CHAPTER 3

INFORMATION SYSTEMS AND ITS COMPONENTS

LEARNING OUTCOMES

After reading this chapter, you will be able to-

❐ Comprehend the knowledge about various components of an Information System and its working.

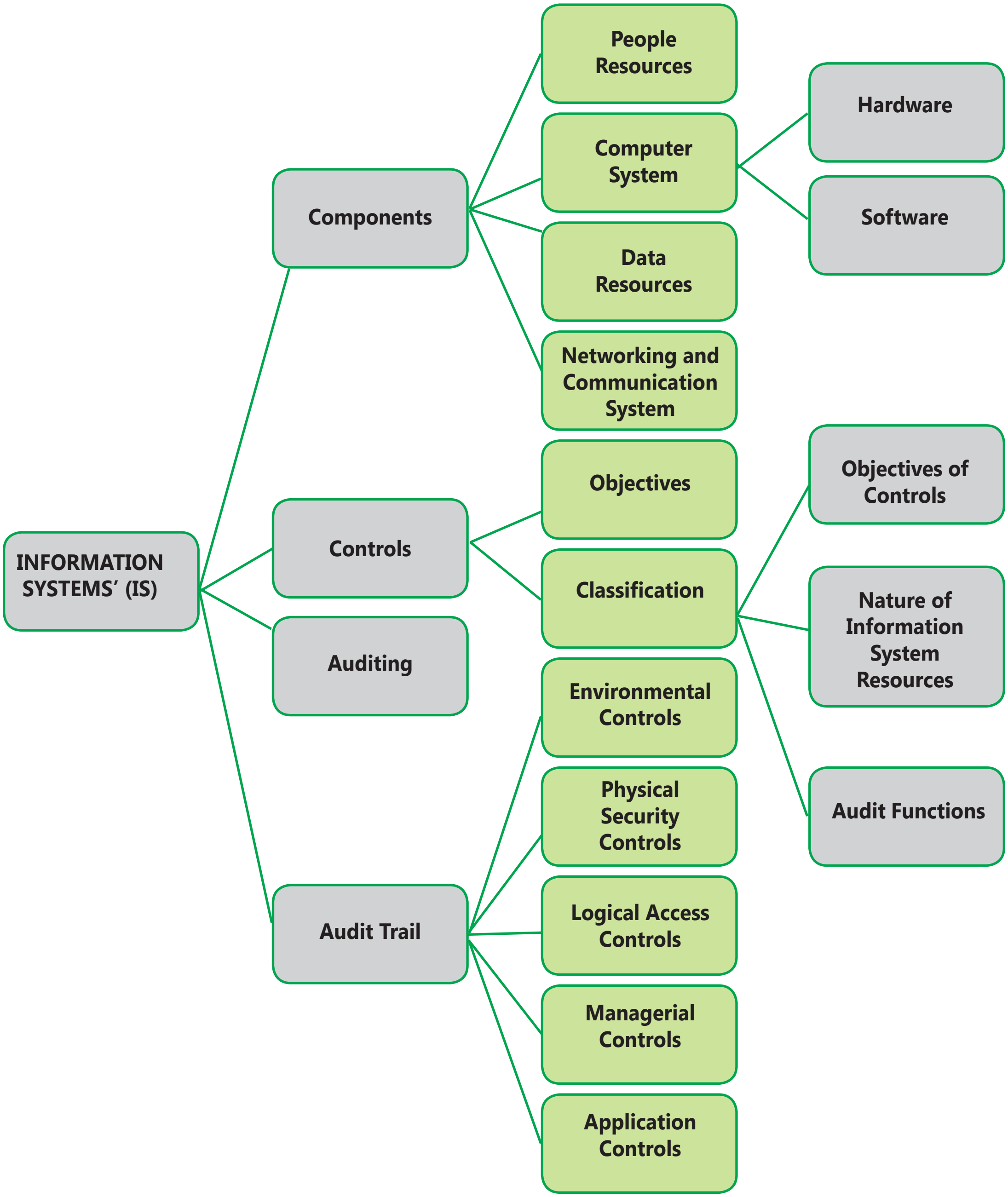
❐ Appreciate nuances of Application Systems, Operating Systems, Database Systems, Networking and Communication Systems.

❐ Grasp various types of threats and their mitigating controls to minimize the impact.

❐ Understand types of controls and audit aspects of various systems.

❐ Comprehend about an organization structure and individual roles and responsibilities.

CHAPTER OVERVIEW



3.1 INTRODUCTION

We are living in a world where we are constantly connected as individuals while some developing and under developed countries are still progressing in terms of internet and mobile devices reach to its masses. The world however has moved on from connection amongst individuals to connection amongst systems. We now have systems that are constantly exchanging information about various things and even about us. This inter-networking of physical devices, vehicles, smart devices, embedded electronics, software, sensors or any such device is often referred to as IoT (Internet of Things).

What is interesting about various emerging technologies is that at its core we have some key elements, namely, Operating System, Application, Database and Networking. In this chapter, we are going to explore each of those key elements.

3.2 INFORMATION SYSTEMS

Information: First of all, we should be able to distinguish between Data and Information. Data is a raw fact and can take the form of a number or statement such as a date or a measurement. It is necessary for businesses to put in place procedures to ensure data have been processed so that they are meaningful. This requires a process that is used to produce information which involves collecting data and then subjecting them to a transformation process in order to create information. Some examples of information include aggregating which summarizes data by such means as taking an average value of a group of numbers. Sorting organizes data so that items are placed in a particular order, for example listing orders by delivery date etc.

System: The system can be defined as "a group of mutually related, cooperating elements with a defined boundary; working on reaching a common goal by taking inputs and producing outputs in organized transformation process."

Not every system has a single goal and often a system contains several subsystems with sub goals, all contributing to meeting the overall system goal. For example, the finance, operations and marketing areas of an organization should all have goals which together help to achieve overall corporate objectives. In systems, data are used as the input for a process that creates information as an output. To monitor the performance of the system, some kind of feedback mechanism is required. In addition, control must be exerted to correct any problems that occur and ensure that the system is fulfilling its purpose. There are thus five components of a generic system in terms of **Input, Process, Output, Feedback and Control.**

In the extensive sense, the term Information Systems (IS) refers to the interaction between processes and technology.

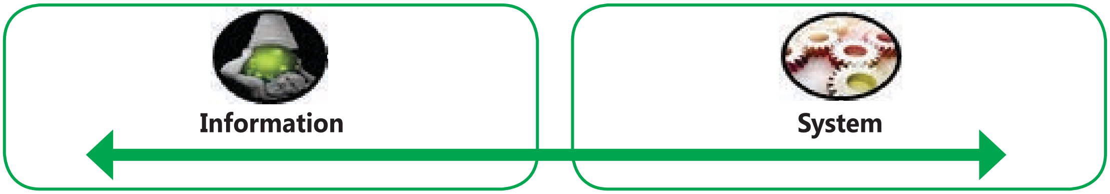


Fig. 3.2.1: Bifurcation of a Terminology 'Information' and 'System'

From the Fig. 3.2.1, we can see how Information and System are interlinked with one another.

Information System: Information System (IS) is a combination of people, hardware, software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose. The system needs inputs from user (key in instructions and commands, typing, scanning) which will then be processed (calculating, reporting) using technology devices such as computers, and produce output (printing reports, displaying results) that will be sent to another user or other system via a network and a feedback method that controls the operation.

In general, any specific Information System aims to support operations, management and decision-making.

The main aim and purpose of each Information System is to convert the data into information which is useful and meaningful. An Information System depends on the resources of people (end users and IS specialists), hardware (machines and media), software (programs and procedures), data (data and knowledge bases), and networks (communications media and network support) to perform input, processing, output, storage, and control activities that transform data resources into information products. This information system model highlights the relationships among the components and activities of information systems. It also provides a framework that emphasizes four major concepts that can be applied to all types of information systems. An Information System model comprises of following steps:

- **Input:** Data is collected from an organization or from external environments and converted into suitable format required for processing.
- **Process:** A process is a series of steps undertaken to achieve desired outcome or goal. Information Systems are becoming more and more integrated with organizational processes, bringing more productivity and better control to those processes. But simply automating activities using technology is not enough. Businesses looking to effectively utilize Information Systems do more. Using technology to manage and improve processes, both within a company and externally with suppliers and customers, is the goal. Technology buzzwords such as business process re-engineering, business process management and

enterprise resource planning all must do with continued improvement of these business processes and the integration of technology with them. Businesses hoping to gain an advantage over their competitors are highly focused on this component of Information Systems.

- **Output:** Then information is stored for future use or communicated to user after application of respective procedure on it.

Three basics activities of an information system that are defined above, helps enterprise in making decisions, control operations, analyse problems and create new products or services as an output, as shown in Fig. 3.2.2. Apart from these activities, information systems also need feedback that is returned to appropriate members of the enterprises to help them to evaluate at the input stage.

Some of the important characteristics of Computer Based Information Systems are given as follows:

- All systems work for predetermined objectives and the system is designed and developed accordingly.
- In general, a system has several interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
- If one subsystem or component of a system fails; in most of the cases, the whole system does not work. However, it depends on 'how the subsystems are interrelated'.
- The way a subsystem works with another subsystem is called interaction. The different subsystems interact with each other to achieve the goal of the system.
- The work done by individual subsystems is integrated to achieve the central goal of the system. The goal of individual subsystem is of lower priority than the goal of the entire system.

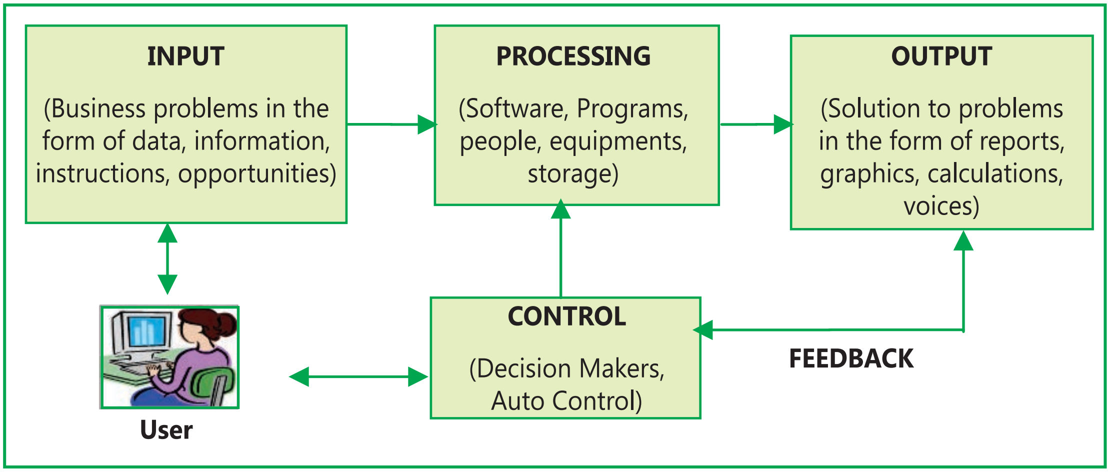

INPUT
(Business problems in the form of data, information, instructions, opportunities)
PROCESSING
(Software, Programs, people, equipments, storage)
OUTPUT
(Solution to problems in the form of reports, graphics, calculations, voices)
User
CONTROL
(Decision Makers, Auto Control)
FEEDBACK

Fig. 3.2.2: Functions of Information Systems

Technology can be thought of as application of scientific knowledge for tactical purposes. From the invention of the wheel to the harnessing of electricity for artificial lighting, technology has played an important role in our lives in so many ways that we tend to take it for granted.

3.3 COMPONENTS OF INFORMATION SYSTEMS

With the help of information systems, enterprises and individuals can use computers to collect, store, process, analyse, and distribute information. There are different types of information systems, i.e. Manual (paper and pencil) information system, Informal (word to mouth) information system, Formal (written procedures) information system and Computer based information system. This chapter mainly focuses on computer based information system. A Computer Based Information system is a combination of people, IT and business processes that helps management in taking important decisions to carry out the business successfully.

Information Systems are networks of hardware and software that people and organizations use to create, collect, filter, process and distribute data. Information Systems are interrelated components working together to collect, process, store and disseminate information to support decision-making, coordination, control, analysis and visualization in an organization. An Information System comprise of **People, Hardware, Software, Data** and **Network** for communication support shown in Fig. 3.3.1.

Here, people mean the IT professionals i.e. system administrator, programmers and end users i.e. the persons, who can use hardware and software for retrieving the desired information. The hardware means the physical components of the computers i.e. server or smart terminals with different configurations like corei3/corei5/corei7 processors etc. and software means the system software (different types of operating systems e.g. UNIX, LINUX, WINDOWS etc.), application software (different type of computer programs designed to perform specific task) and utility software (e.g. tools). The data is the raw fact, which may be in the form of database. The data may be alphanumeric, text, image, video, audio, and other forms. The network means communication media (Internet, Intranet, Extranet etc.).

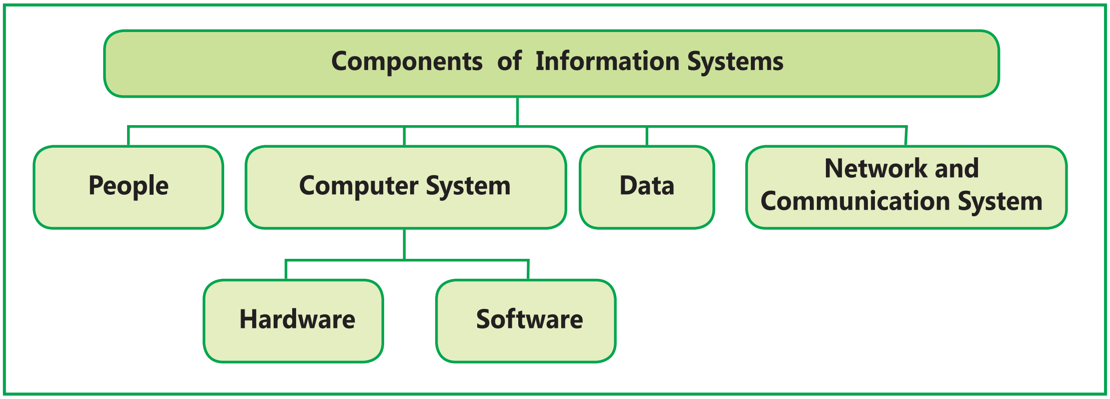

Components of Information Systems
People
Computer System
Data
Network and Communication System
Hardware
Software

Fig. 3.3.1: Components of Information Systems

3.3.1 People Resources

While thinking about Information Systems, it is easy to get too focused on the technological components and forget that we must look beyond these tools at the whole picture and try to understand how technology integrates into an organization. A focus on people involved in Information Systems is the next step. From the helpdesk to the system programmers all the way up to the Chief Information Officer (CIO), all of them are essential elements of the information systems.

People are the most important element in most Computer-based Information Systems. The people involved include users of the system and information systems personnel, including all the people who manage, run, program, and maintain the system.

In the ever-changing world, innovation is the only key, which can sustain long-run growth. More and more firms are realizing the importance of innovation to gain competitive advantage. Accordingly, they are engaging themselves in various innovative activities. Understanding these layers of information system helps any enterprise grapple with the problems it is facing and innovate to perhaps reduce total cost of production, increase income avenues and increase efficiency of systems.

3.3.2 Computer System – Hardware and Software

Computer System: This can be thought of as combination of **Hardware** and **Software**.

Hardware: Information Systems hardware is the part of Information Systems that you can touch-the physical components of technology. Computers, keyboards, hard drives, iPads and flash drives are all examples of Information Systems hardware.

Software: Software is a set of instructions that tells the hardware what to do. Software is not tangible it cannot be touched. When programmers create software, what they are really doing is simply typing out lists of instructions that tell the hardware what to execute. There are several categories of software, with the two main categories being operating system software, which makes the hardware usable and application software, which does something useful. Examples of operating system software: Microsoft Windows, LINUX, etc. Examples of application software: Microsoft Excel, Adobe Photoshop, Microsoft PowerPoint etc.

I. Hardware

Hardware is the tangible portion of our computer systems; something we can touch and see. It basically consists of devices that perform the functions of input, processing, data storage and output activities of the computer. Typical hardware architecture is shown in Fig. 3.3.2.

(i) **Input Devices** are devices through which we interact with the systems and include devices like Keyboard, Mouse and other pointing devices, Scanners & Bar Code, MICR readers, Webcams, Microphone and Stylus/ Touch Screen. Keyboard helps us with text based input, Mouse helps us in position based input, Scanners

& Webcams help in image based input and Microphone helps us in voice based input.

