CHAPTER - 4

INFORMATION SYSTEM AUDIT PROCEDURES
4.1 INFORMATION SYSTEM AUDIT

4.1.1 INTRODUCTION

Information systems auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows the goals to be achieved effectively, and uses resources efficiently.
The information system audit will facilitate the following benefits:

a) Improved safeguarding of assets
b) Improved integrity of data
c) Improved system effectiveness
d) Improved system efficiency

4.1.2 INTENTION OF INFORMATION SYSTEMS AUDITING

The Government or private organizations must control and audit computer-based information systems because the costs of errors and irregularities that arise in these systems can be high. Computer-based information systems do not destabilize the importance of traditional internal control principles. However,
these principles are implemented differently in its own style. Compared with manual information systems, collecting evidence on the reliability of internal controls in computer based information systems is often more complex and critical and it is to be audited.

4.1.3 DEMANDING FACTORS FOR AUDIT IN ORGANIZATIONS

The core factors necessitate the information system audit framework are listed below whose overlook may lead to great repentance.

- Cost of organizational data loss
- Cost of incorrect decision making
- Cost of computer abuse
- Cost of hardware, software and technical personnel
- Cost of computer error
- Cost of privacy
- Cost of computer use

4.1.4 PILLARS OF INFORMATION SYSTEM AUDIT

Many of the principles that underlie the practice of information systems auditing have their roots in other disciplines, such as

- **Traditional auditing**: The knowledge and experience with internal control techniques
- **Computer science**: The latest technical trends in data computation and communications
• **Management:** Managerial skills in development and implementation of information systems

• **Behavioral science:** Auditors must understand the conditions that can lead to behavioral problems and as a result certain system failure can be answered.

---

**Figure: Foundation of information system auditing**

---

### 4.1.5 INFORMATION SYSTEMS AUDITORS

Information systems auditors are the persons who are responsible for collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently. The information system auditors possess traditional auditing skill as well as computer skills. They investigate the ongoing organizational
activities through evidence collection and judge the situation which by following will lead the organizations into limelight. The audit judgment depends on the auditor’s abilities, knowledge, the environment in which they make judgments and their motivation level.

4.1.6 INTERNAL AUDITORS AND EXTERNAL AUDITORS

The two categories of Auditors are internal auditors and external auditors. The internal auditors participate in the concurrent audit in the development of application systems or undertake post implementation reviews of application systems. The external auditors are more likely to undertake general audits.

4.1.7 AUDIT FRAMEWORK

Audit framework is the boundary fixed by Information system auditors to the extent they can perform the auditing activities. The audit framework can be classified into Management Control Framework and Application control framework.

a. MANAGEMENT CONTROL FRAMEWORK

The utmost duty of auditor is, they should observe the management whether they manage the information systems function well or not. The management control framework can be classified as below, whose details are followed in the thesis.

• Top Management Controls
• Systems Development Management Controls
• Programming Management Controls
• Data Resource Management Controls
• Security Management Controls
• Operations Management Controls
• Quality Assurance Management Controls

b. THE APPLICATION CONTROL FRAMEWORK

This involves ensuring that individual application systems safeguard assets, maintain data integrity, and achieve their objectives effectively and efficiently. The application control framework can be classified as follows and are discussed in detailed in the latter sessions.

• Boundary Controls
• Input Controls
• Communication Controls
• Processing Controls
• Database Controls
• Output Controls

4.2 TOP MANAGEMENT CONTROL

4.2.1 INTRODUCTION

Auditors can evaluate top management by examining how well they perform the four major functions:

Planning: Determining the goals of the information systems function and the means of achieving these goals.
Organizing: Gathering, allocating, and coordinating the resources needed to accomplish the goals.

Leading: Motivating, guiding, and communicating with personnel.

Controlling: Comparing actual performance with planned performance as a basis for taking any corrective actions that are needed.

4.2.2 MASTER PLAN

Top management must prepare master plan which is of two types. The long run strategic plan is for next five years which includes Current information assessment, Strategic directions and Development strategy. The short run operational plan is for the current and next year which includes Current plan progress, Proposals to be undertaken and Execution schedule. The three tasks involved in Preparation of plan are Recognizing opportunities and problems, Identifying the resources needed to provide the required information technology and information systems and finally Formulating strategies and tactics for acquiring the needed resources.

4.2.3 PLANNING STYLE

The needs of Information system and its planning change from application to application and from state to state. The auditors must first determine the nature of and amounts of planning that should be undertaken given their organization's needs. The two important planning models are Strategic grid model and Infusion-Diffusion models.
**Strategic-grid model:** In this the nature and amount of information systems planning appropriate to an organization is a function of two important factors

- The strategic importance of an organization's portfolio of existing information systems.
- The strategic importance of an organization's portfolio of proposed systems.

The four types of organizations for which this fits best are Supporting organizations, Factories, Turnaround organizations and Strategic.

**Infusion and Diffusion model:** This focuses on two dimensions

- Infusion—the extent to which information technology and information systems have been integrated into the daily operations of the organization;
- Diffusion—the extent to which information systems and information technology has been dispersed throughout the organization.

The four types of organizations, each with different information systems planning needs are as Traditional, Federation, Backbone and Complex organizations.

