MANAGEMENT INFORMATION SYSTEMS

STUDY TEXT

Copyright

ISBN NO: 9966-760-16-4

First Published 2009

STRATHMORE UNIVERSITY PRESS

P.O. Box 59857, 00200,

Nairobi, Kenya.

Tel: +254 (0) 20 606155 Fax: +254 (0) 20 607498

Design Concept & Layout - Simplicity Ltd - P.O Box 22586-00400 Nairobi. Email: info@simplicityltd.com

Acknowledgment

We gratefully acknowledge permission to quote from the past examination papers of **Kenya Accountants and Secretaries National Examination Board (KASNEB).**

Table of Contents

STUDY TEXT

CHAPTER ONE

INTRODUCTION TO INFORMATION COMMUNICATION TECHNOLOGY AND FILE ORGANISATION

CHAPTER ONE

INTRODUCTION TO INFORMATION COMMUNICATION TECHNOLOGY AND FILE ORGANIZATION

▶ OBJECTIVES

When you have completed this chapter, you should be able to:

1. Identify the various applications of computers and computer systems in organisations.
2. Classify computers into generations.
3. Differentiate hardware and software devices and systems.
4. Describe desirable qualities of information.
5. Indentify computer files

▶ INTRODUCTION

The primary objective of an organization is to satisfy the needs of its clients. It is supposed to be effective and efficient whether it is profit motivated or not. These objectives are majorly achieved through computerisation of the systems, which are fast and economical to organisations.

▶ DEFINITION OF KEY TERMS

Computer - It may be defined as a device that works under the control of stored programmes automatically accept, store and process data to produce information that is the result of that processing.

Input devices - Enters programmes and data into a computer system

Central Processing Unit (CPU) - This is the part of the computer that processes data.

Output devices - They display information processed by the computer system.

Hardware - Refers to the physical, tangible computer equipment and devices

Software - This is a detailed step-by-step sequence of instructions known as programmes which guide computer hardware

Multiprogramming - Multiprogramming is a rudimentary form of parallel processing in which several programmes are run at the same time on a uniprocessor. Since there is only one processor, there can be no true simultaneous execution of different programmes. Instead, the operating system executes part of one programme, then part of another, and so on. To the user it appears that all programmes are executing at the same time.

Multiprocessing - Multiprocessing is the coordinated (simultaneous execution) processing of programmes by more than one computer processor. Multiprocessing is a general term that can mean the dynamic assignment of a programme to one of two or more computers working in tandem or can involve multiple computers working on the same programme at the same time (in parallel).

Multitasking - In a computer operating system, multitasking is allowing a user to perform more than one computer task (such as the operation of an application programme) at a time. The operating system is able to keep track of where you are in these tasks and switch from one task to the other without losing information. Microsoft Windows XP, Vista , IBM's OS/390, and Linux

are examples of operating systems that can do multitasking (almost all of today's operating systems can). When you open your Web browser and then open word at the same time, you are causing the operating system to do multitasking.

Multithreading - It is easy to confuse multithreading with multitasking or multiprogramming, which are somewhat different ideas. Multithreading is the ability of a programme or an operating system process to manage its use by more than one user at a time and to even manage multiple requests by the same user without having to have multiple copies of the programming running in the computer

▶ INDUSTRY CONTEXT

Business process improvement for increased product quality is of continuous importance in any organization. Quality managers' organisations need effective, hands-on tools for decision-making in engineering projects and for rapidly spotting key improvement areas. This is effectively delivered with the use of computers.

▶ EXAM CONTEXT

Introduction to Computers forms the basis of the Information systems study. It is a key field for examiners and the students should make sure that he/she understands the theoretical details to be able to apply the same knowledge to the subsequent topics as well as application questions in exams.

Fast Forward: A computer is a machine that manipulates data according to a list of instructions.

1. What is a computer?

A computer is an information-processing machine. It may also be defined as a device that works under the control of stored programmes that automatically accept, store and process data to produce information that is the result of that processing.

The forms of information processed include:

- Data – e.g. invoices, sales ledger, purchase ledger, payroll, stock controls, etc.
- Text – widely available in many offices with microcomputers
- Graphics – e.g. business graphs, symbols
- Images – e.g. pictures
- Voice – e.g. telephone

Processing includes creating, manipulating, storing, accessing and transmitting of data.

2. Why use computers?

Use of computers has become a necessity in many fields. Computers have revolutionised the way businesses are conducted. This is due to the advantages that computer systems offer over manual systems.