(ii) **Processing Devices** include computer chips that contain the Central Processing Unit and main memory. The Central Processing Unit (CPU or microprocessor) is the actual hardware that interprets and executes the program (software) instructions and coordinates how all the other hardware devices work together. The CPU is built on a small flake of silicon and can contain the equivalent of several million transistors. We can think of transistors as switches which could be "ON" or "OFF" i.e., taking a value of 1 or 0. The processor or CPU is like the brain of the computer. The main function of CPU is to execute programs stored in memory. It consists of three functional units:

- **Control Unit (CU):** CU controls the flow of data and instruction to and from memory, interprets the instruction and controls which tasks to execute and when.
- **Arithmetic and Logical Unit (ALU):** Performs arithmetic operations such as addition, subtraction, multiplication, and logical comparison of numbers: Equal to, Greater than, Less than, etc.
- **Registers:** These are high speed memory units within CPU for storing small amount of data (mostly 32 or 64 bits). Registers could be:
  - **Accumulators:** They can keep running totals of arithmetic values.
  - **Address Registers:** They can store memory addresses which tell the CPU as to where in the memory an instruction is located.
  - **Storage Registers:** They can temporarily store data that is being sent to or coming from the system memory.
  - **Miscellaneous:** These are used for several functions for general purpose.

(iii) **Data Storage Devices** refers to the memory where data and programs are stored. Various types of memory techniques/devices are given as follows:

(a) **Internal Memory:** This includes Processer Registers and Cache Memory.

- **Processor Registers:** Registers are internal memory within CPU, which are very fast and very small.
- **Cache Memory:** There is a huge speed difference between Registers and Primary Memory. To bridge these speed differences, we have cache memory. Cache (pronounced as cash) is a smaller, faster memory, which stores copies of the data from the most frequently used main memory locations so that Processor/Registers can access it more rapidly than main memory. It is the property of locality of

reference, which allows improving substantially the effective memory access time in a computer system.

(b) **Primary Memory/Main Memory:** These are devices in which any location can be accessed by the computer's processor in any order (in contrast with sequential order). These are primarily of two types:

- **Random Access Memory (RAM)**
  - Volatile in nature means Information is lost as soon as power is turned off.
  - This is Read Write memory whose main purpose is to hold program and data while they are in use. Information can be read as well as modified.
  - It is responsible for storing the instructions and data that the computer is using at that present moment.
- **Read Only Memory (ROM)**
  - This is non-volatile in nature (contents remain even in absence of power).
  - Usually, these are used to store small amount of information for quick reference by CPU.
  - Information can be read not modified.
  - Generally used by manufacturers to store data and programs like translators that is used repeatedly.

(c) **Secondary Memory:** CPU refers to the main memory for execution of programs, but these main memories are volatile in nature and hence cannot be used to store data on a permanent basis in addition to being small in storage capacity. The secondary memories are available in bigger sizes, thus programs and data can be stored on secondary memories.

Secondary storage differs from primary storage in that it is not directly accessible by the CPU. The computer usually uses its input/output channels to access secondary storage and transfers the desired data using intermediate area in primary storage. Secondary storage does not lose the data when the device is powered down: it is non-volatile.

The features of secondary memory devices are non-volatility (contents are permanent in nature), greater capacity (they are available in large size), greater economy (the cost of these is lesser compared to register and RAMs) and slow speed (slower in speed compared to registers or primary storage). Storage devices could differ amongst each other in terms of speed and access time, cost/portability, capacity and type of access.

Based on these parameters most common forms of secondary storage are: USB Pen Drives, Floppy drive, Hard Drive, CD, DVD and Smart cards. Fig. 3.3.2 provides diagrammatic representation of computer memory.

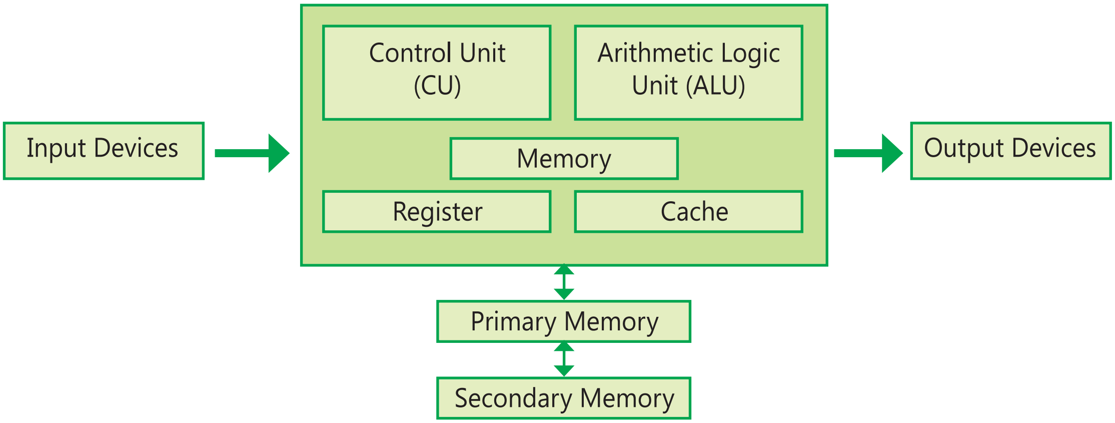


Fig. 3.3.2: Hardware Architecture

(d) **Virtual Memory:** Virtual Memory is in fact not a separate device but an imaginary memory area supported by some operating systems (for example, Windows) in conjunction with the hardware. If a computer lacks the Random-Access Memory (RAM) needed to run a program or operation, Windows uses virtual memory to compensate. Virtual memory combines computer's RAM with temporary space on the hard disk. When RAM runs low, virtual memory moves data from RAM to a space called a paging file. Moving data to and from the paging file frees up RAM to complete its work. Thus, Virtual memory is an allocation of hard disk space to help RAM and depicted in the Fig. 3.3.3.

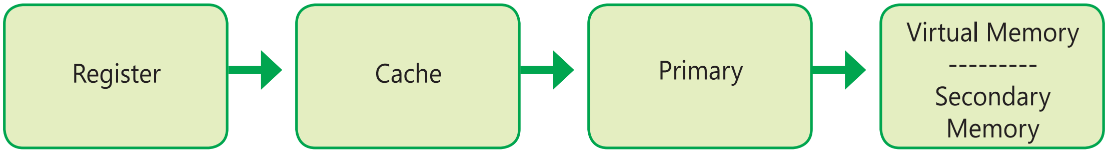


Fig. 3.3.3: Memory Techniques/Devices

(iv) **Output Devices:** Computer systems provide output to decision makers at all levels in an enterprise to solve business problems, the desired output may be in visual, audio or digital forms. Output devices are devices through which system responds. Visual output devices like, a display device visually conveys text, graphics, and video information. Information shown on a display device is called soft copy because the information exists electronically and is displayed for a temporary period. Display devices include CRT monitors, LCD monitors and displays, gas plasma monitors, and televisions.

Some types of output are textual, graphical, tactile, audio, and video.

- **Textual output** comprises of characters that are used to create words, sentences, and paragraphs.
- **Graphical outputs** are digital representations of non-text information such as drawings, charts, photographs, and animation.
- **Tactile output** such as raised line drawings may be useful for some individuals who are blind.
- **Audio output** is any music, speech, or any other sound.
- **Video output** consists of images played back at speeds to provide the appearance of full motion.

Most common examples of output devices are Speakers, Headphones, Screen (Monitor), Printer, Voice output communication aid, Automotive navigation system, Video, Plotter, Wireless etc.

II. Software

Software is defined as a set of instructions that tell the hardware what to do. Software is created through the process of programming. Without software, the hardware would not be functional. Software can be broadly divided into two categories: **Operating Systems Software** and **Application Software** as shown in the Fig. 3.3.4. Operating systems manage the hardware and create the interface between the hardware and the user. Application software is the category of programs that do some processing/task for the user.

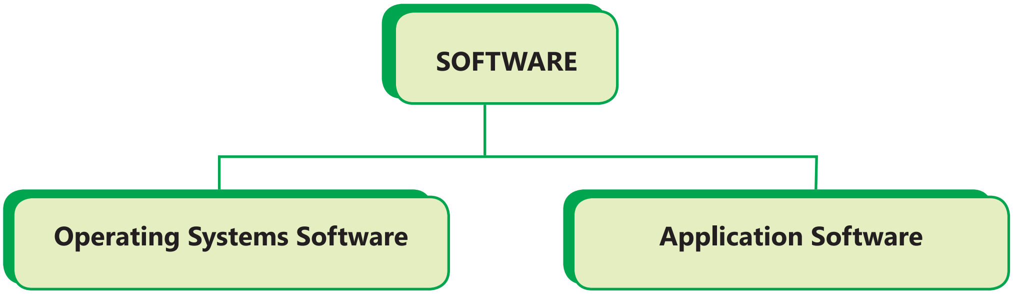


Fig. 3.3.4: Types of Software

(a) Operating Systems Software

An **Operating System (OS)** is a set of computer programs that manages computer hardware resources and acts as an interface with computer applications programs. The operating system is a vital component of the system software in a computer system. Application programs usually require an operating system to function that provides a convenient environment to users for executing their programs. Computer hardware with operating system can thus be viewed as an extended machine, which is more powerful and easy to use. Some prominent Operating systems used nowadays are Windows 7, Windows 8, Linux, UNIX, etc.

All computing devices run an operating system. For personal computers, the most popular operating systems are Microsoft's Windows, Apple's OS X, and different versions of Linux. Smart phones and tablets run operating systems as well, such as Apple's iOS, Google Android, Microsoft's Windows Phone OS, and Research in Motion's Blackberry OS.

A variety of activities are executed by Operating systems which include:

- **Performing hardware functions:** Application programs to perform tasks must obtain input from keyboards, retrieve data from disk & display output on monitors. Achieving all this is facilitated by operating system. Operating system acts as an intermediary between the application program and the hardware.
- **User Interfaces:** An important function of any operating system is to provide user interface. If we remember DOS days, it had a command based User Interface (UI) i.e. text commands were given to computer to execute any command. But today we are more used to Graphic User Interface (GUI) which uses icons & menus like in the case of Windows. So, how we interface with our system will be provided by Operating system.
- **Hardware Independence:** Every computer could have different specifications and configurations of hardware. If application developer would have to rewrite code for every configuration s/he would be in a big trouble. Fortunately, we have operating system, which provides Application Program Interfaces (API), which can be used by application developers to create application software, thus obviating the need to understand the inner workings of OS and hardware. Thus, OS gives us hardware independence.
- **Memory Management:** Memory Management features of Operating System allow controlling how memory is accessed and maximize available memory & storage. Operating systems also provides Virtual Memory by carving an area of hard disk to supplement the functional memory capacity of RAM. In this way, it augments memory by creating a virtual RAM.
- **Task Management:** Task Management feature of Operating system helps in allocating resources to make optimum utilization of resources. This facilitates a user to work with more than one application at a time i.e. multitasking and allows more than one user to use the system i.e. time sharing.
- **Networking Capability:** Operating systems can provide systems with features & capabilities to help connect computer networks. Like Linux & Windows 8 give us an excellent capability to connect to internet.
- **Logical Access Security:** Operating systems provide logical security by

establishing a procedure for identification & authentication using a User ID and Password. It can log the user access thereby providing security control.

- **File management:** The operating system keeps a track of where each file is stored and who can access it, based on which it provides the file retrieval.

(b) Application Software

As the personal computer proliferated inside organizations, control over the information generated by the organization began splintering. Say the customer service department creates a customer database to keep track of calls and problem reports, and the sales department also creates a database to keep track of customer information. Which one should be used as the master list of customers? As another example, someone in sales might create a spreadsheet to calculate sales revenue, while someone in finance creates a different one that meets the needs of their department. However, it is likely that the two spreadsheets will come up with different totals for revenue. Which one is correct? And who is managing all this information? To resolve these issues, various specific purpose applications were created.

Application software includes all that computer software that cause a computer to perform useful tasks beyond the running of the computer itself. It is a collection of programs which address a real-life problem of its end users which may be business or scientific or any other problem. The different types of application software are as follows:

- **Application Suite:** Has multiple applications bundled together. Related functions, features and user interfaces interact with each other. E.g. MS Office 2010 which has MS Word, MS Excel, MS Access, etc.
- **Enterprise Software:** Addresses an enterprise's needs and data flow in a huge distributed environment. E.g. ERP Applications like SAP.
- **Enterprise Infrastructure Software:** Provides capabilities required to support enterprise software systems. E.g. email servers, Security software.
- **Information Worker Software:** Addresses individual needs required to manage and create information for individual projects within departments. E.g. Spreadsheets, CAAT (Computer Assisted Audit Tools) etc.
- **Content Access Software:** Used to access contents and addresses a desire for published digital content and entertainment. E.g. Media Players, Adobe Digital etc.
- **Educational Software:** Holds contents adopted for use by students. E.g. Examination Test CDs
- **Media Development Software:** Addresses individual needs to generate and print electronic media for others to consume. E.g. Desktop Publishing, Video Editing etc.

Some of the most popular and widely accepted benefits of Application Software are as follows:

- **Addressing User needs:** Their single biggest advantage is that it meets the exact needs of the user. Since it is designed specifically with one purpose in mind, the user knows that he should use the specific software to accomplish his task.
- **Less threat from virus:** The threat of viruses invading custom-made applications is very small, since any business that incorporates it can restrict access and can come up with means to protect their network as well.
- **Regular updates:** Licensed application software gets regular updates from the developer for security reasons. Additionally, the developer also regularly sends personnel to correct any problems that may arise from time to time.

There are certain disadvantages of such software as well and these are given as follows:

- **Development is costly:** Developing application software designed to meet specific purposes can prove to be quite costly for developers.
- **Infection from Malware:** If application software is used commonly by many people and shared online, it carries a highly real threat of infection by a computer virus or other malicious programs.

Application Areas of Computer Based Applications

Major areas of computer based applications are finance and accounting, marketing and sales, manufacturing, inventory/stock management, Human Resource Management etc., which are given as follows:

1. **Finance and Accounting –** The main goal of this subsystem (considering Business functions as whole system) is to ensure the financial viability of the organization, enforce financial discipline and plan and monitor the financial budget. It also helps in forecasting revenues, determining the best resources and uses of funds and managing other financial resources. Typical sub-application areas in finance and accounting are -Financial accounting; General ledger; Accounts receivable/ payable; Asset accounting; Investment management; Cash management; Treasury management; Fund management and Balance sheet.
2. **Marketing and Sales –** Marketing and sales activities have a key role for running a business successfully in a competitive environment. The objective of this subsystem is to maximize the sales and ensure customer satisfaction. The marketing system facilitates the chances of order procurement by marketing the products of the company, creating new customers and advertising the products. The sales department may use an order processing system to keep the status and track of orders, generate bills for the orders executed and delivered to the customer, strategies for rendering services during warranty period and beyond, analyzing the sales data by category such as by region, product, sales manor

sales value. The system may also be used to compute commissions for dealers or salesmen and thus helps the corporate managers to take decisions in many crucial areas.

3. **Production or Manufacturing –** The objective of this subsystem is to optimally deploy man, machine and material to maximize production or service. The system generates production schedules and schedules of material requirements, monitors the product quality, plans for replacement or overhauling the machinery and helps in overhead cost control and waste control.

4. **Inventory /Stores Management-** The inventory management system is designed with a view to keeping the track of materials in the stores. The system is used to regulate the maximum and minimum level of stocks, raise alarm at danger level stock of any material, give timely alert for re-ordering of materials with optimal re-order quantity and facilitate various queries about inventory like total inventory value at any time, identification of important items in terms stock value (ABC analysis), identification most frequently moving items (XYZ analysis) etc. Similarly, well-designed inventory management system for finished goods and semi-finished goods provides important information for production schedule and marketing/sales strategy.

5. **Human Resource Management-** Human resource is the most valuable asset for an organization. Utilization of this resource in the most effective and efficient way is an important function for any enterprise. Effective and efficient utilization of manpower in a dispute-free environment in this key functional area ensures to facilitate disruption free and timely services in business. Human Resource Management System (HRMS) aims to achieve this goal. Skill database maintained in HRM system, with details of qualifications, training, experience, interests etc. helps management for allocating manpower to right activity at the time of need or starting a new project. This system also keeps track of employees' output or efficiency. Administrative functions like keeping track of leave records or handling other related functions are also included HRM system. An HRM system may have the following modules – Personnel administration; Recruitment management; Travel management; Benefit administration; Salary administration; Promotion management etc.