### 4.2.4 DIRECTION COMMITTEE

An information systems direction committee should take ultimate responsibility for information systems planning. Depending on the criticality of the Information systems functions of the organization, the functions of the direction committee changes. This committee is popularly called steering committee.
4.2.5 ANALYSIS OF TOP MANAGEMENT ORGANIZING ACTIVITIES

Top management should organize the information system functions properly to safeguard the assets and maintain data integrity. They should Facilitate resources, Manage the personal of the organization and focus on coordinating the activities for smooth functioning. Other organizational activities are as follows.

- Centralization or decentralization of the information systems function
- Hierarchy of Information system staffing
- Position of Information System Function in organization
- Evaluating the leading function
- Evaluating the controlling function

4.3 SYSTEMS DEVELOPMENT MANAGEMENT CONTROLS

4.3.1 INTRODUCTION

These controls provide a contingency perspective on models of the information systems development process that auditors can use as a basis for evidence collection and evaluation. Auditors conduct three types of reviews of the systems development process which includes Concurrent Audit, Post implementation review and General Audit. The responsibilities of System development management controls are shown in the following figure.
4.3.2 NORMATIVE MODELS

To be capable of evaluating the systems development process, auditors need a normative model against which they can compare the systems development practices encountered. Six major normative models of the systems development process are

a) The systems development life-cycle approach, which emphasizes the importance of well-controlled work phases.

b) The socio technical design approach, which emphasizes the importance of jointly optimizing the technical system as well as the social system.

c) The political approach, which emphasizes the importance of understanding the effects that systems can have on the distribution of organizational power.

d) The soft systems approach, which provides ways of helping decision makers learn about ill-structured problems.
e) The prototyping approach, which provides ways of helping resolve the uncertainty often surrounding systems-design tasks.

f) The contingency approach, which emphasizes that the way systems development is undertaken must be adapted in light of the organizational context in which the system is being designed and implemented.

4.3.3 ISSUES FOR EVALUATING SYSTEM DEVELOPMENT PROCESS

To provide the basis for evaluating the systems development process, the following phases provide an agenda of issues that auditors must consider.

- Problem/opportunity definition
- Management of the change process
- Entry and feasibility assessment
- Analysis of the existing system
- Formulation of strategic requirements
- Organizational and job design
- Information processing systems design
- Application software acquisition and development
- Hardware/system software acquisition
- Procedures development
- Acceptance testing
- Conversion
- Operation and maintenance

The specific tasks performed in each phase and the ways in which they are performed should vary depending upon the nature of the system to be developed and the specific context in which
it is being developed. Both designers and auditors must know how to vary their work practices to reflect these contingencies.

Systems development management has responsibility for those functions concerned with analyzing, designing, building, implementing, and maintaining information systems.

4.4 PROGRAMMING MANAGEMENT CONTROLS

4.4.1 INTRODUCTION

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 using certain controls. Some major characteristics of high-quality programs are

- They perform their functions correctly and completely
- They have a high-quality user interface
- They work efficiently
- They are well designed and well documented
- They are easy to maintain
- They are robust under abnormal conditions

4.4.2 PROGRAM DEVELOPMENT LIFE CYCLE

The program development life cycle comprises six major phases which are Planning, Control, Design, Coding, Testing and
Operation and maintenance. The control phase is a continuous phase that runs in parallel with all other phases.

**Planning phase:** During the planning phase of the program development life cycle, management estimates the resources required to develop or acquire programs. Management must also choose a design approach, an implementation approach, integration and testing approach and an organization for the project team.

**Software Cost Estimation Techniques:** Five major software cost-estimation techniques are

- Algorithmic models
- Expert judgment
- Analogy
- top-down estimation
- bottom-up estimation
**Control Phase:** 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. Techniques like Work Breakdown Structures, Gantt charts and PERT charts can be used to monitor progress against plan.

**Gantt Chart for Order-Entry System**

**Design Phase:** Programmers should use a systematic approach to program design, such as any of the structured design approaches or object-oriented design.
Coding Phase: During the coding phase of software development, programmers must choose a module implementation and integration strategy, a coding strategy, and a documentation strategy. Three major module implementation and integration strategies that can be used are Top down, Bottom up and Threads. The documentation strategy should be chosen to ensure program code can be easily read and understood.

Testing Phase: The testing phase of the program development life cycle seeks to ensure a developed or acquired program achieves its specified requirements. Three types of testing can be undertaken.

- unit testing, which focuses on individual program modules
- Integration testing, which focuses on groups of program modules
- whole-of-program testing, which focuses on the total program

Maintenance Phase: Management must establish formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a likely basis. Three types of program maintenance are Repair maintenance, Adaptive maintenance and Perfective maintenance.

4.4.3 ORGANIZING OF PROGRAMMING TEAMS

The structure of programming teams can have an important impact on the quality of the resulting software and the resources consumed to produce the software. There are several ways in
which programming teams may be organized and they are Functional teams, Project teams, Chief programmer teams, Adaptive teams, Controlled-decentralized teams, System Programmers.