The advantages include:

- *Speed* – Computers have higher processing speeds than other means of processing, measured as number of instructions executed per second.
- *Accuracy* – Computers are not prone to errors. So long as the programmes are correct, they will always give correct output. Computers are designed in such a way that many of the inaccuracies, which could arise due to the malfunctioning of the equipment are detected and their consequences avoided in a way that is completely transparent to the user.
- *Consistency* – Given the same data and the same instructions, computers will produce exactly the same answer every time that particular process is repeated.
- *Reliability* – Computer systems are built with fault tolerance features, meaning that failure of one of the components does not necessarily lead to failure of the whole system.
- *Memory capability* – A computer has the ability to store and access large volumes of data.
- *Processing capability* – A computer has the ability to execute millions of instructions per second.
- *Storage* – Computers occupy less storage space compared to manual records.

3. Computer application areas

Some of the areas that computers are used include:

- **Communication** – digital communication using computers is popular and is being adopted worldwide as opposed to analogue communication using the telephony system. Computers have also enhanced communication through email communication, electronic data interchange, electronic funds transfer, Internet etc.

- **Banking** – the banking sector has incorporated computer systems in such areas as credit analysis, fund transfers, customer relations, automated teller machines, home banking, and online banking.

- **Organisational management** – the proliferation of management information systems have aided greatly the processes of managerial planning, controlling, directing as well as decision-making. Computers are used in organisations for transaction processing, managerial control as well as decision-support. Other specific areas where computer systems have been incorporated include sales and marketing, accounting, customer service, etc.

- **Science, research and engineering** – Computers are used:
  - as research tools and in carrying out complex computations
  - for simulation e.g. outer-space simulations, flight simulations
  - as diagnostic and monitoring tools.
  - for computerized maps using global positioning satellite (GPS) technology
  - for modern mass production methods in the auto industry using computer driven technology.

- **Education** – computers incorporate databases of information that are useful in organising and disseminating educational resources. Such e-learning and virtual or distributed classrooms have enabled the teaching industry to have a global reach to students. Computers are also used for marking uniform tests done in schools, school administration and computer aided instructions.

- **Management of information material** - The Internet has massive reference material on virtually every learning area. Computer systems have enabled the efficient administration of library materials for information storage and retrieval.

- **Manufacturing and production** – computer aided design (CAD), computer integrated manufacturing (CIM), process control systems among other technologies are among computer systems that have revolutionised the production industry. CAD and CIM are generic terms applied to the development and design of systems to support design work and to control manufacturing operations.

- **Entertainment** – use of computers in the entertainment industry has increased tremendously over the years. Computers enable high-quality storage of motion pictures and music files using high-speed and efficient digital storage devices such as CDs, VCDs and DVDs. The Internet is also a great source of entertainment resources. Computer games have also become a major source of entertainment.

- **Retailing** – computers are used in point of sale systems and credit card payment systems as well as stock inventories.

- **Home appliances** – computers (especially embedded computers or microprocessors) are included in household items for reasons of economy and efficiency of such items. Major appliances such as microwave ovens, clothes washers, refrigerators and sewing machines are making regular use of microprocessors.

- **Reservation systems** – guest booking, accommodation and bills accounting using computers in hotels have made the process to be more efficient and faster. Airline computer reservation systems have also enhanced and streamlined air travel across major airlines. Major players in the industry have also adopted online reservation systems.

- **Health care and medicine** – computers have played such an important role in the growth and improvement of health care that the use of computers in medicine has become a medical specialty in itself. Computers are used in such areas as maintenance of patient records, medical insurance systems, medical diagnosis and patient monitoring.

4. History of Computers

The first electronic computers were produced in the 1940s. Since then, many breakthroughs in electronics have occurred leading to great improvements in the capacity, processing speed and quality of computer resources.