3.3.3 Data Resources

You can think of data as a collection of facts. For example, your street address, the city you live in a new phone number are all pieces of data. Like software, data is also intangible. By themselves, pieces of data are not very useful. But aggregated, indexed and organized together into a database, data can become a powerful tool for businesses. For years' business houses, have been gathering information with regards to customers, suppliers, business partners, markets, cost, price movement and so on. After collection of information for years companies have now started analyzing this information and creating important insights out of data. Data is now helping companies to create strategy for future. This is precisely the reason why we have started hearing a lot about data analytics in past few years.

- **Data:** Data are the raw bits and pieces of information with no context. Data can be quantitative or qualitative. Quantitative data is numeric, the result of a measurement, count, or some other mathematical calculation. Qualitative data is descriptive. "Ruby Red," the color of a 2013 Ford Focus, is an example of qualitative data. A number can be qualitative too: if I tell you my favorite number is 5, that is qualitative data because it is descriptive, not the result of a measurement or mathematical calculation.

  By itself, data is not that useful. For it to be useful, it needs to be given context. Returning to the example above, if I told you that "15, 23, 14, and 85" are the numbers of students that had registered for upcoming classes that would-be information. By adding the context – that the numbers represent the count of students registering for specific classes – I have converted data into information.

  Once we have put our data into context, aggregated and analyzed it, we can use it to make decisions for our organization. We can say that this consumption of information produces knowledge. This knowledge can be used to make decisions, set policies, and even spark innovation.

  The final step up the information ladder is the step from knowledge (knowing a lot about a topic) to wisdom. We can say that someone has wisdom when they can combine their knowledge and experience to produce a deeper understanding of a topic. It often takes many years to develop wisdom on a particular topic. This is the area covered by Artificial Intelligence & Machine Learning along with Deep Networks are being used.

- **Database:** The goal of many information systems is to transform data into information to generate knowledge that can be used for decision making. To do this, the system must be able to take data, put the data into context, and provide tools for aggregation and analysis. A database is designed for just such a purpose. A database is an organized collection of related information. It is called an organized collection because in a database all data is described and associated with other data. All information in a database should be related as well; separate databases should be created to manage unrelated information. For example, a database that contains information about students should not also hold information about company stock prices. Databases are not always digital – a filing cabinet, for instance, might be considered a form of database. For the purposes of this text, we will only consider digital databases.

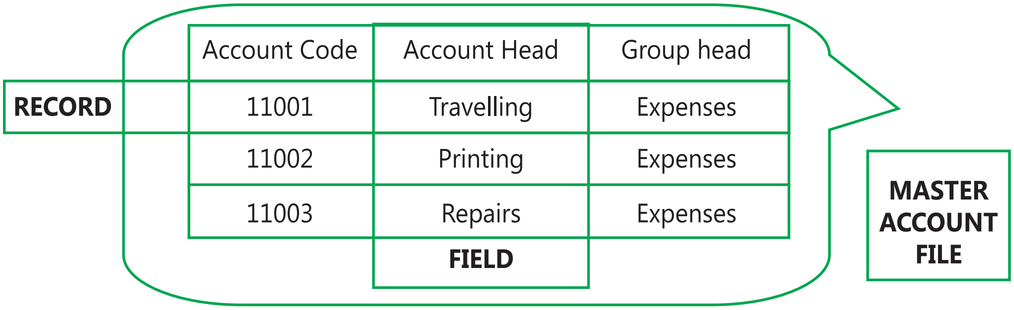
- **Database Management Systems (DBMS):** To achieve the above objectives, we use Data Base Management System. Let's think of a DBMS as basically just a computerized record keeping. Database is just an electronic filing cabinet i.e., a collection of computerized data files. Even this simple system helps us do various operations on the files, such as:
  - o Adding new files to database,
  - o Deleting existing files from database,
  - o Inserting data in existing files,
  - o Modifying data in existing files,
  - o Deleting data in existing files, and
  - o Retrieving or querying data from existing files.

DBMS may be defined as a software that aid in organizing, controlling and using the data needed by the application programme. They provide the facility to create and maintain a well-organized database. Applications access the DBMS, which then accesses the data. Commercially available Data Base Management Systems are Oracle, MySQL, SQL Servers and DB2 etc. DBMS packages generally provide an interface to view and change the design of the database, create queries, and develop reports. Most of these packages are designed to work with a specific type of database, but generally are compatible with a wide range of databases.

Microsoft Access and Open Office Base are examples of personal database-management systems. These systems are primarily used to develop and analyze single-user databases. These databases are not meant to be shared across a network or the Internet, but are instead installed on a device and work with a single user at a time.

- **Database Models:** Databases can be organized in many ways, and thus take many forms. A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized and manipulated. Let's now look at the database model hierarchy. Hierarchy of database is as under:
  - o **Database:** This is a collection of Files.
  - o **File:** This is a collection of Records.
  - o **Record:** This is a collection of Fields.
  - o **Field:** This is a collection of Characters.
  - o **Characters:** These are a collection of Bits.

This hierarchy is shown in the Fig. 3.3.5:



Account Code	Account Head	Group head
11001	Travelling	Expenses
11002	Printing	Expenses
11003	Repairs	Expenses

Fig. 3.3.5: Hierarchy of Databases

Some prominent database models are as follows:

(i) Hierarchical Database Model,

(ii) Network Database Model,

(iii) Relational Database Model, and

(iv) Object Oriented Database Model

A. Hierarchical Database Model: In a **Hierarchical Database Model**, records are logically organized into a hierarchy of relationships. A hierarchically structured database is arranged logically in an inverted tree pattern. For example, an equipment database, diagrammed in Fig. 3.3.6 may have building records, room records, equipment records, and repair records. The database structure reflects the fact that repairs are made to equipment located in rooms that are part of buildings.

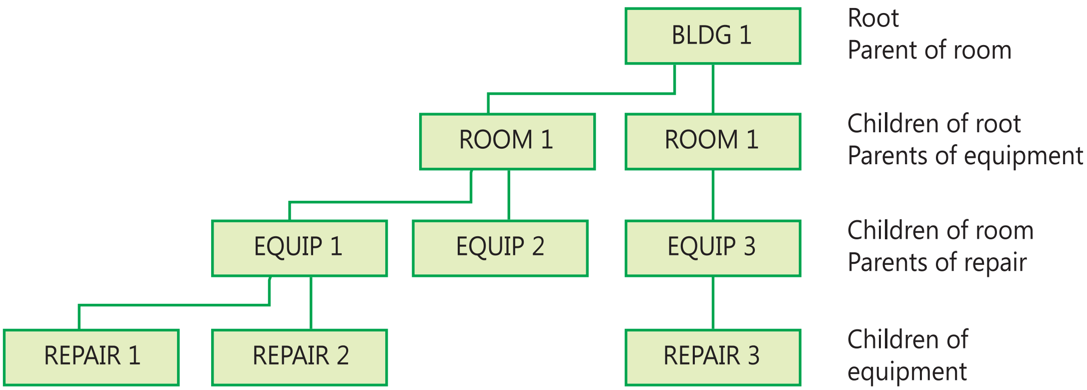


Fig. 3.3.6: Hierarchical Database Model

All records in hierarchy are called **Nodes.** Each node is related to the others in a parent-child relationship. Each parent record may have one or more child records, but no child record may have more than one parent record. Thus, the hierarchical data structure implements one-to-one and one-to-many relationships.

The top parent record in the hierarchy is called the **Root Record**. In this example, building records are the root to any sequence of room, equipment, and repair records. Entrance to this hierarchy by the database management system is made through the root record i.e., building. Records that "own" other records are called **Parent Records.** For example, room records are the parents of equipment records. Room records are also children of the parent record, building. There can be many levels of node records in a database.

B. Network Database Model: The network model is a variation on the hierarchical model, to the extent that it is built on the concept of multiple branches (lower-level structures) emanating from one or more nodes (higher-level structures), while the model differs from the hierarchical model in that branches can be connected to multiple nodes. The network model can represent redundancy in data more efficiently than in the hierarchical model.

A network database structure views all records in sets. Each set is composed of an owner record and one or more member records. However, unlike the hierarchical mode, the network model also permits a record to be a member of more than one set at one time. The network model would permit the equipment records to be the children of both the room records and the vendor records. This feature allows the network model to implement the many-to-one and the many-to-many relationship types.

Network databases generally implement the set relationships by means of pointers that directly address the location of a record on disk. This gives excellent retrieval performance, at the expense of operations such as database loading and reorganization.

For example, suppose that in our database, it is decided to have the following records: repair vendor records for the companies that repair the equipment, equipment records for the various machines we have, and repair invoice records for the repair bills for the equipment. Suppose four repair vendors have completed repairs on equipment items 1,2,3,4,5,6,7 and 8. These records might be logically organized into the sets shown in Fig. 3.3.7.

Notice these relationships:

(i) Repair Vendor 1 record is the owner of the Repair Invoice 1 record. This is a one-to-one relationship.

(ii) Repair Vendor 2 record is the owner of the Repair Invoice 2 and 3 records. This is a one-to-many relationship.

(iii) Repair Vendor 3 record is the owner of Repair Invoice 4 and 5 records, and the Equipment 7 record owns both the Repair Invoice 5 and 6 records because it was fixed twice by different vendors. Because many equipment records can own many Repair Invoice records, these database records represent a many-to-many relationship.

(iv) Equipment 6 record does not own any records now because it is not required to be fixed yet.

(v) Equipment 7 and 8 own Repair Invoice 6 because the repairs to both machines were listed on the same invoice by Repair Vendor 4. This illustrates the many-to-one relationship.

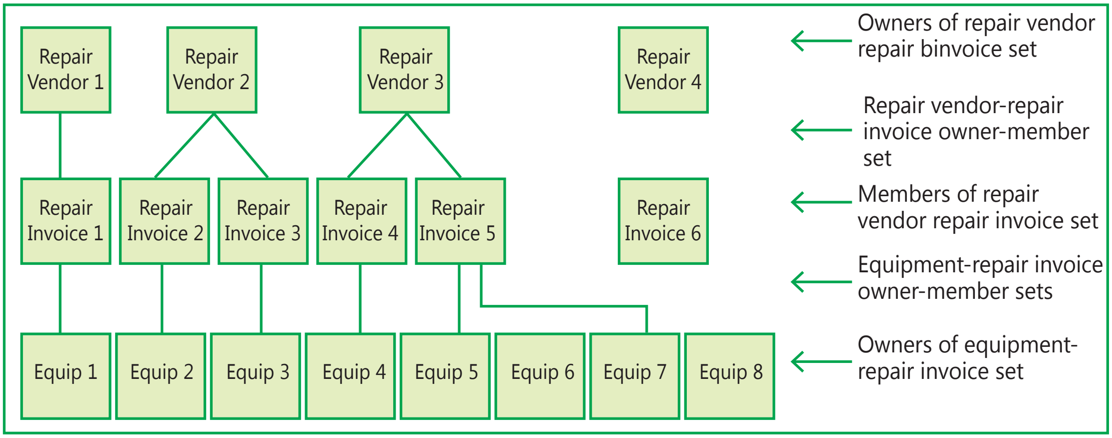


Fig. 3.3.7: Example of Network Database Model

Unlike hierarchical data structures that require specific entrance points to find records in a hierarchy, network data structures can be entered and traversed more flexibly.

C. **Relational Database Model:** A **Relational Database** allows the definition of data and their structures, storage and retrieval operations and integrity constraints that can be organized in a table structure. A table is a collection of records and each record in a table contains the same fields, which define the nature of the data stored in the table. A record is one instance of a set of fields in a table.

Three key terms are used extensively in relational database models: **Relations, Attributes**, and **Domains.** A relation is a table with columns and rows. The named columns of the relation are called attributes, and the domain is the set of values the attributes can take.

All relations (and, thus, tables) in a relational database must adhere to some basic rules to qualify as relations. First, the ordering of columns is immaterial in a table. Second, there can't be identical record in a table. And third, each record will contain a single value for each of its attributes.

A relational database contains multiple tables, with at least similar value occurring in two different records (belonging to the same table or to different tables) that implies a relationship among those two records.

In a relational database, all the tables are related by one or more fields, so that it is possible to connect all the tables in the database through the field(s) they have in common. For each table, one of the fields is identified as a Primary Key, which is the unique identifier for each record in the table. Keys are commonly used to join or combine data from two or more tables. Popular examples of relational databases are Microsoft Access, MySQL, and Oracle.

For example, an **Employee** table may contain a column named **Location** which contains a value that matches the key of a Location table. Keys are also critical in the creation of indexes, which facilitate fast retrieval of data from large tables. Any column can be a key, or multiple columns can be grouped together into a compound key.

D. **Object Oriented Data Base Model:** It is based on the concept that the world can be modelled in terms of objects and their interactions. Objects are entities conveying some meaning for us and possess certain attributes to characterize them and interacting with each other. An **Object-Oriented Database** provides a mechanism to store complex data such as images, audio and video, etc. An object-oriented database (also referred to as object-oriented database management system or OODBMS) is a set of objects. In these databases, the data is modelled and created as objects.

An Object-Oriented Database Management System (OODBMS) helps programmers make objects created in a programming language behave as a database object. Object-oriented programming is based on a series of working objects. Each object is an independently functioning application or program, assigned with a specific task or role to perform. An object-oriented database management system is a relational database designed to manage all these independent programs, using the data produced to quickly respond to requests for information by a larger application.

In the Fig. 3.3.8, the light rectangle indicates that 'engineer' is an object possessing attributes like 'date of birth', 'address', etc. which is interacting with another object known as 'civil jobs'. When a civil job is commenced, it updates the 'current job' attribute of the object known as 'engineer', because 'civil job' sends a message to the latter object.

Objects can be organized by first identifying them as a member of a class / subclass. Different objects of a particular class should possess at least one common attribute. The dark rectangles indicate 'Engineer' as a class and 'Civil Engineer' and also 'Architect' as both subclasses of 'Engineer'. These subclasses possess all the attributes of 'Engineer' over and above each possessing at least one attribute not possessed by 'Engineer'. The line intersecting particular object classes represents the class of structure.

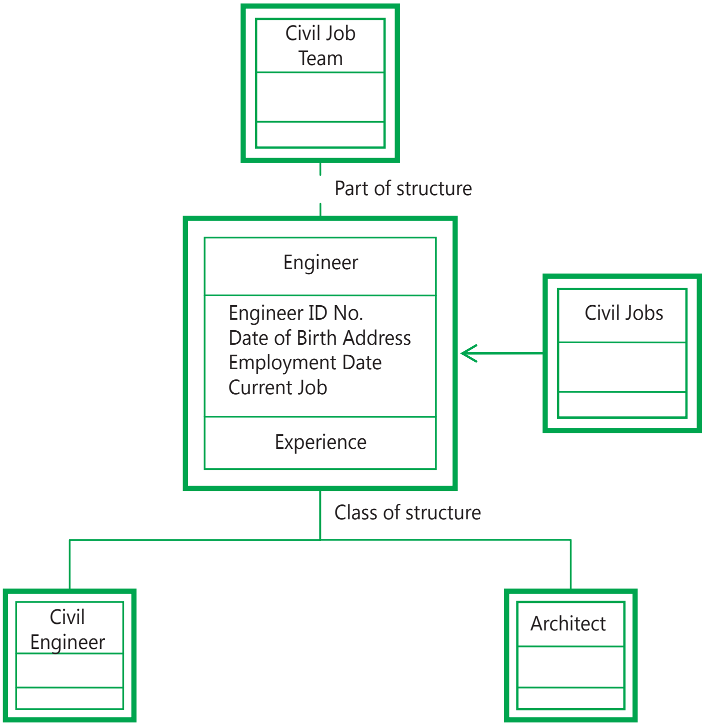


Fig. 3.3.8: An object-oriented database design

Secondly, objects can be identified as a component of some other object. 'Engineers' are components of a 'Civil Job Team' which may have one to more than one number of member(s). An 'Engineer' may not be a member of the 'Civil Job Team' and may not be a member of more than one team. The dotted line intersecting object classes represents the part of structure. Apart from possessing attributes, objects as well as possess methods or services that are responsible for changing their states.

(ii) Advantages of DBMS

Major advantages of DBMS are given as follows:

- **Permitting Data Sharing:** One of the principle advantages of a DBMS is that the same information can be made available to different users.
- **Minimizing Data Redundancy:** In a DBMS duplication of information or redundancy is, if not eliminated, carefully controlled or reduced i.e. there is no need to repeat the same data over and over again. Minimizing redundancy can therefore significantly reduce the cost of storing information on hard drives and other storage devices.
- **Integrity can be maintained:** Data integrity is maintained by having accurate, consistent, and up-to-date data. Updates and changes to the data only must be made in one place in DBMS ensuring Integrity. The chances of making a mistake increase if the same data needs to be changed at several different places than making the change in one place.

