proprietary use to authorized personnel only. Security at this level should be high.
- **Internal Use only:** Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level should controlled but normal.
- **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.

3.10.1 Data Integrity

The organization has to decide about various data integrity controls implementation. The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through various stages of a specific date processing program. In other words, they 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 the 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

Data integrity is a reflection of the accuracy, correctness, validity, and currency of the data. The primary objective in ensuring integrity is to protect the data against erroneous input from authorized users. 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. A user may assume that the visible output is the only system activity but there is possibility that erroneous data could infest the system. A person other than the designer or user should test the application. Again, this is critical if the service desk is outsourced to an application service provider. Release of customer information to such an entity must be controlled through contractual requirements with penalties if data is compromised.

There are six categories of integrity controls summarized in Table 3.10.1.

Table 3.10.1: Data Integrity Controls

Control Category	Threats/Risks	Controls
Source data control	Invalid, incomplete, or inaccurate source data input	Forms design; sequentially pre-numbered forms, turnaround documents; cancellation and storage of documents, review for appropriate authorization; segregation of duties, visual scanning; check-digit

		verification; and key verification.
Input validation routines	Invalid or inaccurate data in computer-processed transaction files	As transaction files are processed, edit programs check key data fields using these edit checks, sequence, field, sign, validity, limit, range, reasonableness, redundant data, and capacity checks. Enter exceptions in an error log; investigate, correct, and resubmit them on time; re-edit them, and prepare a summary error report.
On-line data entry controls	Invalid or inaccurate transaction input entered through on-line terminals	Field, limit, range, reasonableness, sign, validity, and redundant data checks; user-ids and passwords; compatibility tests; automatic system date entry; prompting operators during data entry, pre-formatting, completeness test; closed-loop verification; a transaction log maintained by the system; clear error messages, and data retention sufficient to satisfy legal requirements.
Data processing and storage controls	Inaccurate or incomplete data in computer-processed master files	Policies and procedures (governing the activities of data processing and storage personnel; data security and confidentiality, audit trails, and confidentiality agreements); monitoring and expediting data entry by data control personnel; reconciliation of system updates with control accounts or reports; reconciliation of database totals with externally maintained totals; exception reporting, data currency checks, default values, data marching; data security (data library and librarian, backup copies of data files stored at a secure off-site location, protection against conditions that could harm stored data); use of file labels and write protection mechanisms, database protection mechanisms (data wise administrators, data dictionaries, and concurrent update controls); and data conversion controls.
Output controls	Inaccurate or incomplete computer output	Procedures to ensure that system outputs conform to the organization's integrity objectives, policies, and standards, visual review of computer output, reconciliation of batch totals; proper distribution of output; confidential outputs being delivered are protected from unauthorized access, modification, and misrouting; sensitive or confidential out-put stored in a secure area;

		review of user of computer output for completeness and accuracy, shredding of confidential output no longer needed; error and exception reports.
Data transmission controls	Unauthorized access to data being transmitted or to the system itself; system failures; errors in data transmission	Monitor network to detect week points, backup components, design network to handle peak processing, multiple communication paths between network components, preventive maintenance, data encryption, routing verification (header labels, mutual authentication schemes, callback systems), parity checking; and message acknowledgement procedures (echo checks, trailer labels, numbered batches)

3.10.2 Data Integrity Policies

Major data integrity policies are given as under:

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
- **Division of Environments:** The division of environments into Development, Test, and Production is required for critical systems.
- **Offsite Backup Storage:** Backups older than one month must be sent offsite for permanent storage.
- **Quarter-End and Year-End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes
- **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

3.10.3 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 the data. Multiple levels of data security are necessary in an information system environment; they include database protection, data integrity, and security of the hardware and software controls, physical security over the user, and organizational policies. An IS auditor is responsible to evaluate the following while reviewing the 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.

3.11 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 the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger. The financial control techniques are numerous. A few examples are highlighted here:

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

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

3.12 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 the 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.
- 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, namely, data corruption, slow operations and system break down etc.
- Segregation of duty is not possible, owing to limited number of staff.
- 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: Most of the log-on procedures become active only at the booting of the computer from the hard drive.

The Security Measures that could be exercised to overcome these aforementioned 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.

3.13 Cyber Frauds

With the advancements in the technology, cyber frauds are also increasing day-by-day across the world. One of the major reasons behind the rise of such frauds is as follows:

- Failure of internal control system,
- Failure of organizations to update themselves to new set of risk, and
- 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.