The evolution of computerisation in business may be summarised as:

- **1870s:** Development of the typewriter allows speedier communication and less copying.
- **1920s:** Invention of the telephone enables both Wide Area Networks (WAN) and Local Area Networks (LAN) communication in real time. This marks the beginning of telecommunication.
- **1930s:** Use of scientific management is made available to analyse and rationalise data.
- **1940s**: Mathematical techniques developed in World War II (operations research) are applied to the decisionmaking process.
- **1950s:** Introduction of copying facilitates cheap and faster document production, and the (limited) introduction of Electronic Data Processing (EDP) speeds up large scale transaction processing.
- **1960s:** Emergence of Management Information Systems (MIS) provides background within which office automation can develop.
- **1970s**: Setting up of telecommunication networks to allow for distant communication between computer systems. There is widespread use of word processors in text editing and formatting, advancement in personal computing - emergence of PCs. Use of spreadsheets.
- **1980s**: Development of office automation technologies that combine data, text, graphics and voice. Development of DSS, EIS and widespread use of personal productivity software.
- **1990s**: Advanced groupware; integrated packages, combining most of the office work-clerical, operational as well as management.
- **2000s**: Wide spread use of Internet and related technology in many spheres of organisations including electronic commerce (e-commerce), e-learning, and e-health

Landmark Inventions

- ~500 B.C. - counting table with beads
- ~1150 in China - ABACUS - beads on wires
- 1642 Adding machine - Pascal
- 1822 Difference machine/Analytic Engine - design by Babbage
- 1890 Holerith punched card machine - for U.S. census
- 1944 Mark I (Harvard) - first *stored programme* computer
- 1947 ENIAC (Penn)- first *electronic* stored programme computer
- 1951 UNIVAC - first *commercial* computer; 1954 first installation
- 1964 IBM - first all-purpose computer (business + scientific)
- 1973 HP-65, hand-held, programmable 'calculator'
- ~1975 Altair, Intel - first Micro-computer; CPU on a "chip"

STUDY TEXT

5. Computer Generations

Fast Forward: The capabilities of a personal computer have changed greatly since the introduction of electronic computers.

The classification of computers into generations is based on the fundamental technology employed. Each new generation is characterised by greater speed, larger memory capacity and smaller overall size than the previous one.

i. First Generation Computers (1946 – 1957)

- Used vacuum tubes to construct computers.
- These computers were large in size and writing programmes on them was difficult.
- The following are major drawbacks of First Generation computers.
  - The operating speed was quite slow.
  - Power consumption was very high.
  - It required large space for installation.
  - The programming capability was quite low.
  - Cumbersome to operate – switching between programmes, input and output

ii. Second Generation Computers (1958 - 1964)

- Replaced vacuum tubes with transistors.
- The transistor was smaller, cheaper and dissipated less heat than a vacuum tube.
- The second generation also saw the introduction of more complex arithmetic and logic units, the use of high–level programming languages and the provision of system software with the computer.
- Transistors were smaller than electric tubes and had higher operating speed. They had no filament and required no heating. Manufacturing cost was also lower. Thus the size of the computer got reduced considerably.
- It is in the second generation that the concept of Central Processing Unit (CPU), memory, programming language and input and output units were developed. The programming languages such as COBOL, FORTRAN were developed during this period.

iii. Third Generation Computers (1965 - 1971)

- Had an integrated circuit.
- Although the transistor technology was a major improvement over vacuum tubes, problems remained. The transistors were individually mounted in separate packages and interconnected on printed circuit boards by separate wires. This was a complex, time consuming and error-prone process.
- The early integrated circuits are referred to as small-scale integration (SSI). Computers of this generation were smaller in size, cost less, had larger memory while processing speed was much higher.

iv. Fourth Generation Computers (1972 - Present)

- Employ Large Scale Integrated (LSI) and Very Large Scale Integrated (VLSI) circuit technology to construct computers. Over 1,000 components can be placed on a single integrated-circuit chip.

v. Fifth Generation Computers

- These are computers of 1990s
- Use Very Large Scale Integrated (VLSI) circuit technology to build computers. Over 10,000 components can be incorporated on a single integrated chip.
- The speed is extremely high in fifth generation computer. Apart from this, it can perform *parallel processing*. The concept of *Artificial intelligence* has been introduced to allow the computer to make its own decision.

6. Classification of computers

Computers can be classified in different ways as shown below:

Classification by processing

This is based on how the computer represents and processes the data:

a) **Digital computers** are computers which process data that is represented in the form of discrete values by operating on it in steps. *Digital computers* process data represented in the form of discrete values like 0, 1, 2. They are used for both business data processing and scientific purposes since digital computation results in greater accuracy.

b) **Analog computers** are used for scientific, engineering, and process-controlled purposes. Outputs are represented in the form of graphs. *Analogue computers* process data represented by physical variables and output physical magnitudes in the form of smooth graphs.

c) **Hybrid computers** are computers that have the combined features of digital and analog computers. They offer an efficient and economical method of working out special problems in science and various areas of engineering.