- **Program and File consistency:** Using a DBMS, file formats and programs are standardized. This makes the data files easier to maintain because the same rules and guidelines apply across all types of data. The level of consistency across files and programs also makes it easier to manage data when multiple programmers are involved.
- **User-friendly:** DBMS makes the data access and manipulation easier for the user. DBMS also reduce the reliance of users on computer experts to meet their data needs.
- **Improved security:** DBMSs allow multiple users to access the same data resources which could lead to risk to an enterprise if not controlled. Security constraints can be defined i.e. Rules can be built to give access to sensitive data. Some sources of information should be protected or secured and only viewed by select individuals. Using passwords, database management systems can be used to restrict data access to only those who should see it.
- **Achieving program/data independence:** In a DBMS, data does not reside in applications but data bases program & data are independent of each other.
- **Faster Application Development:** In the case of deployment of DBMS, application development becomes fast. The data is already therein databases, application developer has to think of only the logic required to retrieve the data in the way a user needs.

(iii) Disadvantages of a DBMS

There are basically two major downsides to using DBMSs. One of these is cost (both system and user training), and the other is the threat to data security. These are given as under:

- **Cost:** Implementing a DBMS system can be expensive and time-consuming, especially in large enterprises. Training requirements alone can be quite costly.
- **Security:** Even with safeguards in place, it may be possible for some unauthorized users to access the database. If one gets access to database, then it could be an all or nothing proposition.

Some Related Concepts of Database

- **Big Data:** A new buzzword that has been capturing the attention of businesses lately is big data. The term refers to such massively large data sets that conventional database tools do not have the processing power to analyze them. For example, Walmart must process over one million customer transactions every hour. Storing and analyzing that much data is beyond the power of traditional database-management tools. Understanding the best tools and techniques to manage and analyze these large data sets is a problem that governments and businesses alike are trying to solve. This is an interesting space to explore from a career perspective since everything is nothing more than data. In fact, you and I are nothing more than data points in databases on various companies.
- **Data Warehouse:** As organizations have begun to utilize databases as the

center piece of their operations, the need to fully understand and leverage the data they are collecting has become more and more apparent. However, directly analyzing the data that is needed for day-to-day operations is not a good idea; we do not want to tax the operations of the company more than we need to. Further, organizations also want to analyze data in a historical sense: How does the data we have today compare with the same set of data this time last month, or last year? From these needs arose the concept of the data warehouse.

The concept of the data warehouse is simple: extract data from one or more of the organization's databases and load it into the data warehouse (which is itself another database) for storage and analysis. However, the execution of this concept is not that simple. A data warehouse should be designed so that it meets the following criteria:

- It uses non-operational data. This means that the data warehouse is using a copy of data from the active databases that the company uses in its day-to-day operations, so the data warehouse must pull data from the existing databases on a regular, scheduled basis.
- The data is time-variant. This means that whenever data is loaded into the data warehouse, it receives a time stamp, which allows for comparisons between different time periods.
- The data is standardized. Because the data in a data warehouse usually comes from several different sources, it is possible that the data does not use the same definitions or units. For example, our Events table in our Student Clubs database lists the event dates using the mm/dd/ yyyy format (e.g., 01/10/2013). A table in another database might use the format yy/mm/dd (e.g.13/01/10) for dates. For the data warehouse to match up dates, a standard date format would have to be agreed upon and all data loaded into the data warehouse would have to be converted to use this standard format. This process is called **Extraction-Transformation-Load (ETL).**
- There are two primary schools of thought when designing a data warehouse: **Bottom-Up** and **Top- Down.**
    - The **Bottom-Up Approach** starts by creating small data warehouses, called data marts, to solve specific business problems. As these data marts are created, they can be combined into a larger data warehouse.
    - The **Top-Down Approach** suggests that we should start by creating an enterprise-wide data warehouse and then, as specific business needs are identified, create smaller data marts from the data warehouse.

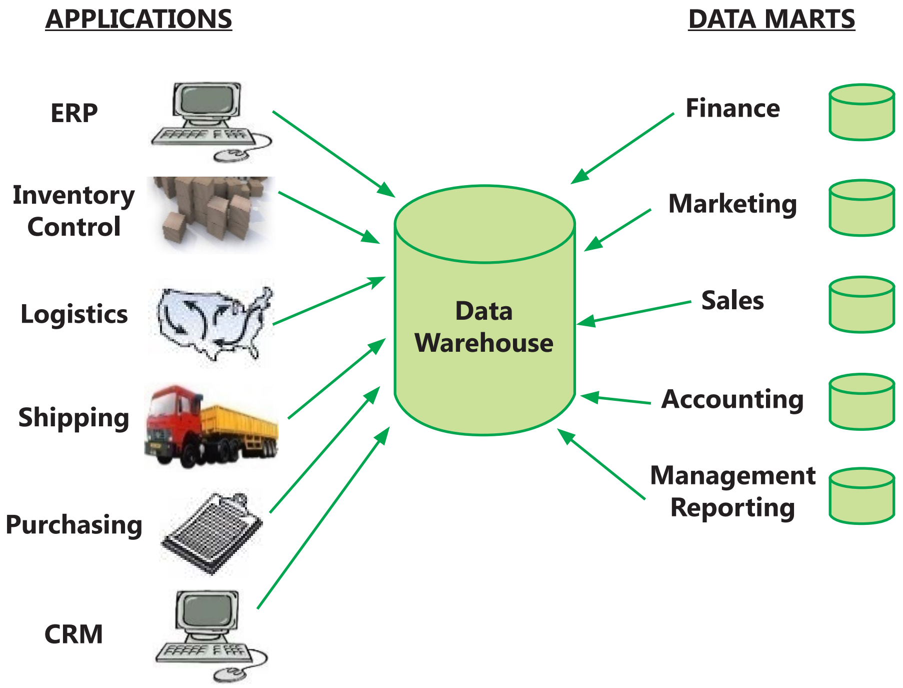


Fig. 3.3.9: Centralized view of Data Warehouse

❖ Benefits of Data Warehouse

Organizations find data warehouses quite beneficial for several reasons (Refer Fig. 3.3.9):

- The process of developing a data warehouse forces an organization to better understand the data that it is currently collecting and, equally important, what data is not being collected.
- A data warehouse provides a centralized view of all data being collected across the enterprise and provides a means for determining data that is inconsistent.
- Once all data is identified as consistent, an organization can generate one version of the truth. This is important when the company wants to report consistent statistics about itself, such as revenue or number of employees.
- By having a data warehouse, snapshots of data can be taken over time. This creates a historical record of data, which allows for an analysis of trends.
- A data warehouse provides tools to combine data, which can provide new information and analysis.

- **Data Mining: Data Mining** is the process of analyzing data to find previously unknown trends, patterns, and associations to make decisions. Generally, data mining is accomplished through automated means against extremely large data sets, such as a data warehouse. An example of data mining includes an analysis of sales from a large grocery chain might determine that milk is purchased more frequently the day after it rains in cities with a population of less than 50,000.
    - o A bank may find that loan applicants whose bank accounts show particular deposit and withdrawal patterns are not good credit risks.
    - o A baseball team may find that collegiate baseball players with specific statistics in hitting, pitching, and fielding make for more successful major league players.

In some cases, a data-mining project is begun with a hypothetical result in mind. For example, a grocery chain may already have some idea that buying patterns change after it rains and want to get a deeper understanding of exactly what is happening. In other cases, there are no presuppositions and a data-mining program is run against large data sets to find patterns and associations. Refer Fig. 3.3.10.

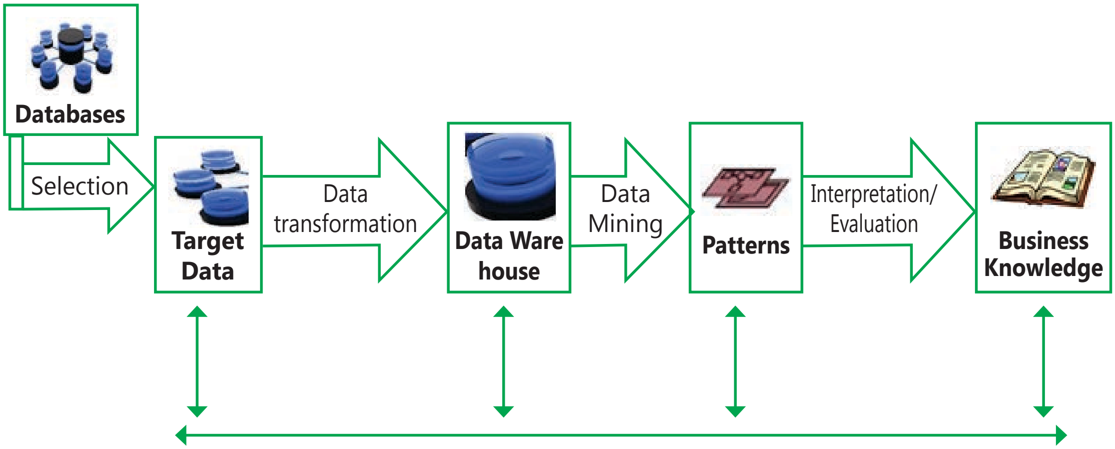


Fig. 3.3.10: Steps involved in Data Mining

3.3.4 Networking and Communication Systems

In today's high speed world, we cannot imagine an information system without an effective communication system. Effective and efficient communication is a valuable resource which helps in good management. To enable this communication, we need communication networks. Telecommunications give an organization the capability to move information rapidly between distant locations and to provide the ability for the employees, customers, and suppliers to collaborate from anywhere, combined with the capability to bring processing power to the point of the application. All of this offers firm important opportunities to restructure its business processes and to capture high competitive ground in the marketplace. Through telecommunications, this value may be:

(i) An increase in the efficiency of operations;

(ii) Improvements in the effectiveness of management; and

(iii) Innovations in the marketplace.

Computer Network is a collection of computers and other hardware interconnected by communication channels that allow sharing of resources and information. Where at least one process in one device can send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. A network is a group of devices connected to each other.

Network and Communication System: These consist of both physical devices and software, links the various pieces of hardware and transfers the data from one physical location to another. Computers and communications equipment can be connected in networks for sharing voice, data, images, sound and video. A network links two or more computers to share data or resources such as a printer.

Every enterprise needs to manage its information in an appropriate and desired manner. The enterprise must do the following for this:

- Knowing its information needs;
- Acquiring that information;
- Organizing that information in a meaningful way;
- Assuring information quality; and
- Providing software tools so that users in the enterprise can access information they require.

Each component, namely the computer in a computer network is called a 'Node'. Computer networks are used for exchange of data among different computers and to share the resources. Field of computer networks is one of the most interesting and rapidly growing fields in computer science. With man's desire for faster and better processing power, existing computer systems are connected to each other to form a computer network which allows them to share CPU, I/O devices, storages, etc. without much of an impact on individual systems.

In real world, we see numerous networks like Telephone/ mobile network, postal networks etc. If we look at these systems, we can analyze that networks could be of two types:

- **Connection Oriented networks:** Wherein a connection is first established and then data is exchanged like it happens in case of telephone networks.

- **Connectionless Networks:** Where no prior connection is made before data exchanges. Data which is being exchanged in fact has a complete contact information of recipient and at each intermediate destination, it is decided how to proceed further like it happens in case of postal networks.

These real-world networks have helped model computer networks. Each of these networks is modeled to address the following basic issues:

- **Routing:** It refers to the process of deciding on how to communicate the data from source to destination in a network.
- **Bandwidth:** It refers to the amount of data which can be sent across a network in given time.
- **Resilience:** It refers to the ability of a network to recover from any kind of error like connection failure, loss of data etc.
- **Contention:** It refers to the situation that arises when there is a conflict for some common resource in a network. For example, network contention could arise when two or more computer systems try to communicate at the same time.

The following are the important benefits of a computer network:

- **Distributed nature of information:** There would be many situations where information must be distributed geographically. E.g. in the case of Banking Company, accounting information of various customers could be distributed across various branches but to make Consolidated Balance Sheet at the year-end, it would need networking to access information from all its branches.
- **Resource Sharing:** Data could be stored at a central location and can be shared across different systems. Even resource sharing could be in terms of sharing peripherals like printers, which are normally shared by many systems. E.g. In the case of a CBS, Bank data is stored at a Central Data Centre and could be accessed by all branches as well as ATMs.
- **Computational Power:** The computational power of most of the applications would increase drastically if the processing is distributed amongst computer systems. For example: processing in an ATM machine in a bank is distributed between ATM machine and the central Computer System in a Bank, thus reducing load on both.
- **Reliability:** Many critical applications should be available 24x7, if such applications are run across different systems which are distributed across network then the reliability of the application would be high. E.g. In a city, there could be multiple ATM machines so that if one ATM fails, one could withdraw money from another ATM.

- **User communication:** Networks allow users to communicate using e-mail, newsgroups, video conferencing, etc.

Telecommunications may provide these values through the following impacts:

(a) **Time compression:** Telecommunications enable a firm to transmit raw data and information quickly and accurately between remote sites.

(b) **Overcoming geographical dispersion:** Telecommunications enable an organization with geographically remote sites to function, to a degree, as though these sites were a single unit. The firm can then reap benefits of scale and scope which would otherwise be unobtainable.

(c) **Restructuring business relationships:** Telecommunications make it possible to create systems which restructure the interactions of people within a firm as well as a firm's relationships with its customers. Operational efficiency may be raised by eliminating intermediaries from various business processes.

3.3.5 Network Related Concepts

Networking communication is full of some very technical concepts based on some simple principles.

- **Packet:** The fundamental unit of data transmitted over the Internet. When a device intends to send a message to another device (for example, your PC sends a request to YouTube to open a video), it breaks the message down into smaller pieces, called packets. Each packet has the sender's address, the destination address, a sequence number, and a piece of the overall message to be sent.
- **Repeater:** A repeater regenerates the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. They do no amplify the signals, however, when the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- **Hub:** A simple network device that connects other devices to the network and sends packets to all the devices connected to it. A hub is basically a multiport repeater that connects multiple wires coming from different branches. Hubs cannot filter data, so data packets are sent to all connected devices. As they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.
- **Bridge:** Bridge is a communications processor that connects two Local Area Networks (LANs) working on the same protocol. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination.
- **MAC Address:** These are most often assigned by the manufacturer of a

Network Interface Controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number.

- **Switch:** A network device that connects multiple devices together and filters packets based on their destination within the connected devices.
- **Router:** A device that receives and analyses packets and then routes them towards their destination. In some cases, a router will send a packet to another router; in other cases, it will send it directly to its destination.
- **Network Topology:** The term 'Topology' defines the physical or logical arrangement of links in a network. It is the geometric representation of the relationship of all the links and linking devices (usually called Nodes) to each other. Common topologies are **Star Network** that involves a central unit with number of terminals tied into it; **Bus Network** in which a single length of wire, cable, or optical fiber (called bus) connects several computers; **Ring Network** much like a bus network, except the length of wire, cable, or optical fiber connects to form a loop; and **Mesh Network** in which each node is connected by a dedicated point to point link to every node.
- **Transmission Mode:** It is used to define the direction of signal flow between two linked devices. There are three types of transmission modes characterized as per the direction of the exchanges:
  - **Simplex** (wherein the data flows in only one direction- unidirectional),
  - **Half-Duplex** (where in the data flows in one direction or the other, but not both at the same time) and
  - **Duplex** (in which the data flows in both directions simultaneously).
- **Protocol:** In computer networking, a protocol is the set of rules that allow two (or more) devices to exchange information back and forth across the network.
- **IP Address:** Every device that communicates on the Internet, whether it be a personal computer, a tablet, a smartphone, or anything else, is assigned a unique identifying number called an IP (Internet Protocol) address. Historically, the IP-address standard used has been IPv4 (version 4), which has the format of four numbers between 0 and 255 separated by a period. For example, let's say the domain wikipedia.org has the IP address of 107.23.196.166. The IPv4 standard has a limit of 4,294,967,296 possible addresses. However, IPv6 standard, which is currently being phased in, is formatted as eight groups of four hexadecimal digits, such as 2001:0db8:85a3:0042:1000:8a2e:0370:7334. The IPv6 standard has a limit of 3.4×1038 possible addresses.
- **Domain Name:** A Domain Name is a human-friendly name for a device on the Internet. These names generally consist of a descriptive text followed by the top-level domain (TLD). For example, Wikipedia's domain name is wikipedia.org;

Wikipedia describes the organization and .org is the top-level domain. In this case, the .org TLD is designed for non-profit organizations. Other well- known TLDs include .com, .net, and .gov.