All of the above are key ingredients to increased instances of cyber frauds. In India, the Information Technology Amendment Act, 2000 and amended in 2008 has specific sections dealing with cyber frauds. The same has been discussed under the regulatory issues of Chapter 7 of the Study Material. The discussion in this part is based on general nature of cyber frauds.

Fraud, as defined by SA 240 (Revised), on "The Auditor's responsibility to consider fraud and error in an audit of financial statements", defines fraud as "intentional misrepresentation of financial information by one or more individuals among employees, management, those charged with governance, or third parties." This definition is in context of financial information; same can be applied to any information used for decision making. Fraud has also 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. Other common forms may be monetary cyber frauds include non-delivery of paid products purchased through online auction etc.

On the basis of the functionality, these are of two types:

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

The fraudster may be from within the organization or from outside the organization. But, it has been observed that most of cyber frauds include more than one individual and one of the team members in many cases is a person within the organization.

3.13.1 Cyber Attacks

Some of the major cyber attacks are as follows:

- **Phishing:** It is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) 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.
- **Network Scanning**: It is a process to identify active hosts of a system, for purpose of getting information about IP addresses etc.
- **Virus/Malicious Code**: As per Section 43 of the 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 or some other event takes place in that computer resource;

- **Spam**: E-mailing the same message to everyone on one or more Usenet News Group or LISTSERV lists is termed as spam.
- **Website Compromise/Malware Propagation**: It includes website defacements. Hosting malware on websites in an unauthorized manner.
- **Others:** These are given as follows:
  - **Cracking:** Crackers are hackers with malicious intentions.
  - **Eavesdropping:** It refers to the listening of the private voice or data transmissions, often using a wiretap.
  - **E-mail Forgery:** Sending e-mail messages that look as if someone else sent it is termed as E-mail forgery.
  - **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.
  - **Scavenging:** This is gaining access to confidential information by searching corporate records.

3.13.2 Impact of Cyber Frauds on Enterprises

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

- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.
- **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 companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.
- **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. There have been instances where share prices of such companies went down, as the news of such attach percolated to the market.
- **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.
- **Sabotage:** The above situation may lead to misuse of such information by enemy country.

3.13.3 Techniques to Commit Cyber Frauds

Following are the major techniques to commit cyber frauds:

- **Hacking:** It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.
- **Cracking:** Crackers are hackers with malicious intentions, which means, un-authorized entry. Now across the world hacking is a general term, with two nomenclatures namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking.
- **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.
- **Data Leakage:** It refers to the unauthorized copying of company data such as computer files.
- **Denial of Service (DoS) Attack:** It refers to an action or series of actions that prevents access to a software system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.
- **Internet Terrorism:** It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.
- **Logic Time Bombs:** These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
- **Masquerading or Impersonation:** In this case, perpetrator gains access to the system by pretending to be an authorized user.
- **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.
- **Piggybacking:** It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
- **Round Down:** Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
- **Scavenging or Dumpster Diving:** It refers to the gaining access to confidential information by searching corporate records.
- **Social Engineering Techniques:** In this case, perpetrator tricks an employee into giving out the information needed to get into the system.
- **Super Zapping:** It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.
- **Trap Door:** In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.

In spite of having various controls as well as countermeasures in place, cyber frauds are happening and increasing on a continuous basis. To overcome these frauds, there is an urgent need to conduct research in the related areas and come up with more appropriate

security mechanisms, which can make the information systems more secure.

3.14 Summary

The chapter deals with Information System Security and its importance to an organization. The chapter defines the categories of information that may be considered sensitive and how same needs to be protected. In addition, the chapter also elaborates the concept of Information System Security Policy and the various components of the same. There is detailed discussion on each of the component of Information System Security Policy. It elaborates the steps to converting policies into Standards, Guidelines and Procedures.

The next part of chapter deals with controls and their types. The chapter elaborates the need for such controls. There is detailed discussion on the nature of controls and its implementation across organization. Failures to implement such controls and the resulting frauds have also been dealt in the chapter.

Appendix-1

Master Checklist on Logical Access Controls

The following is an illustrative Checklist that could be used to review Logical Access Controls within application systems and databases.