Classification by purpose

This is a classification based on the use to which the computer is put.

a) *Special purpose* computers are used for a certain specific function e.g. in medicine, engineering and manufacturing.

b) *General-purpose* computers can be used for a wide variety of tasks e.g. accounting and word processing

Classification by generation

This is a time-based classification coinciding with technological advances.
The computers are categorised as *First generation* through to *Fifth generation.*

a) *First generation.* These were computers of the early 1940s. They used a circuitry of wires and were vacuum tubes. Produced a lot of heat, took a lot of space, were very slow and expensive. Examples are LEO 1 and UNIVAC 1.

STUDY TEXT

b) *Second generation.* These were computers of the early 1950s. Made use of transistors and thus were smaller and faster. (200KHz). Examples include the IBM system 1000.

c) *Third generation.* These were computers of the 1960s. They made use of Integrated Circuits. They had speeds of up to 1MHz. Examples include the IBM system 360.

d) *Fourth generation.* These were computers of the 1970s and 1980s. They used Large Scale Integration (LSI) technology. They had speeds of up to 10MHz. Examples include the IBM 4000 series.

e) *Fifth generation.* These were computers of the 1990s. They used very Large Scale Integration (VLSI) technology and had speeds of up to 400MHz and above.

Classification by power and size/ configuration

a) *Supercomputers.* These are the largest and most powerful. Used to process large amounts of data very quickly. Useful for meteorological or astronomical applications. Examples include Cray and Fujitsu.

b) *Mainframe computers.* Large computers in terms of price, power and size. Require a carefully controlled environment and specialist staff to operate them. Used for centralised processing for large commercial organisations. Manufacturers include International Business Machine (IBM).

c) *Minicomputers.* Their size, speed and capabilities lie somewhere between mainframes and microcomputers. Used as departmental computers in large organisations or as the main computer in medium-sized organisations. Manufacturers of minicomputers include IBM and International Computer Limited (ICL).

d) *Microcomputers.* These are the personal computers commonly used for office and leisure activities. Examples include Hewlett Packard (HP), Compaq and Dell. They include desktops, laptops and palmtops.

STUDY TEXT

7. Data representation in computers

Data exists as electrical voltages in a computer. Since electricity can exist in two states, on or off, binary digits are used to represent data. Binary digits, or bits, can be “0” or “1”. The bit is the basic unit of representing data in a digital computer.

A bit is either a 1 or a 0. These correspond to two electronic/magnetic states of ON (1) and OFF (0) in digital circuits, which are the basic building blocks of computers. All data operated by a computer and the instructions that manipulate that data must be represented in these units. Other units are a combination of these basic units. Such units include:

- 1 byte (B) = 2^3 bits = 8 bits – usually used to represent one character e.g. ‘A’
- 1 kilobyte (KB) – 2^{10} bytes = 1024 bytes (usually considered as 1000 bytes)
- 1 megabyte (MB)– 2^{20} bytes = 1048576 bytes (usually considered as 1000000 bytes/1000 KB)
- 1 gigabyte (GB)– 2^{30} bytes = 1073741824 bytes (usually considered as 1,000,000,000 bytes/1000 MB)

- 1 terabyte (TB) – 2^{40} bytes = 1099511627776 bytes (usually considered as one trillion bytes/1000 GB)

Bit patterns (the pattern of 1s or 0s found in the bytes) represent various kinds of data:

- Numerical values (using the binary number system)
- Text/character data (using the ASCII coding scheme)
- Programme instructions (using the machine language)
- Pictures (using such data formats as gif, jpeg, bmp and wmf)
- Video (using such data formats as avi, mov and mpeg)
- Sound/music (using such data formats as wav, au and mp3)

Computer data is represented using number systems and either one of the character coding schemes.

Character Coding Schemes

(i) ASCII – American Standard Code for Information Interchange

ASCII is the most common format for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is represented with a 7-bit binary number (a string of seven 0s or 1s). 128 possible characters are defined.

Unix and DOS-based operating systems use ASCII for text files. Windows NT and 2000 uses a newer code, Unicode. IBM's S/390 systems use a proprietary 8-bit code called EBCDIC. Conversion programmes allow different operating systems to change a file from one code to another. ASCII was developed by the American National Standards Institute (ANSI).