4.5 DATA RESOURCE MANAGEMENT CONTROLS

4.5.1 INTRODUCTION

Data is a critical resource that must be carefully planned, managed, centralized and controlled properly. For data to be managed better, four objectives must be achieved

- Users must be able to share data
- Data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed
- It must be possible to modify data fairly easily in light of changing user requirements
- The integrity of data must be preserved

4.5.2 DATA BASE ABSTRACTION

The data which is necessary is made accessible with the concept of database abstraction which comprises of External schema, Conceptual schema, Internal schema and Stored database.
4.5.3 ADMINISTRATION OF DATABASE CONCEPTS

Data administrator (DA) and Database administrator (DBA):

Administrative solutions for the database have come in the form of the data administration and database administration roles. The data administrator handles administrative and policy matters. The database administrator handles technical matters.

Functions of DA and DBA: A major task that data administrators and database administrators perform is to mediate when conflict arises in a shared data environment. In addition, they undertake the following five functions
a) Defining, creating, redefining and retiring data
b) Making the database available to users
c) Informing and servicing users
d) Maintaining database integrity
e) Monitoring operations and performance

**Auditors Co-ordination:** Auditors need a good understanding of the data administrator's and database administrator's roles. If the incumbents do not perform these roles effectively, the quality of the database environment can be seriously undermined. The incumbents can also provide auditors with important information they need to know about control strengths and weaknesses and the means by which they can access the database for evidence collection and evaluation purposes. The organizational placement hierarchy of database administrator is to report to data administrator and works directly under chief information officer.

**Maintaining Database Integrity:** The DA and DBA play a major role in maintaining the integrity of database. There are six areas in which they must undertake control activities which include Definition control, Existence control, Access control, Update control, Concurrency control, Quality control.

**Auditors control over Data:** Auditors should carefully evaluate an organization's use of and control over its data repository system. If it is used properly, a data repository system 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.
Auditors can also use a data repository system to assist them to undertake an audit. Balancing the activities of data administrator and database administrator are critical for auditors to attain goals.

4.6 SECURITY MANAGEMENT CONTROLS

4.6.1 INTRODUCTION

The key task of security management controls are to identify major threats to the information systems function and to design, implement, operate, and maintain controls that reduce expected losses from these threats to an acceptable level. Information security administrators are responsible for ensuring that information systems assets are secure. Assets are secure when the expected losses that will occur over some time are at an acceptable level. The two types of information systems security are Physical security and Logical security.
Physical security protects the physical information systems assets of an organization—personnel, hardware, facilities, supplies, and documentation. Logical security protects data/information and software.

4.6.2 SECURITY ADMINISTRATORS

The specially trained and experienced persons who take care of physical and logical securities are called security administrators. Security administrators tend to have responsibility for controls over malicious and non malicious threats to physical security and malicious threats to logical security.
Security program: A major task of security administrators is to conduct a security program. A security program is a series of ongoing, regular, periodic reviews conducted to ensure that assets associated with the information systems function are safeguarded adequately. The major steps involved in security program are Preparation of a project plan, Identification of assets, Valuation of assets, Threats identification, Threats likelihood assessment, Exposures analysis, Controls adjustment, Report preparation.

Threats to the security of information systems assets: The major threats to the security of information systems assets are Fire, water, energy variations, structural damage, pollution, unauthorized intrusion, viruses and worms, misuse of software, hackers etc. The administrators exercise proper care to control these threats to safeguard the information system assets.

4.7 OPERATIONS MANAGEMENT CONTROLS

4.7.1 INTRODUCTION

Operations management is responsible for the daily running of hardware and software facilities so that Production application systems can accomplish their work and Development staff can design, implement and maintain application systems.

4.7.2 FUNCTIONS OF OPERATIONS MANAGEMENT

Operations management typically exercises controls over Computer operations, Communications network control, Data preparation and entry, Production control, File library, Documentation and program library, Help desk/technical support,
Capacity planning and performance monitoring, Outsourced operations.

a) **Computer operations**: Controls over computer operations govern the activities that support the day-to-day execution of either test or production systems. Three types of controls must exist.

- Those that prescribe the functions that either human operators or automated operations facilities must perform.
- Those that prescribe how jobs are to be scheduled on the hardware / software platform.
- Those that prescribe how hardware is to be maintained in good operating order.

b) **Network operations**: Network operations govern the activities of wide area and local area networks. In wide area networks, careful control should be exercised over network control terminals. These terminals allow powerful access and action privileges to be executed to monitor and maintain a network. A network control terminal provides access to specialized systems software that allows Starting and stopping lines and processes, Monitoring network activity levels, Renaming communications lines, Generating system statistics, Resetting queue lengths, Increasing backup frequency, Inquiring as to system status, Transmitting system warning and status messages and Examining data traversing a communications line.

In local area networks, file servers must be secured. Unauthorized access to a file server can allow an intruder to
disrupt the operations of a local area network or compromise
data integrity within the network.

c) Data preparation and Entry: Data preparation and data entry facilities should be designed to promote speed and accuracy and to maintain the well-being of keyboard operators. Keyboard operators should also be well trained to perform data preparation and data entry tasks. Suitable backup must exist for input data and data preparation and data entry devices.

d) Production control section: The production control section under operations management performs five major functions which are Receipt and dispatch of input and output, Job scheduling, Management of service-level agreements with users, Transfer pricing / charge-out control, Acquisition of computer consumables.

e) File library: The file-library function within the operations area takes responsibility for the management of an organization's machine-readable storage media. The four functions to be undertaken are as follows.