No	Checkpoints
	User Access Management Policy and Procedure
1.	Whether the user access management policy and procedure are documented?
2.	Whether the user access management policy and procedure are approved by the management?
3.	Whether the user access management policy and procedure document includes: - Scope and objective. - Procedure for user ID creation, approval, review, suspension, and deletion. - Granting access to third parties. - Password management. - User access rights assignment & modifications. - Emergency access Granting. - Monitoring access violations. - Review and update of document.
	User Access Management
1.	Whether User ID & access rights are granted with an approval from appropriate level of IS and functional head? *(Verify the user ID creation, granting of access right and approval process)*
2.	Whether the organization follows the principle of segregation of duties adequately in granting access rights?
3.	Whether User IDS are in a unique format? *(Verify the naming conventions for the user IDs)*
4.	Whether invalid login attempts are monitored and User IDs are suspended on specific attempt? *(Verify the parameters set for unsuccessful login attempt)*
5.	Whether the organisation follows complex composition for password parameters? *(Complex composition of password parameter should be used as to make it difficult for guessing and prevent unauthorised users from access e.g. special character and numbers should be part of password, Restrict use of organisation's name, 123, xyz or other generic terms as password)*
6.	Whether granting access to the third parties is according to the User Access Management policy and procedure?

	(The organization should specify and implement a process for granting access to third parties like contractors, suppliers, auditors, consultants etc.)
7.	Whether users are forced to change password on first log-on and at periodic intervals? *(Verify password parameters for first log on and password aging)*
8.	Whether the organisation implemented clear screen and clear desk policies? *(On the desktop classified information should not be available, similarly no classified information should be available on the table unattended)*
9.	Whether the organisation restricted concurrent log- on? *(One user ID should not be allowed to login from two different terminals at the same time)*
10.	Whether users' IDs are shared? *(Verify whether users' IDs are shared among the employees/ users or not?)*
11.	Whether multiple user IDs are allocated to a single individual?
12.	Are user access policy and procedure documents communicated / available to the respective users?
13.	Whether User IDs and Password are communicated to the user in a secured manner? *(Verify the procedure for communicating user ID and password for the first time and after suspension)*
14.	Whether the organisation reviews user IDs and access rights at periodic intervals?
15.	Whether the organisation monitors logs for the user access?
16.	Whether policy and procedure are documents reviewed and updated at regular intervals?
17.	Whether the access to scheduled job is restricted to the authorised?
18.	Whether an emergency user creation is according to the policy and procedure for User Access Management? *(Verify the emergency access granting procedure, including approvals and monitoring)*
19.	Whether periodic review process ensures user accounts align with business needs and removal on termination/transfer? (*Review and evaluate procedures for creating user accounts and ensure that accounts are created only when there's a legitimate business need and that accounts are removed or disabled in a timely fashion in the event of termination or job change.)*
20.	Whether passwords are shadowed and use strong hash functions? *(Ensure the strength hashing algorithm of.)*

21.	Review the process for setting initial passwords for new users and communicating those passwords and evaluate the tracking of each account to a specific employee.
22.	Whether the use of groups and access levels set for a specific group determines the restrictiveness of their use? (Evaluate the use of passwords, access rights at the group level)
23.	Ensure that the facility to logon as super/root user is restricted to system console for security reasons.
24.	Check whether the parameters to control the maximum number of invalid logon attempts has been specified properly in the system according to the security policy.
25.	Check whether password history maintenance has been enabled in the system to disallow same passwords from being used again and again on rotation basis.
26.	Verify the parameters in the system to control automatic log-on from a remote system, concurrent connections a user can have, users logged on to the system at odd times (midnight, holidays, etc) and ensure whether they have been properly set according to security policy.
	Maintenance of sensitive user accounts
1.	Ascertain as to who is the custodian of sensitive passwords such as super/root user and verify if that person is maintaining secrecy of the password, whether the password has been preserved in a sealed envelope with movement records for usage in case of emergency.
2.	From the log file, identify the instances of use of sensitive passwords such as super user and verify if records have been maintained with reason for the same. Ensure that such instances have been approved/ authorized by the management.
3.	From the log file, identify the instances of unsuccessful logon attempts to super user account and check the terminal ID / IP address from which it is happening. Check if appropriate reporting and escalation procedures are in place for such violations

Appendix-2

Master Checklist for Physical and Environmental Security

To ensure that IS assets are maintained in a secured manner within a controlled environment, the following checklist is given:

Sr. No.	Check points
Secured Physical Access	
1.	Whether Physical Access Control Policy is documented and approved?