- **Domain Name Server (DNS):** DNS which acts as the directory on the Internet. When a request to access a device with a domain name is given, a DNS server is queried. It returns the IP address of the device requested, allowing for proper routing.
- **Packet Switching:** When a packet is sent from one device out over the Internet, it does not follow a straight path to its destination. Instead, it is passed from one router to another across the Internet until it is reaches its destination. In fact, sometimes two packets from the same message will take different routes. Sometimes, packets will arrive at their destination out of order. When this happens, the receiving device restores them to their proper order.
- **Wi-Fi:** Wi-Fi is a technology that takes an Internet signal and converts it into radio waves. These radio waves can be picked up within a radius of approximately 65 feet by devices with a wireless adapter. Several Wi-Fi specifications have been developed over the years, starting with 802.11b (1999), followed by the 802.11g specification in 2003 and 802.11n in 2009. Each new specification improved the speed and range of Wi- Fi, allowing for more uses. One of the primary places where Wi-Fi is being used is in the home. However, with increase in smart phone sales, Wi-Fi hotspot services are being provided at various public places to provide better customer service.
- **Voice Over IP (VoIP):** A growing class of data being transferred over the Internet is Voice Data. A protocol called VoIP enables sounds to be converted to a digital format for transmission over the Internet and then recreated at the other end. By using many existing technologies and software, voice communication over the Internet is now available to anyone with a browser (think Skype, Google Hangouts, Whatsapp calls).

3.4 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.

3.4.1 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 centralized data center. In the past, the financial information would have been spread throughout the organization 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 organization'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.

3.4.2 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 as follows:

- 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 or 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.

3.4.3 Impact of Technology on 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 etc. The topic is covered in detail in later section of the chapter.

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 computerized 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.

3.5 CLASSIFICATION OF INFORMATION SYSTEMS' CONTROLS

Internal controls can be classified into various categories to illustrate the interaction of various groups in the enterprise and their effect on information systems on different basis. These categories have been represented in the Fig. 3.5.1:

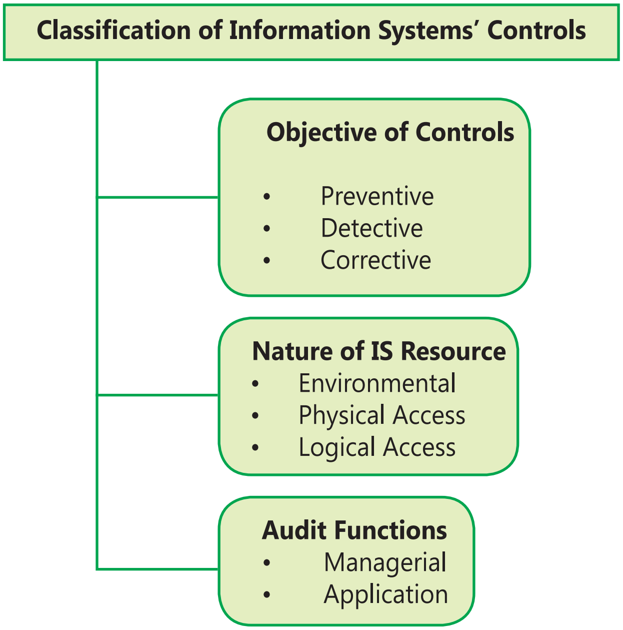


Fig. 3.5.1: Classification of IS Controls

3.5.1 Classification based on "Objective of Controls"

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

(A) Preventive Controls: These controls prevent errors, omissions, or security incidents from occurring. Examples include simple data-entry edits that block alphabetic characters from being entered in numeric fields, access controls that protect sensitive data/ system resources from unauthorized people, and complex and dynamic technical controls such as anti virus software, firewalls, and intrusion prevention systems. In other words, Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. Some of the examples of Preventive Controls are as follows:

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 3.5.1 shows how the same purpose is achieved by using manual and computerized controls.

Table 3.5.1: 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. In other words, Detective Controls detect errors or incidents that elude preventive controls. For example, a detective control may identify account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities. Detective controls can also include monitoring and analysis to uncover activities or events that exceed authorized limits or violate known patterns in data that may indicate improper manipulation. For sensitive electronic communications, detective controls can indicate that a message has been corrupted or the sender's secure identification cannot be authenticated.

Some of the examples of Detective Controls are as follows:

Cash counts; Bank reconciliation; Review of payroll reports; Compare transactions on reports to source documents; Monitor actual expenditures against budget; Use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend; Hash totals; Check points in production jobs; Echo control in telecommunications; Duplicate checking of calculations; Past-due accounts report; The internal audit functions; Intrusion Detection System; Cash counts and bank reconciliation, and Monitoring expenditures against budgeted amount.

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.

(C) **Corrective Controls:** It is desirable to correct errors, omissions, or incidents once they have been detected. They vary from simple correction of data-entry errors, to identifying and removing unauthorized users or software from systems or networks, to recovery from incidents, disruptions, or disasters. Generally, it is most efficient to prevent errors or detect them as close as possible to their source to simplify correction. These corrective processes also should be subject to preventive and detective controls, because they represent another opportunity for errors, omissions, or falsification.

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. For example- Complete changes to IT access lists if individual's role changes is a corrective control. If an accounts clerk is transferred to the sales department as a salesman his/her access rights to the general ledger and other finance functions should be removed and he/she should be given access only to functions required to perform his sales job.

Some of the other examples of Corrective Controls are as follows:

Submit corrective journal entries after discovering an error; A Business Continuity Plan (BCP); Contingency planning; Backup procedure; Rerun procedures; Change input value to an application system; and Investigate budget variance and report violations.

The main characteristics of the corrective controls are as follows:

- 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.

3.5.2 Classification based on "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, Uninterrupted Power Supply (UPS), smoke detection, fire-extinguishers, dehumidifiers etc. The Table 3.5.2 enlists all the environmental exposure and their controls.

Table 3.5.2: Controls for Environmental Exposures

I. Fire Damage: It is a major threat to the physical security of a computer installation.

Controls for Environmental Exposures: Some of the major ways of protecting the installation against fire damage are as follows:

- Both automatic and manual fire alarms may be placed at strategic locations and a control panel may be installed to clearly indicate this.
- 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.
- Manual fire extinguishers can be placed at strategic locations.
- Fireproof Walls; Floors and Ceilings surrounding the Computer Room and Fire Resistant Office Materials such as wastebaskets, curtains, desks, and cabinets should be used.
- Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station.
- All staff members should know how to use the system. The procedures to be followed during an emergency should be properly documented are Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon dioxide based fire extinguishers.
- Less Wood and plastic should be in computer rooms.
- Use a gas based fire suppression system.

- To reduce the risk of firing, the location of the computer room should be strategically planned and should not be in the basement or ground floor of a multi-storey building.
- Regular Inspection by Fire Department should be conducted.
- Fire supression systems should be supplemented and not replaced by smoke detectors.
- **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. In all circumstances saving human life should be given paramount importance.
- **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).
- **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.

II. Power Spikes: This is caused due to a very short pulse of energy in a power line.

Controls for Environmental Exposures: Some of the major ways of protecting the installation against power spikes as follows:

- The risk of damage due to power spikes can be reduced using Electrical Surge Protectors that are typically built into the Un-interruptible Power System (UPS).
- **Un-interruptible 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.
- Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power.
- **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.

III. 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.

Controls for Environmental Exposures: Some of the major ways of protecting the installation against water damage are as follows:

- Wherever possible have waterproof ceilings, walls and floors;
- Ensure an adequate positive drainage system exists;
- Install alarms at strategic points within the installation;
- In flood areas have the installation above the upper floors but not at the top floor;
- Water proofing; and
- Water leakage Alarms.

IV. Pollution Damage and others : 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.

Controls for Environmental Exposures: Some of the controls are as follows:

- **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.
- **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. Refer the Table 3.5.3.

Table 3.5.3: Controls for Physical Exposures

I. Physical Exposures: This includes abuse of data processing resources; Blackmail; Embezzlement (an act of dishonestly withholding assets for 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 equipment's or documents; Public disclosure of sensitive information; and Unauthorized entry.

Controls for Physical Exposures

i. Locks on Doors

- **Cipher locks (Combination Door Locks)** - Cipher locks are used in low security situations or when many 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, 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 not be duplicated.
- **Electronic Door Locks** – A magnetic or embedded chip-based plastics card key or token may be entered a reader to gain access in these systems.

ii. 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 color of the badge can be changed. Sophisticated photo IDs can also be utilized as electronic card keys.

iii. **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.

iv. **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, 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 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.

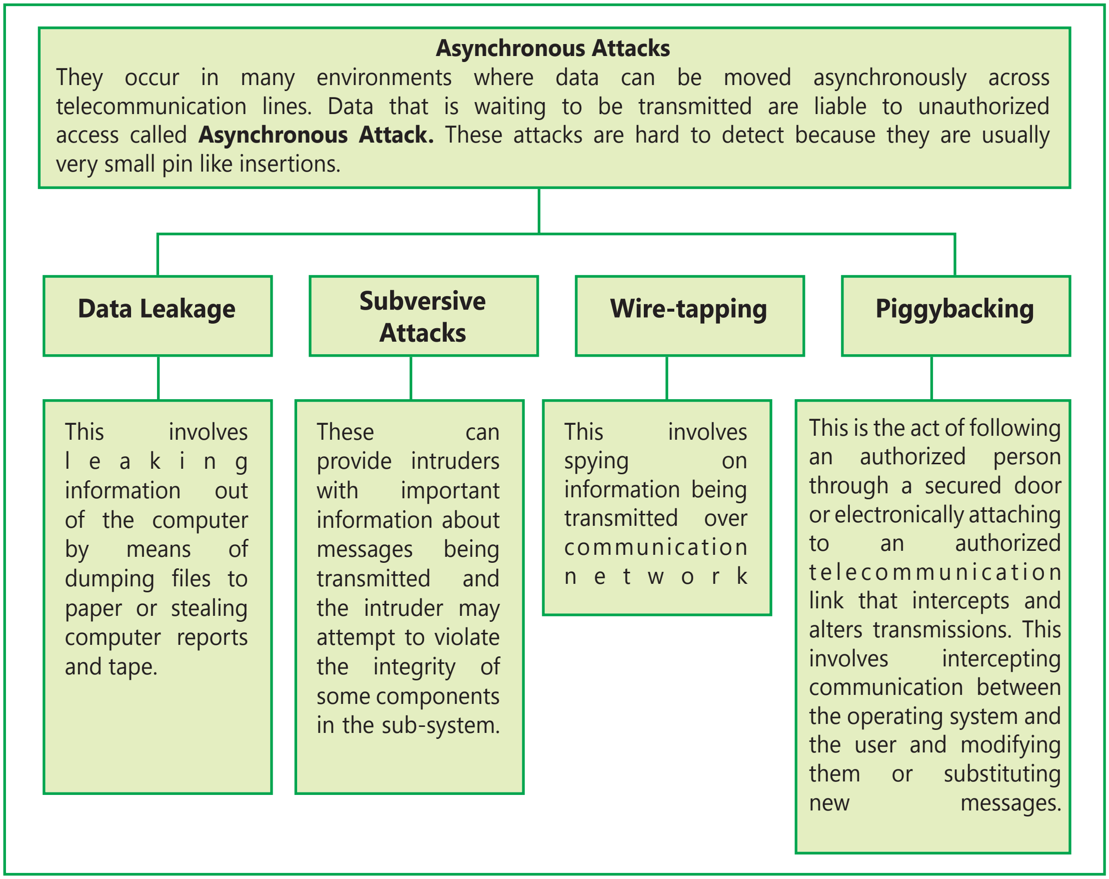
Compromise or absence of logical access controls in the organizations may result in potential losses due to exposures that may lead to the total shutdown of the computer functions. Intentional or accidental exposures of logical access control encourage technical exposures (in the Table 3.5.4) and computer crimes (in the Fig. 3.5.2). These are given as follows:

Table 3.5.4: Technical Exposures

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

- **Data Diddling:** This involves the change of data before or after they entered 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.
- **Christmas Card:** It is a well-known example of Trojan and 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.
- **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.



Asynchronous Attacks

They occur in many environments where data can be moved asynchronously across telecommunication lines. 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.

Data Leakage

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

Subversive Attacks

These can provide intruders with important information about messages being transmitted and the intruder may attempt to violate the integrity of some components in the sub-system.

Wire-tapping

This involves spying on information being transmitted over communication network

Piggybacking

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

Fig. 3.5.2: Asynchronous Attacks

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 as follows:

- 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.

Some of the Logical Access Controls are listed below:

I. **User Access Management:** This is an important factor that involves the following:

- **User Registration:** Information about every user is documented. Some questions like why and who is the user granted the access; has the data owner approved the access, and has the user accepted the responsibility? etc. are answered. The de-registration process is also equally important.
- **Privilege management:** Access privileges are to be aligned with job requirements and responsibilities and are to be minimal w.r.t their job functions. For example, an operator at the order counter shall have direct access to order processing activity of the application system.
- **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.

II. **User Responsibilities:** User awareness and responsibility are also important factors and are as follows:

- **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.

III. **Network Access Control:** An Internet connection exposes an organization to the harmful elements of the outside world. The protection 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:** 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 that will allow only authorized traffic between the organization and the outside to pass through it. 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 with a key to convert the original message called the Clear text into Cipher text. This is decrypted at the receiving end. 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

IV. **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 Job Scheduling; 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'. Hence, protecting operating system access is extremely crucial and can be achieved using following steps.

- **Automated terminal identification:** This will help to ensure that a specified session could only be initiated from a certain location or computer terminal.
- **Terminal log-in procedures:** A log-in procedure is the first line of defense against unauthorized access as it 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 and accordingly authorizes the log-in.
- **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. For example, no computer access after 8.00 p.m. and before 8.00 a.m. - or on a Saturday or Sunday.

V. **Application and Monitoring System Access Control:** Some of the steps are as follows:

- **Information access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user can 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.

VI. Mobile Computing: In today's organizations, computing facility is not restricted to a certain data center alone. Ease of access on the move provides efficiency and results in additional responsibility on the management to maintain information security. 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.

3.5.3 Classification based on"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.

I. 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.
  - **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 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.
- **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; ie.. 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:
  - o How much the organization should be spending on the information systems function?
  - o 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 based on **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 he expected benefits and resource consumption and finally the review committee must establish priorities.

II. 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 and formally authorized to ensure their economic justification and feasibility. 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. Regardless of the technology involved, the user can create a detailed written descriptive document of the logical needs that must be satisfied by the system. 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 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.
- **Internal Auditor's Participation:** The internal auditor plays an important role in the control of systems and should become involved at the inception of the system development process to make conceptual suggestions regarding system requirements and controls and 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. 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).

III. 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 3.5.5. 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 3.5.5: 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.

IV. 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 like dual recording of data; periodic dumping of data; logging input transactions and changes to the data are used.

(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.

V. 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.

VI. 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 based on "Nature of Information System Resources – Environmental Controls, Physical Controls and Logical Access Controls 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 3.5.6:

Table 3.5.6: 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, despite 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. 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. Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations.

BCP (Business Continuity Planning) Controls: These controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption.

VII. 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 wellbeing 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.

(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 provided 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.

B. Application Controls and their Categories

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.

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 can 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:

I. **Boundary Controls:** The major controls of the boundary system are the access control mechanisms that links the authentic users to the authorized resources, they are permitted to access. The boundary subsystem establishes the interface between the would-be user of a computer system and the computer itself. The access control mechanism has three major purposes:

- o **Identification:** To establish the identity and authenticity of would-be users of a computer system ie. the system must ensure that it has an authentic user.
- o **Authentication:** To establish the identity and authenticity of the resources that users wish to employ ie. users must ensure that they are given authentic resources. Users may provide four factor of authentication information.

- o **Authorization:** To restrict the actions taken by users who obtain computer resources to a set of authorized actions ie. the users may be allowed to employ resources only in restricted ways. The user can provide these factors of input information for the authentication process and gain access to his required resources. Major Boundary Control are 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).
- ◆ **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.

II. Input Controls

Data that is presented to an application as input data must be validated for authorization, reasonableness, completeness, and integrity. 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 as shown in Fig. 3.5.3:

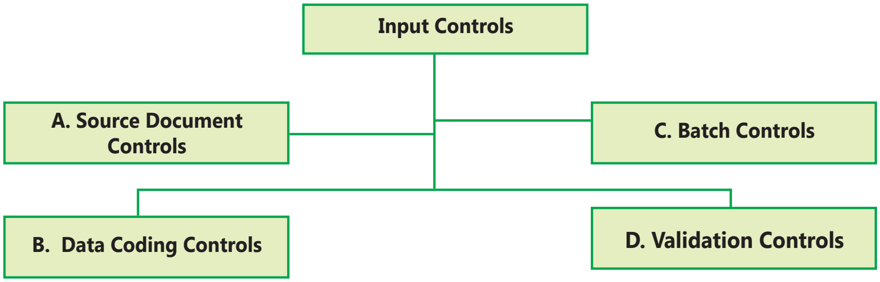


Fig. 3.5.3: Classification of Input Controls

The details of Source Document Controls is given in Table 3.5.7.