- Ensuring that removable storage media are stored securely in a clean environment
- Ensuring that storage media are used only for authorized purposes
- Maintaining storage media in good working order
- Locating storage media appropriately at either on-site or offsite facilities.

f) Documentation and program library: The documentation and program library function takes responsibility for maintaining
the documentation needed to support computer operations and managing the inventory of acquired or licensed software. Documentation should be kept up-to-date and be used only by authorized parties. Acquired or licensed software should be carefully managed so it is not lost or stolen, its documentation is not lost or stolen.

g) Help Desk / Technical Support: The help desk/technical support function in the operations area has two primary responsibilities

- Assisting end users to employ end-user hardware and software, such as microcomputers, spreadsheet packages, database management packages, and local area networks.
- Providing technical support for production systems by assisting with problem resolution.

h) Capacity planning and performance monitoring: Operations management must continuously monitor the performance of the hardware/software platform to ensure that systems are executing efficiently, an acceptable response time or turnaround time is being achieved, and an acceptable level of uptime is occurring.

i) Outsourced operations: Operations management often has responsibility for managing the day-to-day activities associated with an outsourcing contract. The following four types of controls must be exercised.

- Ongoing evaluation of the financial viability of the outsourcing vendor
• Ensuring compliance with the outsourcing contract's terms and conditions

• Ensuring the ongoing reliability of controls in the outsourcing vendor's operations

• Maintaining procedures for disaster recovery with the outsourcing vendor.

4.8 QUALITY ASSURANCE MANAGEMENT CONTROLS

4.8.1 INTRODUCTION

Quality assurance (QA) management ensures that the information systems produced by the information systems function achieve certain quality goals and that development, implementation, operation and maintenance of information systems obey with a set of quality standards.

4.8.2 MOTIVATIONS TOWARD THE QA ROLE

The various reasons why the information systems QA role has emerged in many areas are as follows.

• Increasingly organizations are producing safety-critical systems.

• Users are becoming more demanding in terms of the quality of the software for customer satisfaction.

• Organizations are undertaking more ambitious

• Information systems projects and to meet the requirements stringent quality control standards are demanded.
• Organizations are becoming increasingly concerned about their liabilities for which quality standards are to be maintained.

• Poor control over the production, implementation, operation, and maintenance of software can be costly in terms of missed deadlines, dissatisfied users etc.

• Improving the quality of software is part of a worldwide trend among organizations to improve the quality of the goods and services they sell.

4.8.3 QA FUNCTIONS

The various quality assurance functions are as follows.

a) Developing Quality Goals: The first function of QA personnel is to develop quality goals and to assist in the development of quality goals for specific information systems. Obtaining consensus on quality goals can be difficult because different stakeholders have differing perspectives on quality, quality goals might need to vary across information systems, and at times quality goals may conflict with one another. The goals should define quality characters such as Functionality of software, Reliability, Usability, Efficiency, Maintainability and Portability. The quality assurance personnel prepares a plan of action before deciding the goals which as shown in the below figure.
b) Developing, Promulgating, and Maintaining Standards for the Information Systems Function: The second function of QA personnel is to develop, promulgate, and maintain information systems standards. Standards are the backbone of planning and control activities in the information systems function. QA personnel are in the best position to be responsible for standards because they should be the most knowledgeable about standards, they should be perceived as independent, and they have incentives to keep standards up to date.
c) Monitoring Compliance with QA Standards: The third function of QA personnel is to monitor compliance with standards. Monitoring must be undertaken in terms of general standards that govern the overall information systems function and specific standards that govern a particular information system.

d) Identifying Areas for Improvement: The fourth function of QA personnel is to identify areas for improvement. Identifying areas for improvement should be part of an ongoing process that leads to higher-quality information systems being produced. QA personnel should make recommendations for improvement based on facts rather than intuition or experience. The improvement of quality is a continuous spiral process.
e) Reporting to Management: The fifth function of QA personnel is to report to management. Regular reports on compliance with general standards and specific standards must be prepared. Reports must be positive in nature, contain no surprises and be based on sound analyses that are supported by concrete facts.

f) Training in QA Standards and Procedures: The sixth function of QA personnel is to train all other information systems personnel in quality assurance standards and procedures. One type of training focuses on general knowledge about standards and procedures. Another type focuses on specific training that is needed to support the development, implementation, operation, and maintenance of a specific application system.

4.9 BOUNDARY CONTROLS

4.9.1 INTRODUCTION

The boundary subsystem establishes the interface between the would-be user of a computer system and the computer system itself. Controls in the boundary subsystem have three purposes

(a) To establish the identity and authenticity of would-be users.

(b) To establish the identity and authenticity of computer system resources that users wish to employ.

(c) To restrict the actions undertaken by users who obtain computer resources to an authorized set.
4.9.2 Cryptographic Controls

Cryptographic controls are used extensively throughout the boundary subsystem. Cryptographic controls protect the privacy of data and prevent unauthorized modifications of data. They achieve this goal by scrambling data so it is not meaningful to anyone who does not have the means to unscramble it. The three popular techniques used in cryptography are Transposition ciphers, Substitution ciphers and Product ciphers.