(ii) EBCDIC – Extended Binary Coded Decimal Interchange Code

EBCDIC is a binary code for alphabetic and numeric characters that IBM developed for its larger operating systems. It is the code for text files that is used in IBM's OS/390 operating system for its S/390 servers and that thousands of corporations use for their legacy applications and databases. In an EBCDIC file, each alphabetic or numeric character is represented with an 8-bit binary number (a string of eight 0's or 1's). 256 possible characters (letters of the alphabet, numerals and special characters) are defined.

(iii) Unicode

Unicode is an entirely new idea in setting up binary codes for text or script characters. Officially called the Unicode Worldwide Character Standard, it is a system for "the interchange, processing, and display of the written texts of the diverse languages of the modern world." It also supports many classical and historical texts in a number of languages.

Number Systems

(i) Decimal system (base 10)

This is the normal human numbering system where all numbers are represented using base 10.

The decimal system consists of 10 digits namely 0 to 9. This system is not used by the computer for internal data representation. The position of a digit represents its relation to the power of ten.

E.g. $45780 = \{(0\times10^0) + (8\times10^1) + (7\times10^2) + (5\times10^3) + (4\times10^4)\}$

(ii) Binary system (base 2)

This is the system that is used by the computer for internal data representation whereby numbers are represented using base 2. Its basic units are 0 and 1, which are referred to as BITs (BInary digiTS). 0 and 1 represent two electronic or magnetic states of the computer that are implemented in hardware. The implementation is through the use of electronic switching devices called gates, which like a normal switch are in either one of two states: ON (1) or OFF (0).

The information supplied by a computer as a result of processing must be decoded in the form understandable to the user.

E.g. Number 15 in decimal is represented as 1111 in binary system:

$1111 = \{(1\times2^0) + (1\times2^1) + (1\times2^2) + (1\times2^3)\}$

$= 1 + 2 + 4 + 8 = 15$

(iii) Octal system (base 8)

Since binary numbers are long and cumbersome, more convenient representations combine groups of three or four bits into octal (base 8) digits respectively. In octal number system, there are only eight possible digits, that is, 0 to 7. This system is more popular with microprocessors because the number represented in octal system can be used directly for input and output operations. Complex binary numbers with several 1's and 0's can be conveniently handled in base eight. The binary digits are grouped into binary digits of threes and each group is used to represent an individual octal digit.

For example: the binary number 10001110011 can be handled as 2163 octal number.

That is

010	001	110	011
↓	↓	↓	↓
2	1	6	3

(iv) Hexadecimal (base 16)