Table 3.5.7: Source Document Controls

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. 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:	• **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.

The details of Data Coding Controls is given in Table 3.5.8.

Table 3.5.8: Data Coding Controls

B. Data Coding Controls: Two types of errors can corrupt a data code and cause processing errors. 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. These are transcription and transposition errors, which are as these:

Transcription Errors: It is a special type of data entry error that is commonly made by human operators or by Optical Character Recognition (OCR) programs. 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: It is a simple error of data entry that occur when two digits that are either individual or part of larger sequence of numbers are reversed (Transpose) when posting a transaction. 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 non-adjacent digits are transposed. For example, 12345 are recorded as 32154.

The details of Batch Controls is given in Table 3.5.9.

Table 3.5.9: Batch Controls

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 that occur are as follows:
  - o **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.
  - o **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 are as follows:
  - o **Financial totals:** Grand totals calculated for each field containing money amounts.
  - o **Hash totals:** Grand totals calculated for any code on a document in the batch, eg., the source document serial numbers can be totalled.
  - o **Document/Record Counts:** Grand totals for number of documents in record in batch.

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:
  - o **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.
  - o **Picture Checks:** These checks against entry into processing of incorrect/ invalid characters.
  - o **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.
  - o **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.
  - o **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.
  - o **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:
  - o **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.

III. Communication Controls

Three major types of exposure arise in the communication subsystem:

- Transmission impairments can cause difference between the data sent and the data received;
- Data can be lost or corrupted through component failure; and
- A hostile party could seek to subvert data that is transmitted through the subsystem.

Communication Controls discuss exposures in the communication subsystem, controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internet working 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 3.5.10 below gives an overview of how physical components can affect communication subsystem reliability.

Table 3.5.10: 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 cannot 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 **Wide Area Network (WAN)**, 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: (a) bus topology, (b) Tree topology, (c) Ring topology, and (d) 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:
  - they often encompass components that are owned by other parties (e.g. a telephone company);
  - they provide relatively low-speed communication among nodes; and
  - they span large geographic areas

  Except for 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. Bridge, Router, Switch and Gateways are some of the Internetworking devices.

IV. 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 3.5.11.

Table 3.5.11: Controls to reduce expected losses from errors and irregularities associated with Central processors

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. The failure might be transient (that disappears after a short period), intermittent (that reoccurs periodically), or permanent (that does not correct with time). For the transient and intermittent errors; retries and re-execution might be successful, whereas for permanent errors, the processor must halt and report the error.

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.

(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 as follows:

- **Run-to-Run Totals:** These helps 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 like 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.

V. 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 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 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.

VI. Output Controls

Output 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 must be enforced both in a batch-processing environment as well as in an online environment. Various Output Controls are as follows:

- **Storage and Logging of sensitive, critical forms:** Pre-printed stationery should be stored securely to prevent unauthorized destruction orremoval 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 can 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.

3.6 INFORMATION SYSTEMS' AUDITING

IS Auditing is defined as the process of attesting objectives (those of the external auditor) that focus on asset safeguarding, data integrity and management objectives (those of the internal auditor) that include effectiveness and efficiency both. This enables organizations to better achieve four major objectives that are as follows:

- **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorized access.
- **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organization requires all the time. It is also important from the business perspective of the decision maker, competition and the market environment.
- **System Effectiveness Objectives:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.

- **System Efficiency Objectives:** To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

3.6.1 Need for Audit of Information Systems

Factors influencing an organization toward controls and audit of computers and the impact of the information systems audit function on organizations are depicted in the Fig. 3.6.1.

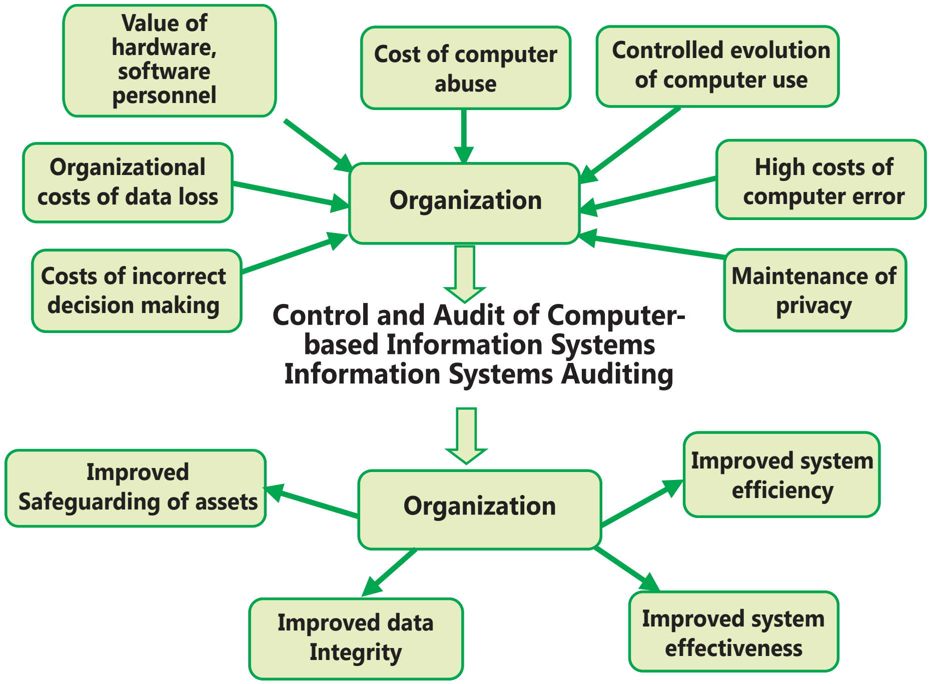

Value of hardware, software personnel
Cost of computer abuse
Controlled evolution of computer use
Organizational costs of data loss
Organization
High costs of computer error
Costs of incorrect decision making
Maintenance of privacy
Control and Audit of Computer-based Information Systems Information Systems Auditing
Improved Safeguarding of assets
Organization
Improved system efficiency
Improved data Integrity
Improved system effectiveness

Fig. 3.6.1: Impact of Controls and Audit influencing an Organization

Let us now discuss these reasons in details:

- **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.

- **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high-level decisions require accurate data to make quality decision rules.

- **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)

- **Value of Computer Hardware, Software and Personnel:** These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.

- **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
- **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
- **Controlled evolution of computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

3.6.2 IS Audit and Audit Evidence

According to SA-230, Audit Documentation refers to the record of audit procedures performed, relevant audit evidence obtained, and conclusions the auditor reached (terms such as “working papers” or “work papers” are also sometimes used). The objects of an auditor’s working papers are to record and demonstrate the audit work from one year to another. Evidences are also necessary for the following purposes:

- Means of controlling current audit work;
- Evidence of audit work performed;
- Schedules supporting or additional item in the accounts; and
- Information about the business being audited, including the recent history.

In IS environment, the critical issue is that evidences are not available in physical form, but are in electronic form.

3.6.3 Inherent Limitations of Audit

To be able to prepare proper report, auditor needs documented evidences. The problem of documents not available in physical form has been highlighted at many places. Following is list of actions that auditor needs to take to address the problems:

- Use of special audit techniques, referred to as Computer Assisted Audit Techniques, for documenting evidences. Elaborated under this part, later on.
- Audit timing can be so planned that auditor is able to validate transactions as they occur in system.

Auditor shall form his/her opinion based on above processes. As per (SA 200) “Overall Objectives of An Independent Auditor and Conduct of An Audit in Accordance With Standards of Auditing”, any opinion formed by the auditor is subject to inherent limitations of an audit which include:

- The nature of financial reporting;
- The nature of audit procedures;
- The need for the audit to be conducted within a reasonable period of time and at a reasonable cost.
- The matter of difficulty, time, or cost involved is not in itself a valid basis for the auditor to omit an audit procedure for which there is no alternative or to be satisfied with audit evidence that is less than persuasive.
- Fraud, particularly fraud involving senior management or collusion.
- The existence and completeness of related party relationships and transactions.
- The occurrence of non-compliance with laws and regulations.
- Future events or conditions that may cause an entity to cease to continue as a going concern.

3.6.4 Concurrent or Continuous Audit

Today, organizations produce information on a real-time, online basis. Real-time recordings need real-time auditing to provide continuous assurance about the quality of the data that is continuous auditing. Continuous auditing enables auditors to significantly reduce and perhaps to eliminate the time between occurrence of the client's events and the auditor's assurance services thereon. Errors in a computerized system are generated at high speeds and the cost to correct and rerun programs are high. If these errors can be detected and corrected at the point or closest to the point of their occurrence the impact thereof would be the least. Continuous auditing techniques use two bases for collecting audit evidence. One is the use of embedded modules in the system to collect, process, and print audit evidence and the other is special audit records used to store the audit evidence collected.

Types of Audit Tools: Different types of continuous audit techniques may be used. Some modules for obtaining data, audit trails and evidences may be built into the programs. Audit software is available, which could be used for selecting and testing data. Many audit tools are also available; some of them are described below:

(i) **Snapshots:** Tracing a transaction is a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to dwell upon while involving such a system are to locate the snapshot points based on materiality of transactions when the snapshot will be captured and the reporting system design and implementation to present data in a meaningful way.

(ii) **Integrated Test Facility (ITF):** The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases the auditor must decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

(iii) **System Control Audit Review File (SCARF):** The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

(iv) **Continuous and Intermittent Simulation (CIS):** This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way:

- The database management system reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
- CIS replicates or simulates the application system processing.
- Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
- Exceptions identified by CIS are written to a exception log file.
- The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

(v) **Audit Hooks:** There are audit routines that flag suspicious transactions. For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification displays a message on the auditor's terminal.

3.7 AUDIT TRAIL

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

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning.

- The **Accounting Audit Trail** shows the source and nature of data and processes that update the database.
- The **Operations Audit Trail** maintains a record of attempted or actual resource consumption within a system.

Applications System Controls involve ensuring that individual application systems safeguard assets (reducing expected losses), maintain data integrity (ensuring complete, accurate and authorized data) and achieve objectives effectively and efficiently from the perspective of users of the system from within and outside the organization.

(i) **Audit Trail Objectives:** Audit trails can be used to support security objectives in three ways:

- **Detecting Unauthorized Access:** Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.
- **Reconstructing Events:** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.

- **Personal Accountability:** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

(ii) **Implementing an Audit Trail:** The information contained in audit logs is useful to accountants in measuring the potential damage and financial loss associated with application errors, abuse of authority, or unauthorized access by outside intruders. Logs also provide valuable evidence or assessing both the adequacies of controls in place and the need for additional controls. Audit logs, however, can generate data in overwhelming detail. Important information can easily get lost among the superfluous detail of daily operation. Thus, poorly designed logs can be dysfunctional.

3.7.1 Auditing Environmental Controls

Related aspects are given as follows:

(a) **Role of Auditor in Auditing Environmental Controls:** The attack on the World Trade Centre in 2001 has created a worldwide alert bringing focus on business continuity planning and environmental controls. Audit of environmental controls should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against environmental risks. Some of the critical audit considerations that an IS auditor should consider while conducting his/her audit is given below:

(b) **Audit of Environmental Controls:** Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. Auditing environmental controls requires knowledge of building mechanical and electrical systems as well as fire codes. The IS auditor needs to be able to determine if such controls are effective and if they are cost-effective. Auditing environmental controls requires attention to these and other factors and activities, including:

- **Power conditioning:** The IS auditor should determine how frequently power conditioning equipment, such as UPS, line conditioners, surge protectors, or motor generators, are used, inspected and maintained and if this is performed by qualified personnel.

- **Backup power:** The IS auditor should determine if backup power is available via electric generators or UPS and how frequently they are tested. He or she should examine maintenance records to see how frequently these components are maintained and if this is done by qualified personnel.

- **Heating, Ventilation, and Air Conditioning (HVAC):**The IS auditor should determine if HVAC systems are providing adequate temperature and humidity levels, and if they are monitored. Also, the auditor should determine if HVAC systems are properly maintained and if qualified persons do this.

- **Water detection:** The IS auditor should determine if any water detectors are used in rooms where computers are used. He or she should determine how frequently these are tested and if they are monitored.
- **Fire detection and suppression:** The IS auditor should determine if fire detection equipment is adequate, if staff members understand their function, and if they are tested. He or she should determine how frequently fire suppression systems are inspected and tested, and if the organization has emergency evacuation plans and conducts fire drills.
- **Cleanliness:** The IS auditor should examine data centers to see how clean they are. IT equipment air filters and the inside of some IT components should be examined to see if there is an accumulation of dust and dirt.

3.7.2 Auditing Physical Security Controls

(a) Role of IS Auditor in Auditing Physical Access Controls

Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

- **Risk Assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
- **Controls Assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
- **Review of Documents:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

(b) Audit of Physical Access Controls: Auditing physical security controls requires knowledge of natural and man made hazards, physical security controls, and access control systems.

(i) **Siting and Marking:** Auditing building siting and marking requires attention to several key factors and features, including:

- **Proximity to hazards:** The IS auditor should estimate the building's distance to natural and man made hazards, such as Dams; Rivers, lakes, and canals; Natural gas and petroleum pipelines; Water mains and pipelines; Earthquake faults; Areas prone to landslides; Volcanoes; Severe weather such as hurricanes, cyclones, and tornadoes; Flood zones; Military bases; Airports; Railroads and Freeways. The IS auditor should determine if any risk assessment regarding hazards has been performed and if any compensating controls that were recommended have been carried out.

- **Marking:** The IS auditor should inspect the building and surrounding area to see if building(s) containing information processing equipment identify the organization. Marking may be visible on the building itself, but also on signs or parking stickers on vehicles.

(ii) **Physical barriers:** This includes fencing, walls, barbed/razor wire, bollards, and crash gates. The IS auditor needs to understand how these are used to control access to the facility and determine their effectiveness.

(iii) **Surveillance:** The IS auditor needs to understand how video and human surveillance are used to control and monitor access. He or she needs to understand how (and if) video is recorded and reviewed, and if it is effective in preventing or detecting incidents.

(iv) **Guards and dogs:** The IS auditor needs to understand the use and effectiveness of security guards and guard dogs. Processes, policies, procedures, and records should be examined to understand required activities and how they are carried out.

(v) **Key-Card systems:** The IS auditor needs to understand how key-card systems are used to control access to the facility. Some points to consider include: Work zones: Whether the facility is divided into security zones and which persons are permitted to access which zones whether key-card systems record personnel movement; What processes and procedures are used to issue key-cards to employees? etc.

3.7.3 Auditing Logical Access Controls

(a) Role of IS Auditor in Auditing Logical Access Controls

Auditing Logical Access Controls requires attention to several key areas that include the following:

(i) **Network Access Paths:** The IS auditor should conduct an independent review of the IT infrastructure to map out the organization's logical access paths. This will require considerable effort and may require the use of investigative and technical tools, as well as specialized experts on IT network architecture.

(ii) **Documentation:** The IS auditor should request network architecture and access documentation to compare what was discovered independently against existing documentation. The auditor will need to determine why any discrepancies exist. Similar investigations should take place for each application to determine all of the documented and undocumented access paths to functions and data.

(b) Audit of Logical Access Controls

(I) User Access Controls: User access controls are often the only barrier between unauthorized parties and sensitive or valuable information. This makes the audit of user access controls particularly significant. Auditing user access controls requires keen attention to several key factors and activities in four areas:

(i) Auditing User Access Controls: These are to determine if the controls themselves work as designed. Auditing user access controls requires attention to several factors, including:

- **Authentication:** The auditor should examine network and system resources to determine if they require authentication, or whether any resources can be accessed with out first authenticating.
- **Access violations:** The auditor should determine if systems, networks, and authentication mechanisms can log access violations. These usually exist in the form of system logs showing invalid login attempts, which may indicate intruders who are trying to log in to employee user accounts.
- **User account lockout:** The auditor should determine if systems and networks can automatically lock user accounts that are the target of attacks. A typical system configuration is one that will lock a user account after five unsuccessful logins attempts within a short period.
- **Intrusion detection and prevention:** The auditor should determine if there are any IDSs or IPSs that would detect authentication-bypass attempts. The auditor should examine these systems to see whether they have up-to-date configurations and signatures, whether they generate alerts, and whether the recipients of alerts act upon them.
- **Dormant accounts:** The IS auditor should determine if any automated or manual process exists to identify and close dormant accounts. Dormant accounts are user (or system) accounts that exist but are unused. These accounts represent a risk to the environment, as they represent an additional path between intruders and valuable or sensitive data.
- **Shared accounts:** The IS auditor should determine if there are any shared user accounts; these are user accounts that are routinely (or even infrequently) used by more than one person. The principal risk with shared accounts is the inability to determine accountability for actions performed with the account.
- **System accounts:** The IS auditor should identify all system-level accounts on networks, systems, and applications. The purpose of each system account should be identified, and it should be determined if each system account is still

required (some may be artefacts of the initial implementation or of an upgrade or migration). The IS auditor should determine who has the password for each system account, whether accesses by system accounts are logged, and who monitors those logs.