Public-key cryptosystems: A major disadvantage of conventional or private-key cryptosystems is that the parties who wish to exchange information must share a private, secret key. To overcome this disadvantage, public-key cryptosystems have been developed. Public-key cryptosystems use two different keys to encrypt data and to decrypt data. One key can be made public and the other key is kept private.

![Public Key Cryptosystem Diagram]

**PUBLIC KEY CRYPTOSYSTEM**
4.9.3 ACCESS CONTROLS

Access controls restrict use of computer system resources to unauthorized users, limit the actions users can undertake with respect to those resources and ensure that users obtain only authentic computer resources. Users can provide three classes of authentication information to an access control mechanism:

(a) Remembered information (e.g., passwords)
(b) Possessed objects (e.g., plastic cards)
(c) Personal characteristics (e.g., fingerprints).

An access control mechanism can be either Discretionary access control or Mandatory access control.

4.9.4 PERSONAL IDENTIFICATION NUMBERS

Personal identification numbers (PINs) are a form of remembered information used to authenticate users of electronic funds transfer systems and some other systems. Several phases in the life cycle of PINs are Generation of the PIN, Issuance and delivery of the PIN to users, Validation of the PIN upon entry at a terminal device, Transmission of the PIN across communication lines, Processing of the PIN, Storage of the PIN, Change of the PIN, Replacement of the PIN, Termination of the PIN.

4.9.5 DIGITAL SIGNATURES

A digital signature is a string of O’s and 1’s used to authenticate a user. It is the equivalent of the analog signature that humans use to sign documents. Unlike analog
signatures, however, digital signatures should be impossible to forge. The most common way to implement digital signatures is via public-key cryptosystems. The sender of a message signs the message with their private key and receivers of the message verify the signature by decrypting the message using the sender's public key.

4.9.6 PLASTIC CARDS

Plastic cards are primarily a means of identifying individuals who wish to use a computer system. Controls need to be in place and working to reduce exposures to an acceptable level at a number of phases in the life cycle of plastic cards.

(a) Application by the user for a card

(b) Preparation of the card

(c) Issue of the card

(d) Use of the card

(e) Return of the card

(f) Destruction of the card.

4.9.7 Audit Trail Controls

The audit trail should record all material events that occur within the boundary subsystem. It can be analyzed to search for errors or irregularities. It can also be analyzed for evidence of ineffective or inefficient resource consumption.
4.10 INPUT CONTROLS

4.10.1 INTRODUCTION

Components in the input subsystem are responsible for bringing both data and instructions into the information system. Data can be input into an information system in diverse ways. For example, it can be entered directly into an information system via a keyboard, a touch screen, or a mouse. Alternatively, it can be recorded first on some medium, such as a source document and later keyed into an information system at a terminal or read via some type of optical scanner.

4.10.2 INPUT CONTROLLING METHODS

The type of data input method used in an information system affects asset safeguarding, data integrity, system effectiveness, and system efficiency objectives. For example, as more human intervention is required to input data into an information system, the likelihood of error occurring rises. The different methods of input to the applications are discussed below.
**Figure: 4.11 - Input Methods**

**Source Document Design:** Source documents are used to capture input data, good source document design is important to achieving asset safeguarding, data integrity, system effectiveness, and system efficiency objectives. For example, the choice of a source document's layout and style affects the likelihood of the person completing the source document making an error.

**Data-Entry Screen Design:** If data is keyed into an information system via a terminal, high quality screen design is important to minimizing input errors and to achieving effective and efficient input of data. Data-entry screens should be designed so they are uncluttered and symmetrically balanced.
**Data Codes:** Data codes are used to identify an entity uniquely. Poorly designed data codes cause recording and keying errors. Error rates increase as the code becomes longer, a mix of alphabetic and numeric characters, and unpredictable character sequences are used. The different types of data codes are Serial codes, Bock sequence codes, Hierarchical codes and Association codes.

**Check digit:** A check digit is a redundant digit added to a code that enables the accuracy of other characters in the code to be checked. Because overheads arise from using check digits, they should be used only to verify the accuracy of critical codes—for example, customer numbers or product numbers.

**Batch Controls:** Batching is the process of grouping together transactions that bear some type of relationship to each other. Physical and logical bathes are the regular techniques in use.

**Validation of Data Input:** Four types of validation checks can be exercised over input data

(a) Field checks, which do not depend on the values of other fields in the input record

(b) Record checks, which depend on the values of other fields in the input record

(c) Batch checks, which depend on the characteristics of a batch of input records

(d) File checks, which test whether the characteristics of a file used during input are congruent with the expected characteristics of the file.
**Reporting data Input Errors:** Errors identified by the input validation program should be reported in a clear, concise, courteous, and neutral manner. Errors that cannot be corrected immediately should be written to an error file so the data in error is not lost. Users should be reminded of any errors that they do not clear promptly from the error file.