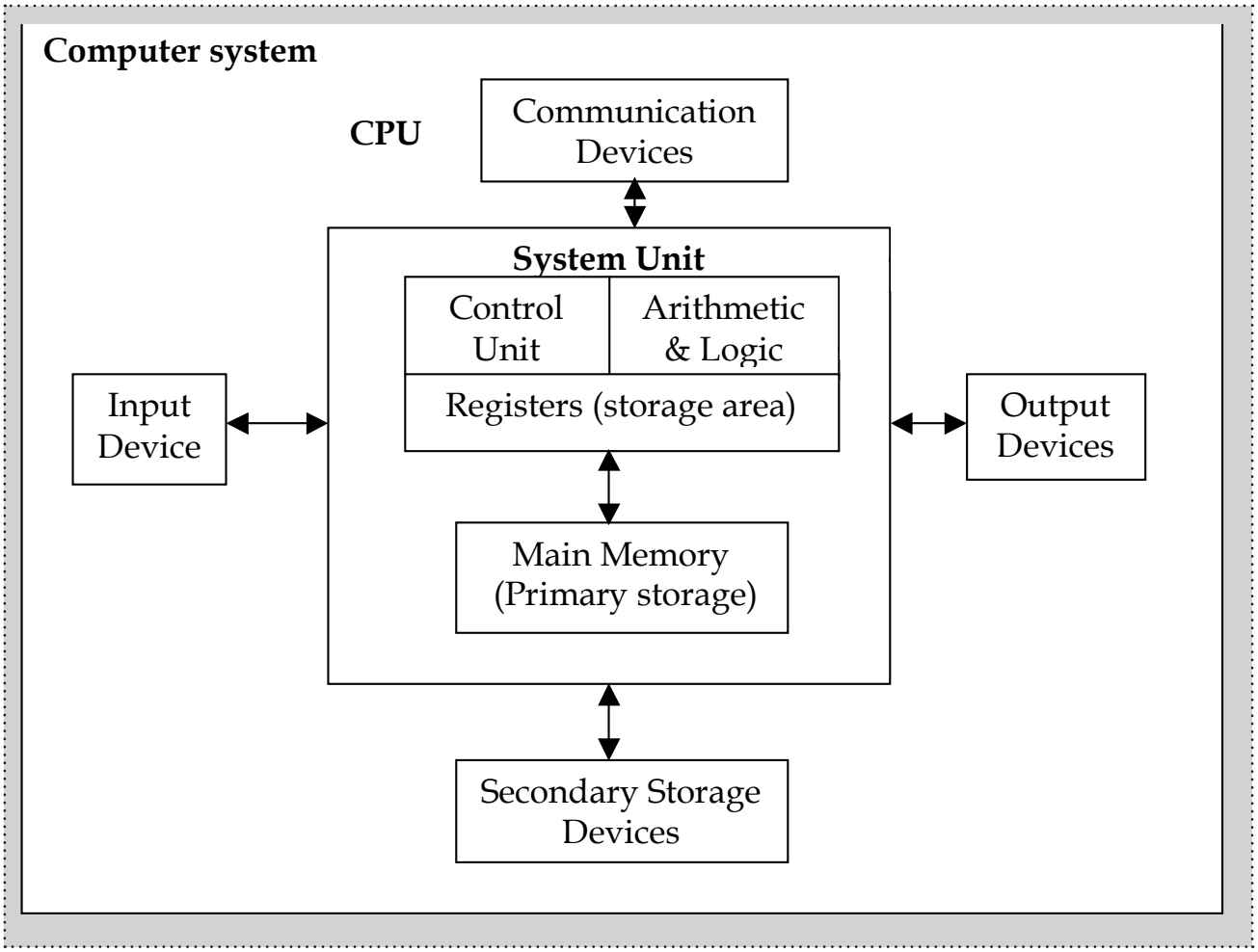
The hexadecimal number system is similar to octal system with the exception that the base is 16 and there must be 16 digits. The 16 symbols used in this system are the decimal digits 0 to 9 and alphabets A to F. Hexadecimal numbers are used because more complex binary notations can be simplified by grouping the binary digits into groups of four, each group representing a hexadecimal digit. For example, the binary number 0001.0010.1010.0000 can be handled in base 16 as 12A0.

That is

0001	0010	1010	0000
↓	↓	↓	↓
1	2	A	0

8. Functional/Logical parts of a digital computer

The system unit houses the processing components of the computer system. All other computer system devices are called peripherals, and are connected directly or indirectly into the system unit.



- **Input devices** – Enters programme and data into a computer system.
- **Central Processing Unit (CPU) –** This is the part of the computer that processes data. Consists of main memory, control unit and arithmetic and logic unit.
- **Main Memory** – Temporary storage to hold programmes and data during execution/ processing.
- **Control Unit** – Controls execution of programmes.
- **Arithmetic Logic Unit (ALU)** – Performs actual processing of data using programme instructions.
- **Output devices** – Displays information processed by the computer system.
- **Storage devices** – Permanent storage of data and programmes before and after it is processed by the computer system.
- **Communication devices –** Enable communication with other computers.

8.1 Hardware

Refers to the physical, tangible computer equipment and devices, which provide support for major functions such as input, processing (internal storage, computation and control), output, secondary storage (for data and programmes), and communication.

Hardware categories

A computer system is a set of integrated devices that input, output, process, and store data and information. Computer systems are currently built around at least one digital processing device. There are five main hardware components in a computer system: the central processing unit (CPU); primary storage (main memory); secondary storage; and input and output devices.

Basic elements of hardware

The basic elements that make up a computer system are:

a) **Input**
Most computers cannot accept data in forms customary to human communication such as speech or hand-written documents. It is necessary, therefore, to present data to the computer in a way that provides easy conversion into its own electronic pulse-based forms. This is commonly achieved by typing data using the keyboard or using an electronic mouse or any other input device.

- **Keyboard** can be connected to a computer system through a terminal. A terminal is a form of input and output device. A terminal can be connected to a mainframe or other types of computers called a host computer or server. There are four types of terminals namely dumb, intelligent, network and Internet.