(ii) **Auditing Password Management:** Auditing password management requires attention to several key technologies and activities, including the following:

- **Password standards:** The IS auditor needs to examine password configuration settings on information systems to determine how passwords are controlled. Some of the areas requiring examination are- how many characters must a password have and whether there is a maximum length; how frequently must passwords be changed; whether former passwords may be used again; whether the password is displayed when logging in or when creating a new password etc.

(iii) **Auditing User Access Provisioning:** Auditing the user access provisioning process requires attention to several key activities, including:

- **Access request processes:** The IS auditor should identify all user access request processes and determine if these processes are used consistently throughout the organization.
- **Access approvals:** The IS auditor needs to determine how requests are approved and by what authority they are approved. The auditor should determine if system or data owners approve access requests, or if any accesses are ever denied.
- **New employee provisioning:** The IS auditor should examine the new employee provisioning process to see how a new employee's user accounts are initially set up. The auditor should determine if new employees' managers are aware of the access requests that their employees are given and if they are excessive.
- **Segregation of Duties (SOD):** The IS auditor should determine if the organization makes any effort to identify segregation of duties. This may include whether there are any SOD matrices in existence and if they are actively used to make user access request decisions.
- **Access reviews:** The IS auditor should determine if there are any periodic access reviews and what aspects of user accounts are reviewed; this may include termination reviews, internal transfer reviews, SOD reviews, and dormant account reviews.

(iv) **Auditing Employee Terminations:** Auditing employee terminations requires attention to several key factors, including:

- **Termination process:** The IS auditor should examine the employee termination process and determine its effectiveness. This examination should include understanding on how terminations are performed and how user account management personnel are notified of terminations.

- **Access reviews:** The IS auditor should determine if any internal reviews of terminated accounts are performed, which would indicate a pattern of concern for effectiveness in this important activity. If such reviews are performed, the auditor should determine if any missed terminations are identified and if any process improvements are undertaken.
- **Contractor access and terminations:** The IS auditor needs to determine how contractor access and termination is managed and if such management is effective.

(II) **User Access Logs:** The IS auditor needs to determine what events are recorded in access logs. The IS auditor needs to understand the capabilities of the system being audited and determine if the right events are being logged, or if logging is suppressed on events that should be logged.

- **Centralized access logs:** The IS auditor should determine if the organization's access logs are aggregated or if they are stored on individual systems.
- **Access log protection:** The auditor needs to determine if access logs can be altered, destroyed, or attacked to cause the system to stop logging events. For especially high-value and high-sensitivity environments, the IS auditor needs to determine if logs should be written to digital media that is unalterable, such as optical WORM (write once read many)media.
- **Access log review:** The IS auditor needs to determine if there are policies, processes, or procedures regarding access log review. The auditor should determine if access log reviews take place, who performs them, how issues requiring attention are identified, and what actions are taken when necessary.
- **Access log retention:** The IS auditor should determine how long access logs are retained by the organization and if they are back up.

(III) **Investigative Procedures:** Auditing investigative procedures requires attention to several key activities, including:

- **Investigation policies and procedures:** The IS auditor should determine if there are any policies or procedures regarding security investigations. This would include who is responsible for performing investigations, where information about investigations is stored, and to whom the results of investigations are reported.
- **Computer crime investigations:** The IS auditor should determine if there are policies, processes, procedures, and records regarding computer crime investigations. The IS auditor should understand how internal investigations are transitioned to law enforcement.
- **Computer forensics:** The IS auditor should determine if there are procedures

for conducting computer forensics. The auditor should also identify tools and techniques that are available to the organization for the acquisition and custody of forensic data. The auditor should identify whether any employees in the organization have received computer forensics training and are qualified to perform forensic investigations.

(IV) Internet Points of Presence: The IS auditor who is performing a comprehensive audit of an organization's system and network system needs to perform a "points of presence" audit to discover what technical information is available about the organization's Internet presence. Some of the aspects of this intelligence gathering include:

- **Search engines:** Google, Yahoo!, and other search engines should be consulted to see what information about the organization is available. Searches should include the names of company officers and management, key technologists, and any internal-only nomenclature such as the names of projects.
- **Social networking sites:** Social networking sites such as Facebook, LinkedIn, Myspace, and Twitter should be searched to see what employees, former employees, and others are saying about the organization. Any authorized or unauthorized "fan pages" should be searched as well.
- **Online sales sites:** Sites such as Craigslist and eBay should be searched to see if anything related to the organization is sold online.
- **Domain names:** The IS auditor should verify contact information for known domain names, as well as related domain names. For instance, for the organization mycompany.com; organizations should search for domain names such as mycompany.net, mycompany.info, and mycompany.biz to see if they are registered and what contents are available.
- **Justification of Online Presence:** The IS auditor should examine business records to determine on what basis the organization established online capabilities such as e-mail, Internet-facing web sites, Internet e-commerce, Internet access for employees, and so on. These services add risk to the business and consume resources. The auditor should determine if a viable business case exists to support these services or if they exist as a "benefit" for employees.

3.7.4 Managerial Controls and their Audit Trails

The auditors play a vital role in evaluating the performance of various controls under managerial controls. Some of the key areas that auditors should pay attention to while evaluating Managerial controls and its types are provided below:

I. Top Management and Information Systems Management Controls

The major activities that senior management must perform are – **Planning, Organizing, Leading** and **Controlling**. The Role of auditor at each activity is discussed below:

- **Planning:** Auditors need to evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not. A poor-quality information system is ineffective and inefficient leading to losing of its competitive position within the marketplace.
- **Organizing:** Auditors should be concerned about how well top management acquires and manages staff resources for three reasons:
  - The effectiveness of the IS function depends primarily on the quality of its staff. The IS staff need to remain up to date and motivated in their jobs.
  - Intense competition and high turnover have made acquiring and retaining good information system staff a complex activity.
  - Empirical research indicates that the employees of an organization are the most likely persons to perpetrate irregularities.
- **Leading:** Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership – for example, staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function. Auditors may use both formal and informal sources of evidence to evaluate how well top managers communicate with their staff.
- **Controlling:** Auditors should focus on subset of the control activities that should be performed by top management – namely, those aimed at ensuring that the information systems function accomplishes its objectives at a global level. Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.

II. System Development Management Controls

Three different types of audits may be conducted during system development process as discussed in the Table 3.7.1:

Table 3.7.1: Different types of Audit during System Development Process

Concurrent Audit	Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.
Post -implementation Audit	Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.
General Audit	Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements for systems effectiveness and efficiency.

An external auditor is more likely to undertake general audits rather than concurrent or post-implementation audits of the systems development process. For internal auditors, management might require that they participate in the development of material application systems or undertake post-implementation reviews of material application systems as a matter of course.

III. Programming Management Controls

Some of the major concerns that an Auditor should address under different activities involved in Programming Management Control Phase are provided in Table 3.7.2.

Table 3.7.2: Audit Trails under Programming Management Controls

Phase	Audit Trails
Planning	◆ They should evaluate whether nature of and extent of planning are appropriate to different types of s/w that are developed or acquired. ◆ They must evaluate how well the planning work is being undertaken.
Control	◆ They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. ◆ They must gather evidence on whether the control procedures are operating reliably. For example - they might first choose a sample if past and current software development and acquisition projects carried out at different locations in the organization they are auditing.
Design	◆ Auditors should find out whether programmers use some type of systematic approach to design. ◆ Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
Coding	◆ Auditors should seek evidence – ○ On the level of care exercised by programming management in choosing a module implementation and integration strategy. ○ To determine whether programming management ensures that programmers follow structured programming conventions. ○ To check whether programmers employ automated facilities to assist them with their coding work.
Testing	◆ Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. ◆ Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users. ◆ Auditors primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.
Operation and Maintenance	◆ Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. ◆ Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

IV. Data Resource Management Controls

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

V. Quality Assurance Management Controls

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

VI. Security Management Controls

- Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not;
- Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and
- Auditors check whether the organizations have opted for an appropriate insurance plan or not.

VII. Operations Management Controls

- Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.
- Auditors can use interviews, observations, and review of documentation to evaluate -
    - the activities of documentation librarians;
    - how well operations management undertakes the capacity planning ad performance monitoring function;
    - the reliability of outsourcing vendor controls;
    - whether operations management is monitoring compliance with the outsourcing contract; and
    - Whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.

3.7.5 Application Controls and their Audit Trails

Audit Trail Controls: Two types of audit trails that should exist in each subsystem are as follows:

- An **Accounting Audit Trail** to maintain a record of events within the subsystem; and
- An **Operations Audit Trail** to maintain a record of the resource consumption associated with each event in the subsystem.

We shall now discuss Audit Trails for Application Controls in detail.

I. Boundary Controls

This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources. This includes the following:

- Identity of the would-be user of the system;
- Authentication information supplied;
- Resources requested;
- Action privileges requested;
- Terminal Identifier;
- Start and Finish Time;
- Number of Sign-on attempts; and
- Resources provided/denied.

Accounting Audit Trail

- Action privileges allowed/denied.

Operations Audit Trail

- • Resource usage from log-on to log-out time.
- • Log of Resource consumption.

II. Input Controls

This maintains the chronology of events from the time data and instructions are captured and entered into an application system until the time they are deemed valid and passed onto other subsystems within the application system.

Accounting Audit Trail

- The identity of the person(organization) who was the source of the data;
- The identity of the person(organization) who entered the data into the system;
- The time and date when the data was captured;

- The identifier of the physical device used to enter the data into the system;
- The account or record to be updated by the transaction;
- The standing data to be updated by the transaction;
- The details of the transaction; and
- The number of the physical or logical batch to which the transaction belongs.

Operations Audit Trail

- Time to key in a source document or an instrument at a terminal;
- Number of read errors made by an optical scanning device;
- Number of keying errors identified during verification;
- Frequency with which an instruction in a command language is used; and
- Time taken to invoke an instruction using a light pen versus a mouse.

III. Communication Controls

This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.

Accounting Audit Trail

- Unique identifier of the source/sink node;
- Unique identifier of each node in the network that traverses the message; Unique identifier of the person or process authorizing dispatch of the message; Time and date at which the message was dispatched;
- Time and date at which the message was received by the sink node;
- Time and date at which node in the network was traversed by the message; and
- Message sequence number; and the image of the message received at each node traversed in the network.

Operations Audit Trail

- Number of messages that have traversed each link and each node;
- Queue lengths at each node; Number of errors occurring on each link or at each node; Number of retransmissions that have occurred across each link; Log of errors to identify locations and patterns of errors;
- Log of system restarts; and
- Message transit times between nodes and at nodes.

IV. Processing Controls

The audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.

Accounting Audit Trail

- To trace and replicate the processing performed on a data item.
- To follow triggered transactions from end to end by monitoring input data entry, intermediate results and output data values.
- To check for existence of any data flow diagrams or flowcharts that describe data flow in the transaction, and whether such diagrams or flowcharts correctly identify the flow of data.
- To check whether audit log entries recorded the changes made in the data items at any time including who made them.

Operations Audit Trail

- A comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used.
- A comprehensive log on software consumption – compilers used, subroutine libraries used, file management facilities used, and communication software used.

V. Database Controls

The audit trail maintains the chronology of events that occur either to the database definition or the database itself.

Accounting Audit Trail

- To confirm whether an application properly accepts, processes, and stores information.
- To attach a unique time stamp to all transactions.
- To attach before-images and after-images of the data item on which a transaction is applied to the audit trail.
- Any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.
- To not only test the stated input, calculation, and output rules for data integrity, but also should assess the efficacy of the rules themselves.

Operations Audit Trail

- To maintain a chronology of resource consumption events that affects the database definition or the database.

VI. Output Controls

The audit trail maintains the chronology of events that occur from the time the content of the output is determined until the time users complete their disposal of output because it no longer should be retained.

Accounting Audit Trail

- What output was presented to users;
- Who received the output;
- When the output was received; and
- What actions were taken with the output?

Operations Audit Trail

- To maintain the record of resources consumed – graphs, images, report pages, printing time and display rate to produce the various outputs.

3.8 ORGANIZATION STRUCTURE AND RESPONSIBILITIES

Organizations require structure to distribute responsibility to groups of people with specific skills and knowledge. The structure of an organization is called an organization chart (org chart).Organizing and maintaining an organization structure requires that many factors be considered. In most organizations, the organization chart is a living structure that changes frequently, based upon several conditions including the following:

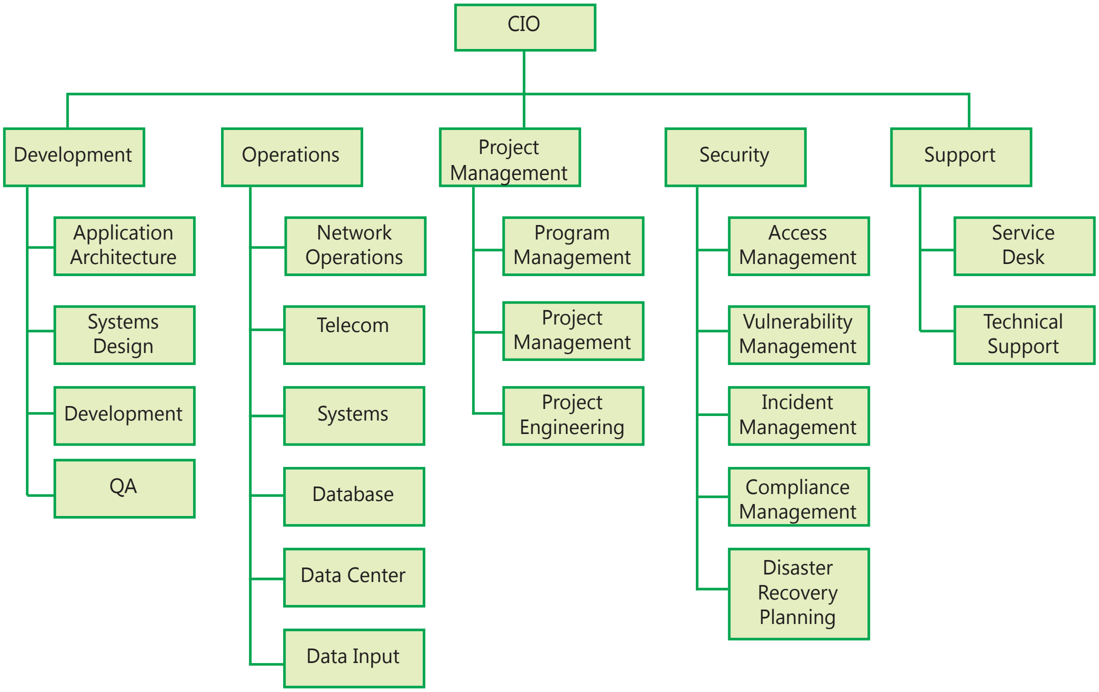


Fig. 3.8.1: Organization Structure - Example

Short- and long-term objectives: Organizations sometimes move departments from one executive to another so that departments that were once far from each other (in terms of the org chart structure) will be near each other. This provides new opportunities for developing synergies and partnerships that did not exist before the reorganization (reorg). These organizational changes are usually performed to help an organization meet new objectives that require new partnerships and teamwork that were less important before. Fig. 3.8.1 depicts an organization structure (illustrative only).

- **Market conditions:** Changes in market positions can cause an organization to realign its internal structure in order to strengthen itself. For example, if a competitor lowers its prices based on a new sourcing strategy, an organization may need to respond by changing its organizational structure to put experienced executives incharge of specific activities.
- **Regulation:** New regulations may induce an organization to change its organizational structure. For instance, an organization that becomes highly regulated may elect to move its security and compliance group away from IT and place it under the legal department, since compliance has much more to do with legal compliance than industry standards.
- **Available talent:** When someone leaves the organization (or moves to another position within the organization), particularly in positions of leadership, a space opens in the org chart that often cannot be filled right away. Instead, senior management will temporarily change the structure of the organization by moving the leaderless department under the control of someone else. Often, the decisions of how to change the organization will depend upon the talent and experience of existing leaders, in addition to each leader's workload and other factors. For example, if the director of IT program management leaves the organization, the existing department could temporarily be placed under the IT operations department, in this case because the director of IT operations used to run IT program management. Senior management can see how that arrangement works out and later decide whether to replace the director of IT program management position or to do something else.