![Diagram](image)

**Figure 4.12 - Use of an error file for data validation**

**Instructions to information system:** Some of the major ways in which instructions can be entered into an information system are as follows

(a) Menu-driven languages, which ask users to select from a list of options with which they are presented;

(b) Question-answer dialogs, which ask users to respond to questions presented by the application system

(c) Command languages, which require users to recall and initiate instructions for the application system;
(d) Forms-based languages, which require users to specify commands in the context of some input or output form;
(e) Natural languages, which allow users to instruct an application system via freeform input
(f) Direct-manipulation interfaces, which allow users to enter instructions to an application system via direct manipulation of objects on a screen. Each of these methods of instruction input has their strengths and weaknesses in terms of data integrity, system effectiveness, and system efficiency objectives.

**Instruction validation:** Three types of validation checks can be exercised over instruction input are Lexical validation, which evaluates whether commands contain valid commands, Syntactic validation which evaluates whether commands contain a string of valid operations and Semantic validation, which evaluates whether the actions to be invoked by a command are meaningful.

**Audit Trail Controls:** The accounting audit trail in the input subsystem must record the origin, contents and timing of the data and instructions entered into an application system. The operations audit trail in the input subsystem records the resources consumed to process data and instruction input.

**4.11 COMMUNICATION CONTROLS**

**4.11.1 INTRODUCTION**

Components in the communication subsystem are responsible for transporting data among all the other subsystems within a
system and for transporting data to or receiving data from another system. The communication subsystem is becoming an increasingly important component of computer-based information systems.

4.11.2 COMMUNICATION SUBSYSTEM EXPOSURES

The exposures arise in the communication subsystem are as follows

- Data is transported across a communication subsystem can be impaired through attenuation, delay distortion, and noise
- The hardware and software components in a communication subsystem can fail

The communication subsystem can be subjected to passive or active subversive attacks. Passive attacks include unauthorized reading of data and analysis of traffic on communication lines. Subversive attacks include message insertion, message deletion, message modification, altering the order of messages, duplicating messages, disrupting communications and establishing spurious associations within the communication subsystem.

One way to reduce expected losses in the communication subsystem is to choose physical components that have characteristics which make them reliable and that incorporate features or provide controls which mitigate the possible effects of exposures.
4.11.3 TRANSMISSION IMPAIRMENTS

Transmission media can be either bounded or unbounded. Bounded media comprise twisted-pair wire, coaxial cable, and optical fiber. Unbounded media comprise terrestrial and satellite microwave, radio frequency and infrared rays. Transmission media differ in terms of their transmission speed, susceptibility to transmission impairments and susceptibility to passive and active subversive threats.

4.11.4 COMMUNICATION CONSIDERATION CONTROLS

Communication lines: The reliability of data communications can be improved by choosing a private communication line rather than a public line. Public lines use the normal public switching exchange facilities. As a result, users have no control over the lines allocated to them. Private lines undergo a process called conditioning to mitigate the effects of transmission impairments.

Modems: Modems convert binary signals to analog signals and vice versa. They affect the reliability of the communication subsystem in three ways

(a) They increase the speed with which data can be transmitted over a communication line, thereby reducing the overheads associated with controls.

(a) They reduce the number of line errors that occur through distortion through a process called equalization.

(b) They reduce the number of line errors that occur through noise.
Port-protection devices: Port-protection devices are used to mitigate exposures associated with dial-up access to computer systems. They perform the following security functions:

(a) Permit users to make connections to the host computer system only from authorized telephone numbers.
(b) Enforce password protection to the host system.
(c) Maintain an audit trail of all successful and unsuccessful attempts.

Multiplexers and Concentrators: Multiplexing and concentration techniques allow the capacity of a communication line to be used more effectively. They permit multiple low-cost message sources to share a high-cost communication line. They affect system reliability by:

(a) Making more channel capacity available for control purposes.
(b) Providing alternative paths for messages if one path fails.
(c) Making it more difficult for wire tapers to disentangle the myriad of messages passing over a communication line.

Error Detection: Errors that occur on a communication line because of attenuation, distortion or noise must be detected and corrected. Three techniques used to detect errors are loop checks by returning copy of message to sender, parity checks which adds redundant bits to a message that are a function of
the other bits in a message and cyclic redundancy checks which includes mathematical error detection concepts.

**Error Correction:** Two techniques used to correct errors are
(a) Forward error correcting codes, which enable the correct data to be determined if it is received in error.
(b) Retransmission, which involves requesting the sender to retransmit data received in error.

**Flow Controls:** Flow controls are needed to ensure that one node in a network does not flood another node because it transmits data too quickly. Two protocols used to exercise flow control are the stop-and-wait protocol and the sliding-window protocol. The former involves the sender transmitting a frame of data and then waiting for instructions from the receiver before it transmits a further frame. The latter allows frames to be transmitted concurrently with the receiver processing earlier frames that it received. Thus, the sliding-window protocol makes better use of line capacity.

**Link Controls:** In wide area networks, line error controls and flow controls are incorporated into link protocols. If an organization uses a major link protocol like the Higher-level Data Link Control protocol or the Synchronous Data Link Control protocol, reliable error controls and flow controls most likely will be in place and working.
**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. Four types of network topology are used within local area networks. The different topologies are bus topology, tree topology, ring topology, star topology, mesh topology.

**Polling Methods:** Polling techniques establish an order in which nodes can gain access to channel capacity. Two common polling methods are

(a) Centralized polling, in which a master node polls subordinate nodes.

(b) Distributed polling, in which each node takes some responsibility for control over channel access.