2.	Whether the policy on the following is appropriate and covers: - Lay out of facilities - Physical Security of the assets - Physical access to the assets - Maintenance of the assets - Signage on the facilities - Labels for assets - Visitors' authorization and recording - Entrance and exit procedures - Legal & regulatory requirements
3.	Whether critical Information System facilities (like data center) are located appropriately? (Verify the location for the following as:- - Protection against natural disasters like earthquakes, flooding, extreme weather etc. - Not in congested places - Not being on ground or top floor - Not being below ground level to avoid water leakage etc. - Not having a showcase window - Not having a direct access from the outside or through a public hallway - Place which is not obvious externally)
4.	Whether the access to IS facilities is controlled through a secured mechanism? (Verify the access control mechanism - e.g. access card, lock and key or manned reception)
5.	Whether the access to the IS facilities is limited to approved persons only? (Approved persons may include employees, vendors and customers)
6.	Whether the physical access control procedures are adequate and appropriate for approved persons? (Access should be provided on need to do and need to know basis)
7.	Whether the visitor to critical IS facilities are escorted by employees? (Records for visitors' access should be maintained)
8.	Whether a periodical review of access rights is carried out?
9.	Whether the physical security is continually addressed?
10.	Whether all access routes are identified and controls are in place?
11.	Whether the security awareness is created not only in IS function but also across the organization?
12.	Whether the physical security is ensured at suppliers' facilities also in cases where organization's' assets (either physical or data) are processed at supplier's

	facilities?
13.	Whether the usage of any equipment outside the business premises for information processing is authorized by the management?
14.	Is the security provided to equipment used outside business premises similar to / same as that offered to equipment used inside the business premises?
15.	Whether adequate monitoring equipments are present to monitor the movements of the personnel inside the facility?
16.	In case of outsourced software, whether all maintenance work is carried out only in the presence of/ with the knowledge of appropriate IS staff?
17.	Whether appropriate access controls like password, swipe card, bio-metric devices etc. are in place and adequate controls exist for storing the data/ information on them? Are there controls to ensure that the issue and re-collection of such access devices are authorized and recorded?
18.	Whether access violations are recorded, escalated to higher authorities and appropriate action taken?
19.	Whether employees are required to keep the critical / sensitive documents in secured places?
20.	Check if IS facility is accessed for information security related risks with respect to lighting, building orientation, signage and neighborhood characteristics are identified?
21	Verify that surveillance systems are designed and operating properly?
22	Ensure that physical access control procedures are comprehensive and being followed by security staff.
23	Verify if the security controls in place are appropriate to prevent intrusion into sensitive IS facilities –data centre, communication hubs, emergency power services facilities?
24	Review facility monitoring measures to ensure that alarm conditions are addressed promptly.
Environmental Controls	
1.	Whether the Environmental Control policy is documented and approved?
2.	Whether IS facilities are situated in a place that is fire resistant? (Verify for wall, floor, false ceiling, furniture and cabling being noncombustible / fire resistant / fire retardant)
3.	Whether smoking restrictions in IS facilities are in place?
4.	Whether adequate smoke / temperature detectors are installed, connected to the fire alarm system and tested?

5.	Whether fire prevention instructions are clearly posted and fire alarm buttons clearly visible?
6.	Whether emergency power-off procedures are laid down and evacuation plan with clear responsibilities in place?
7.	Whether fire prevention and control measures implemented are adequate and tested periodically?
8.	Whether fire drill and training are conducted periodically?
9.	Whether air-conditioning, ventilation and humidity control procedures are in place, tested periodically and monitored on an ongoing basis?
10.	Whether an adequate alternate power arrangement is available? If so, is it covered under maintenance?
11.	Whether alternative water, fuel, air-conditioning and humidity control resources are available?
12.	Check if heating, ventilation, and air-conditioning systems maintain constant temperatures within a data center and other IS facilities?
13.	Evaluate the data center's use of electronic shielding to verify that radio emissions do not affect computer systems or that system emissions cannot be used to gain unauthorized access to sensitive information.
14.	Verify if there are sufficient battery backup systems providing continuous power during momentary black-outs and brown-outs along with generators that protect against prolonged power loss and are in working condition.
15.	Ensure that a fire alarm is protecting a critical IS facility like data center from the risk of fire, a water system is configured to detect water in high-risk areas of the data center and a humidity alarm is configured to notify data center personnel of either high or low-humidity conditions.
16.	Check logs and reports on the alarm monitoring console(s) and alarm systems which are to be monitored continually by data center/IS facility personnel.
17.	Verify that fire extinguishers are placed every 50ft within data center isles and are maintained properly with fire suppression systems to protect the data center from fire.
18.	Whether there are emergency plans that address various disaster scenarios for example backup data promptly from off-site storage facilities?
19.	Ensure if there exists a comprehensive disaster recovery plan that key employees are aware of their roles in the event of a disaster and are updated and tested regularly.
20.	Ensure that detail of part inventories and vendor agreements are accurate and current and maintained as critical assets.