3.8.1 Roles and Responsibilities

The topic of roles and responsibilities is multidimensional: it encompasses positions and relationships on the organization chart, it defines specific job titles and duties, and it denotes generic expectations and responsibilities regarding the use and protection of assets.

3.8.2 Individual Roles and Responsibilities

Several roles and responsibilities fall upon all individuals throughout the organization.

- **Executive management:** The most senior managers and executives in an organization are responsible for developing the organization's mission, objectives, and goals, as well as policy. Executives are responsible for enacting security policy, which defines (among other things) the protection of assets.
- **Owner:** An owner is an individual (usually but not necessarily a manager) who is the designated owner-steward of an asset. Depending upon the organization's security policy, an owner may be responsible for the maintenance and integrity of the asset, as well as for deciding who is permitted to access the asset. If the asset is information, the owner may be responsible for determining who may access and make changes to the information.
- **Manager:** A manager is, in the general sense, responsible for obtaining policies and procedures and making them available to their staff members. They should also, to some extent, be responsible for their staff members' behaviour.
- **User**: Users are individuals (at any level of the organization) who use assets in the performance of their job duties. Each user is responsible for how he or she uses the asset, and does not permit others to access the asset in his or her name. Users are responsible for performing their duties lawfully and for conforming to organization policies.

These generic roles and responsibilities should apply across the organization chart to include every person in the organization.

3.8.3 Job Titles and Job Descriptions

A Job Title is a label that is assigned to a job description. It denotes a position in the organization that has a given set of responsibilities, and which requires a certain level and focus of education and prior experience.

An organization that has a program of career advancement may have a set of career paths or career ladders that are models showing how employees may advance. For each job title, a career path will show the possible avenues of advancement to other job titles, and the experience required to reach those other job titles.

Job titles in IT have matured and are quite consistent across organizations. This consistency helps organizations in several ways:

- **Recruiting:** When the organization needs to find someone to fill an open position, the use of standard job titles will help prospective candidates more easily find positions that match their criteria.
- **Compensation baselining:** Because of the chronic shortage of talented IT workers, organizations are forced to be more competitive when trying to attract new workers. To remain competitive, many organizations periodically undertake a regional compensation analysis to better understand the levels of compensation

paid to IT workers in other organizations. The use of standard job titles makes the task of comparing compensation far easier.

- **Career advancement:** When an organization uses job titles that are consistent in the industry, IT workers have a better understanding of the functions of positions within their own organizations and can more easily plan how they can advance. The remainder of this section includes many IT job titles with a short description (not a full job description by any measure) of the function of that position.

Virtually all organizations also include titles that denote the level of experience, leadership, or span of control in an organization. These titles may include executive vice president, senior vice president, vice president, senior director, director, general manager, senior manager, manager and supervisor. Larger organizations will use more of these, and possibly additional titles such as district manager, group manager, or area manager.

(a) Executive Management: Executive managers are the chief leaders and policymakers in an organization. They set objectives and work directly with the organization's most senior management to help make decisions affecting the future strategy of the organization.

- **CIO (Chief Information Officer):** This is the title of the top most leader in a larger IT organization.
- **CTO (Chief Technical Officer):** This position is usually responsible for an organization's overall technology strategy. Depending upon the purpose of the organization, this position may be separate fromIT.
- **CSO (Chief Security Officer):** This position is responsible for all aspects of security, including information security, physical security, and possibly executive protection (protecting the safety of senior executives).
- **CISO (Chief Information Security Officer):** This position is responsible for all aspects of data-related security. This usually includes incident management, disaster recovery, vulnerability management, and compliance.
- **CPO (Chief Privacy Officer):** This position is responsible for the protection and use of personal information. This position is found in organizations that collect and store sensitive information for large numbers of persons.

(b) Software Development

Positions in software development are involved in the design, development, and testing of software applications.

- **Systems Architect:** This position is usually responsible for the overall information systems architecture in the organization. This may or may not include overall data architecture as well as interfaces to external organizations.

- **Systems Analyst:** A systems analyst is involved with the design of applications, including changes in an application's original design. This position may develop technical requirements, program design, and software test plans. In cases where organizations license applications developed by other companies, systems analysts design interfaces to other applications.
- **Software Developer, Programmer:** This position develops application software. Depending upon the level of experience, persons in this position may also design programs or applications. In organizations that utilize purchased application software, developers often create custom interfaces, application customizations, and custom reports.
- **Software Tester:** This position tests changes in programs made by software developers.

(c) Data Management

Positions in data management are responsible for developing and implementing database designs and for maintaining databases.

- **Database Architect:** This position develops logical and physical designs of data models for applications. With sufficient experience, this person may also design an organization's overall data architecture.
- **Database Administrator (DBA):** This position builds and maintains databases designed by the database architect and those databases that are included as a part of purchased applications. The DBA monitors databases, tunes them for performance and efficiency, and troubleshoots problems.
- **Database Analyst:** This position performs tasks that are junior to the database administrator, carrying out routine data maintenance and monitoring tasks.

(d) Network Management

Positions in network management are responsible for designing, building, monitoring, and maintaining voice and data communications networks, including connections to outside business partners and the Internet.

- **Network Architect:** This position designs data and (increasingly) voice networks and designs changes and upgrades to the network as needed to meet new organization objectives.
- **Network Engineer:** This position builds and maintains network devices such as routers, switches, firewalls, and gateways.
- **Network Administrator:** This position performs routine tasks in the network such as making minor configuration changes and monitoring event logs.
- **Telecom Engineer:** Positions in this role work with telecommunications

technologies such as data circuits, phone systems, and voice email systems.

(e) Systems Management

Positions in systems management are responsible for architecture, design, building, and maintenance of servers and operating systems. This may include desktop operating systems as well.

- **Systems Architect:** This position is responsible for the overall architecture of systems (usually servers), both in terms of the internal architecture of a system, as well as the relationship between systems. This position is usually also responsible for the design of services such as authentication, e-mail, and times synchronization.
- **Systems Engineer:** This position is responsible for designing, building, and maintaining servers and server operating systems.
- **Storage Engineer:** This position is responsible for designing, building, and maintaining storage subsystems.
- **Systems Administrator:** This position is responsible for performing maintenance and configuration operations on systems.

(f) General Operations

Positions in operations are responsible for day-to-day operational tasks that may include networks, servers, databases, and applications.

- **Operations Manager:** This position is responsible for overall operations that are carried out by others. Responsibilities will include establishing operations shift schedules.
- **Operations Analyst:** This position may be responsible for the development of operational procedures; examining the health of networks, systems, and databases; setting and monitoring the operations schedule; and maintaining operations records.
- **Controls Analyst:** This position is responsible for monitoring batch jobs, data entry work, and other tasks to make sure that they are operating correctly.
- **Systems Operator:** This position is responsible for monitoring systems and networks, performing backup tasks, running batch jobs, printing reports, and other operational tasks.
- **Data Entry:** This position is responsible for keying batches of data from hard copy sources.
- **Media Librarian:** This position is responsible for maintaining and tracking the use and whereabouts of backup tapes and other media.

(g) Security Operations

Positions in security operations are responsible for designing, building, and monitoring security systems and security controls, to ensure the confidentiality, integrity, and availability of information systems.

- **Security Architect:** This position is responsible for the design of security controls and systems such as authentication, audit logging, intrusion detection systems, intrusion prevention systems, and firewalls.
- **Security Engineer:** This position is responsible for designing, building, and maintaining security services and systems that are designed by the security architect.
- **Security Analyst:** This position is responsible for examining logs from firewalls, intrusion detection systems, and audit logs from systems and applications. This position may also be responsible for issuing security advisories to others inIT.
- **User Account Management:** This position is responsible for accepting approved requests for user access management changes and performing the necessary changes at the network, system, database, or application level. Often this position is carried out by personnel in network and systems management functions; only in larger organizations is user account management performed in security or even in a separate user access department.
- **Security Auditor:** This position is responsible for performing internal audits of IT controls to ensure that they are being operated properly.

(h) Service Desk

Positions at the service desk are responsible for providing front line support services to IT and IT's customers.

- **Help desk Analyst:** This position is responsible for providing front line user support services to personnel in the organization.
- **Technical Support Analyst:** This position is responsible for providing technical support services to other IT personnel, and perhaps also to IT customers.

3.9 SEGREGATION OF DUTIES

Information systems often process large volumes of information that is sometimes highly valuable or sensitive. Measures need to be taken in IT organizations to ensure that individuals do not possess sufficient privileges to carry out potentially harmful actions on their own. Checks and balances are needed, so that high-value and high-sensitivity activities involve the coordination of two or more authorized individuals. The concept of **Segregation of Duties (SOD)**, also known as separation of duties, ensures that single individuals do not possess excess privileges that could result in unauthorized activities such as fraud or the manipulation or exposure of sensitive data.

The concept of segregation of duties has been long-established in organization accounting departments where, for instance, separate individuals or groups are responsible for the creation of vendors, the request for payments, and the printing of checks. Since accounting personnel frequently handle checks and currency, the principles and practices of segregation of duties controls in accounting departments are the norm.

3.9.1 Segregation of Duties Controls

Preventive and detective controls should be put into place to manage segregation of duties matters. In most organizations, both the preventive and detective controls will be manual, particularly when it comes to unwanted combinations of access between different applications. However, in some transaction-related situations, controls can be automated, although they may still require intervention by others.

3.9.2 Some Examples of Segregation of Duties Controls

- **Transaction Authorization:** Information systems can be programmed or configured to require two (or more) persons to approve certain transactions. Many of us see this in retail establishments where a manager is required to approve a large transaction or a refund. In IT applications, transactions meeting certain criteria (for example, exceeding normally accepted limits or conditions) may require a manager's approval to be able to proceed.

- **Split custody of high-value assets:** Assets of high importance or value can be protected using various means of split custody. For example, a password to an encryption key that protects a highly-valued asset can be split in two halves, one half assigned to two persons, and the other half assigned to two persons, so that no single individual knows the entire password. Banks do this for central vaults, where a vault combination is split into two or more pieces so that two or more are required to open it.

- **Workflow:** Applications that are workflow-enabled can use a second (or third) level of approval before certain high-value or high-sensitivity activities can take place. For example, a workflow application that is used to provision user accounts can include extra management approval steps in requests for administrative privileges.

- **Periodic reviews:** IT or internal audit personnel can periodically review user access rights to identify whether any segregation of duties issues exist. The access privileges for each worker can be compared against a segregation of duties control matrix.

When SOD issues are encountered during a segregation of duties review, management will need to decide how to mitigate the matter. The choices for mitigating a SOD issue include

- **Reduce access privileges:** Management can reduce individual user privileges so that the conflict no longer exists.
- **Introduce a new mitigating control:** If management has determined that the person(s) need to retain privileges that are viewed as a conflict, then new preventive or detective controls need to be introduced that will prevent or detect unwanted activities. Examples of mitigating controls include increased logging to record the actions of personnel, improved exception reporting to identify possible issues, reconciliations of data sets, and external reviews of high-risk controls.

3.10 SUMMARY

In the present contemporary world, apart from change the thought-provoking terminology is business which is a driving force behind change and how to insight into trade is a dynamic called integration. Organizations of the 1990's concentrated on the re-engineering and redesign of their business processes to endorse their competitive advantage. To endure in the 21st century, organizations have started paying attention on integrating enterprise-wide technology solutions to progress their business processes called Business Information Systems (BIS). Now, every organization integrates part or all of its business functions together to accomplish higher effectiveness and yield. The thrust of the argument was that Information Technology (IT), when skillfully employed could in various ways differentiate an organization from its competition, add value to its services or products in the eyes of its customers, and secure a competitive advantage in comparison to its competition.

Although information systems have set high hopes to companies for their growth as it reduces processing speed and helps in cutting cost,but most of the research studies show that there is a remarkable gap between its capabilities and the business-related demands that senior management is placing on it. We learnt how any enterprise to be effective and efficient must use Business Process Automation (BPA), which is largely aided by Computers or IT. Information systems, which forms the backbone of any enterprise comprises of various layers such as: Application software, Database Management Systems (DBMS), System Software: Operating Systems, Hardware, Network Links and People-Users.

This Chapter has provided an overview on the importance of information systems in an IT environment and how information is generated. there has been a detailed discussion on Information System Audit, its need and the method of performing the same. Chapter outlines the losses that an organization may face, incase, it does not get it audited.

3.11 TEST YOUR KNOWLEDGE

3.11.1 Theory Questions

1. What does an Information System Model comprise of?

   (Refer Section 3.2)

2. Discuss important characteristics of Computer Based Information Systems.

   (Refer Section 3.2)

3. What do you understand by the term 'Operating System'? Discuss various operations performed by the Operating System.

   (Refer Section 3.3.2)

4. Mention different types of Application Software.

   (Refer Section 3.3.2)

5. Discuss advantages and disadvantages of Database Management Systems.

   (Refer Section 3.3.3)

6. What do you understand by Boundary Controls? Explain major Boundary Control techniques in brief.

   (Refer Section 3.5.3)

7. Briefly explain major update and report controls regarding Database Controls in brief.

   (Refer Section 3.5.3)

8. What do you mean by Corrective Controls? Explain with the help of examples. Also, discuss their broad characteristics in brief.

   (Refer Section 3.5.1)

9. What do you mean by Preventive Controls? Explain with the help of examples. Also, discuss their broad characteristics in brief.

   (Refer Section 3.5.1)

10. Write short notes on the following:

    (i) Snapshots (Refer Section 3.6.4)

    (ii) Audit Hooks (Refer Section 3.6.4)

11. As an IS Auditor of a company, you want to use SCARF technique for collecting some information, which you want to utilize for discharging some of your functions. Briefly describe the type of information that can be collected using SCARF technique.

(Refer Section 3.6.4)

12. What are the factors influencing an organization towards control and audit of computers?

    (Refer Section 3.6.1)

3.11.2 Multiple Choice Questions

1. Which of the following is not a component of Information Systems?
   (a) People
   (b) Data
   (c) Network
   (d) Transaction Processing System

2. Which of the following is not a functional unit of Central Processing Unit (CPU)?
   (a) Control unit
   (b) Input Devices
   (c) Registers
   (d) Arithmetic and Logic Unit

3. The full form of RAM is ____________.
   (a) Random Access Memory
   (b) Read Access Memory
   (c) Random Accessible Memory
   (d) Random Authorization Memory

4. Which of the following term is not used in Relational Database Models?
   (a) Relations
   (b) Attributes
   (c) Objects
   (d) Tables

5. Which of the following is not a Corrective Control?
   (a) Backup Procedure
   (b) Rerun Procedure
   (c) Contingency Planning
   (d) Hash Totals

6. ________ is the conversion of data into a secret code for storage in databases and transmission over networks.

   (a) Cipher Text

   (b) Encryption

   (c) Decryption

   (d) Logging

7. Under Data Coding Control, _____ occurs when a digit or character is removed from the end of a code.

   (a) Transposition Error

   (b) Substitution Error

   (c) Addition Error

   (d) Truncation Error

8. In computer networks, ________ refers to the ability of a network to recover from any kind of error like connection failure, loss of data etc.

   (a) Routing

   (b) Resilience

   (c) Contention

   (d) Bandwidth

9. Under Application Controls, _________maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources.

   (a) Boundary Controls

   (b) Input Controls

   (c) Communication Controls

   (d) Processing Controls

9. Under Application Controls, _________ maintains the chronology of events that occur either to the database definition or the database itself.

   (a) Output Controls

   (b) Input Controls

   (c) Database Controls

   (d) Processing Controls

10. Which of these is not a mobile operating system?

   (a) Android

   (b) iOS

(c) Tywin

(d) Windows Phone OS

11. Which of these is not an example of Relational Database?

(a) Access

(b) MySQL

(c) Java

(d) Oracle

13. VoIP stands for __________.

(a) Visual Over Internet Protocol

(b) Voice Over Internet Programme

(c) Voice Outside Internet Protocol

(d) Voice Over Internet Protocol

14. ________ technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions.

(a) Audit hooks

(b) SCARF

(c) Integrated Test Facility (ITF)

(d) Continuous and Intermittent Simulation (CIS)

15. SCARF stands for ___________.

(a) System Control Audit Review File

(b) System Control Audit Report File

(c) Simulation Control Audit Review File

(d) System Control Audit Review Format

Answers

1	(d)	2	(b)
3	(a)	4	(c)
5	(d)	6	(b)
7	(d)	8	(b)
9	(a)	10	(c)
11	(c)	12	(c)
13	(d)	14	(b)
15	(a)		