**Internetworking Controls:** Internetworking is the process of connecting two or more communication networks together so the users of one network can communicate with the users of another network. Different types of devices are used to connect different networks are bridges, routers and gateways. These devices improve the reliability of the total network because they allow sub networks which are highly reliable.

**Accounting Audit Trail:** The accounting audit trail in the communication subsystem must record the contents of and passage of each message that passes through a network. The operations audit trail in the communication subsystem records the resources consumed to transport data through a network. High-quality test and diagnostic equipment should be available to
monitor the operations of the network. Adequate logs should be maintained to effect prompt recovery when the communication subsystem fails.

4.12 PROCESSING CONTROLS

4.12.1 INTRODUCTION

The processing subsystem is responsible for computing, sorting, classifying, and summarizing data. The major components in the processing subsystem are the central processor on 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.

4.12.2 PROCESSOR CONTROLS

Four types of controls are used to reduce expected losses from errors and irregularities associated with central processors. First, errors in processors can be detected via parity checks or instruction validity checks. If the errors are transient, they can be corrected by attempting to execute failed instructions again.

Second, to prevent irregularities, privileged instructions can be executed only if the processor is in a special supervisor state.

Third, timing controls can be used to prevent the processor remaining in an endless loop because of a program error.
Fourth, processor components can be replicated to allow processing to continue in the event that a processor component fails.

**Error Detection and Correction:** Two types of controls are used to reduce expected losses from errors and irregularities associated with real memory. First, memory errors can be detected via parity checks and Hamming codes. Hamming codes also allow errors to be corrected. Second, access controls, which are implemented via boundary registers, can be used to ensure one process does not gain unauthorized access to the real memory assigned to another process.

**Virtual Memory Controls:** Virtual memory exists when the addressable storage space is larger than the available real memory space. Two types of controls can be exercised over blocks of virtual memory. First, the addressing mechanism should check that the memory reference is within the bounds of the block allocated to the process. Second, an access control mechanism should check to see that the actions a process wants...
to exercise on a block are within its allowed set of privileges.

**Operating System Integrity:** A reliable operating system achieves five goals:

(a) It protects itself from user processes;

(b) It protects users from one another;

(c) It protects users from themselves;

(d) It protects itself from itself; and

(e) It brings operations to an orderly halt in the event of environmental failure

**Operating System Integrity Threats:** There are four types of threats to operating system integrity

(a) Privileged personnel abuse their powers

(b) Possible penetrates deceive privileged personnel into giving them special powers

(c) Special devices are used to detect electromagnetic radiation, emit electromagnetic radiation or wiretap communication lines

(d) Possible penetrates interact with an operating system to determine and exploit a flaw in the system.

Operating system integrity can be breached via two types of covert channel.

Operating system flaws arise for two reasons. First, the access control policy designed for the system is defective.
Second, the access control policy is implemented incorrectly in the operating system.

**Reference Monitors and Kernels:** To improve the design and implementation of the security features in an operating system, reference monitors are sometimes used. A reference monitor is an abstract mechanism that checks each request by a subject to use an object complies with a security policy. A reference monitor is implemented via a security kernel, which is a mechanism supported by hardware, firmware or software.

**Design and Implementation Considerations:** Because operating systems are complex, critical pieces of software, they need to be carefully designed and implemented. Top-down design and structured programming principles should be followed. The system should be designed and specified as a hierarchy of layers corresponding to different levels of abstraction of the functions to be performed.

**Application Software Controls:** Application software can exercise three levels of checks in the processing subsystem:
Field checks, which evaluate whether field overflow or out-of-range values have occurred.

Record checks, which evaluate whether the contents of a field are reasonable or whether a field has the correct sign.

File checks, which employ cross-footing and control totals to check overall processing is accurate and complete.

Reliability of Application software: The reliability of application software can be improved if programmers use good programming style in the software they write. They should handle rounding correctly for required precision with accuracy, minimize human intervention in providing parameter values, should undertake complex numerical calculations and use redundant routines to cross-check the accuracy of complex numerical calculations.

Audit Trail Controls: Of all subsystems, perhaps the most extensive operations audit trail is maintained in the processing subsystem. Logging facilities in the operating system can be used to record resource consumption data, security-sensitive events, hardware malfunctions and user-specified events. Special software is often available to interrogate the operations audit trail.

4.13 DATABASE CONTROLS

4.13.1 INTRODUCTION

The database subsystem is responsible for defining, creating, modifying, deleting, and reading data in an information system.
It maintains declarative data, relating to the static aspects of real-world objects and their associations, and procedural data, relating to the dynamic aspects of real-world objects and their associations. The major components in the database subsystem are the database management system used to manage data, the application programs that perform operations on data, the central processor and primary storage in which operations are performed, and the storage media that maintains the permanent or semi permanent copy of the database.

4.13.2 CONSIDERABLE DATABASE CONTROLS

**Access controls:** Access controls are used in the database subsystem to prevent unauthorized access to and use of data. A discretionary access control policy can be used, which allows users to specify who can access the data they own and what action privileges they have with respect to the data. A mandatory access control policy requires a system administrator to assign security aspects to data that cannot be changed by database users.

**Integrity Controls:** A good database management system will enforce various types of integrity constraints to maintain the accuracy, completeness and uniqueness of instances of the constructs used within the conceptual modeling or data modeling approach used to structure data in the database.

**Distributed database concurrency Controls:** Data integrity can be violated when two processes are allowed concurrent access to a data item. One process could read and update a data item at the same time as another process reads and updates the data item. The effect of one update operation can be lost. Locking
out one process while the other process completes its update can lead to a situation called deadlock in which two processes are waiting for each other to release a data item that the other needs. A widely accepted solution to deadlock is two-phase locking, in which all the data items needed to propagate the effects of a transaction are first obtained and locked from other processes. The data items are not released until all updates on the data items have been completed.

A DEADLOCK SITUATION

Cryptographic Controls: Cryptographic controls can be used to protect the integrity of data in the database. The primary means of encrypting data is block encryption, because use of stream encryption would mean other blocks of data have to be retrieved to decrypt the required data. In the case of portable storage media, encryption can be carried out by a cryptographic device in the controller. The privacy of data is protected if the media is stolen, but one user's data is not protected from access by another user. To protect one user's data from access by another user, cryptographic keys must be assigned to the owner of the data and those users allowed accessing the data.
File Handling Controls: File handling controls are used to prevent accidental destruction of data contained on a storage medium by an operator, user or program. They include internal labels, generation numbers, retention dates, control totals, magnetic tape file protection rings, read-only switches, and external labels.

Accounting Audit Trail: The accounting audit trail in the database subsystem maintains the chronology of events that occur to the database definition or the database itself. It must permit either an implosion operation or an explosion operation. Under implosion, a data item can be traced from its source to the data item it affects. Under explosion, the sequence of events that have occurred to a data item in the database definition or the database can be reconstructed.
Operations Audit Trail: The operations audit trail in the database subsystem maintains the chronology of resource consumption events that affect the database definition or the database. Data administrators and database administrators can use the operations audit trail to determine when the database needs to be reorganized or when the processes that access the database need to be rewritten to improve their efficiency.

Existence Controls: Existence controls are needed to recover the database from five types of failure.
• Application program error
• System software error
• Hardware failure
• Procedural error
• Environmental failure

Existence controls encompass both a backup strategy and a recovery strategy. Recovery strategies take two forms.

(a) Roll forward, whereby the current state of the database is recovered from a previous version.

(b) Rollback, whereby a previous state of the database is recovered from the current state.

**Backup:** The original copy of data is duplicated on secondary storage media which is referred as Backup copy. If the original copy of data gets damaged because of untoward situation, then the backup copy is recovered. The different methods of backup are Grandfather-father-son backup, Dual recording backup, Dumping, Differential files or Shadow Paging etc.

**Logging:** Logging involves recording a transaction that changes the database or an image of the record changed by an update action. Different types of logs are transaction logs, Before image logs and After image logs.
4.14 OUTPUT CONTROLS

4.14.1 INTRODUCTION

The output subsystem provides functions that determine the content of data that will be provided to users, the ways data will be formatted and presented to users and the ways data will be prepared for and routed to users. Best way to represent data is through lattice tables which gives detailed distribution of output to users.

4.14.2 CONSIDERABLE OUTPUT CONTROLS

INFEERENCE CONTROLS: Inference controls are used in the output subsystem to prevent compromise of statistical databases from which users can obtain only aggregate statistics rather than the values of individual data items. They are used to prevent Positive compromise, Negative compromise, exact compromise, approximate compromise.

RESTRICTION CONTROLS: One form of inference controls is restriction controls, which limit the set of responses that will be provided to users to try to protect the confidentiality of data about persons in the database. They can take various forms. For example, they might not provide a response to users if their query on the database results in smaller than a certain number of persons having attribute values that satisfy the query.

PERTURBATION CONTROLS: These controls introduce some type of noise into the statistics calculated on the basis of records retrieved from the database. They can be exercised on the records used as input to a statistical function. For example,
results can be rounded up and down to the nearest integer multiple of a fixed, rounding base—say, multiples of five.

**BATCH OUTPUT PRODUCTION AND DISTRIBUTION CONTROLS:** Batch output is output that is produced at some operations facility and subsequently distributed to the custodians or users of the output. Controls need to be established over the production and distribution of batch output to ensure that accurate, complete and timely output is provided only to authorized custodians and users.

**STATIONERY SUPPLIES STORAGE CONTROLS:** Controls can be exercised over various phases in the production and distribution of batch output—for example, securing the storage of any special stationery used to produce batch output, ensuring that only authorized users are permitted to execute batch report programs, ensuring that the contents of spooling/printer files cannot be altered, preventing unauthorized parties from viewing the contents of confidential reports as they are printed, collecting reports promptly to prevent their loss and shredding batch output when it is no longer required.

**REPORT PROGRAM EXECUTION CONTROLS:** Batch output reports can be designed to facilitate exercising effective and efficient controls over them. For example, the title page of a batch output report should show the distribution list for the report and the person to contact if operational problems are encountered in producing the report. Similarly, the detail pages should contain page numbers so loss of or unauthorized removal of pages from the report can be detected.
AUDIT TRAIL CONTROLS: The output subsystem should maintain the chronology of events that occur from the time the content of output is being assimilated until the time users complete their disposal of output because it no longer should be retained.