- **Dumb Terminal**
  - Used to input and receive data only.
  - It cannot process data independently.
  - A terminal used by an airline reservation clerk to access a mainframe computer for flight information is an example of a dumb terminal

- **Intelligent Terminal**
  - Includes a processing unit, memory, and secondary storage.
  - It uses communications software and a telephone hookup or other communications link.
  - A microcomputer connected to a larger computer by a modem or network link is an example of an intelligent terminal.

- **Network Terminal**
  - Also known as a thin client or network computer.
  - It is a low cost alternative to an intelligent terminal.
  - Most network terminals do not have a hard drive.
  - This type of terminal relies on a host computer or server for application or system software.

- **Internet Terminal**
  - Is also known as a web terminal.
    - It provides access to the Internet and displays web pages on a standard television set.
    - It is used almost exclusively in homes.

- **Direct data entry devices –** Direct entry creates machine-readable data that can go directly to the CPU. It reduces human error that may occur during keyboard entry. Direct entry devices include pointing, scanning and voice-input devices.
- Pen input devices e.g. Lightpen
  Pen input devices are used to select or input items by touching the screen with the pen. Light pens accomplish this by using a white cell at the tip of the pen. When the light pen is placed against the monitor, it closes a photoelectric circuit. The photoelectric circuit identifies the spot for entering or modifying data. Engineers who design microprocessor chips or airplane parts use light pens.

- Touch sensitive screen inputs
  Touch sensitive screens, or touch screens allow the user to execute programmes or select menu items by touching a portion of a special screen. Behind the plastic layer of the touch screen are crisscrossed invisible beams of infrared light. Touching the screen with a finger can activate actions or commands. Touch screens are often used in ATMs, information centres, restaurants and stores. They are popularly used at petrol stations for customers to select the grade of fuel or request a receipt at the pump (in developed countries), as well as in fast-food restaurants to allow clerks to easily enter orders.

STUDY TEXT

Scanning Devices

Scanning devices, or scanners, can be used to input images and character data directly into a computer. The scanner digitises the data into machine-readable form.

- **The scanning devices used in direct-entry include the following:**
- **Image Scanner**– converts images on a page to electronic signals.
- **Fax Machine** – converts light and dark areas of an image into format that can be sent over telephone lines.
- **Bar-Code Readers** – photoelectric scanner that reads vertical striped marks printed on items.
- **Character and Mark Recognition Devices** – scanning devices used to read marks on documents.

Character and Mark Recognition Device Features

- Can be used by mainframe computers or powerful microcomputers.
- There are three kinds of character and mark recognition devices:
  - Magnetic-ink character recognition (MICR)
    Magnetic ink character recognition, or MICR, readers are used to read the numbers printed at the bottom of checks in special magnetic ink. These numbers are an example of data that is both machine readable and human

readable. The use of MICR readers increases the speed and accuracy of processing checks.

- Optical-character recognition (OCR)
  Read special preprinted characters, such as those on utility and telephone bills.
- Optical-mark recognition (OMR)
  Reads marks on tests – also called mark sensing. Optical mark recognition readers are often used for test scoring since they can read the location of marks on what is sometimes called a mark sense document. This is how, for instance, standardised tests such as the KCPE, SAT or GMAT are scored.

Voice–input devices

Voice-Input Devices can also be used for direct input into a computer. Speech recognition can be used for data input when it is necessary to keep your hands free. For example, a doctor may use voice recognition software to dictate medical notes while examining a patient. Voice recognition can also be used for security purposes to allow only authorised people into certain areas or to use certain devices.

- Voice-input devices convert speech into a digital code.
- The most widely used voice-input device is the microphone.
- A microphone, sound card and software form a voice recognition system.

Note:

Point-of-sale (POS) terminals (electronic cash registers) use both keyboard and direct entry.

- **Keyboard Entry** can be used to type in information.
- **Direct Entry** can be used to read special characters on price tags.

Point-of-sale terminals can use wand readers or platform scanners as direct entry devices.

- Wand readers or scanners reflect light on the characters.
- Reflection is changed by photoelectric cells to machine-readable code.
- Encoded information on the product's barcode e.g. price appear on terminal's digital display.

b) Storage

Data and instructions enter main storage and are held until when needed to be worked on. The instructions dictate action to be taken on the data. Results of the action will be held until they are required for output.

c) Control

Each computer has a control unit that fetches instructions from main storage, interprets them, and issues the necessary signals to the components making up the system. It directs all hardware operations necessary in obeying instructions.

d) Processing

Instructions are obeyed and the necessary arithmetic and logic operations are carried out on the data. The part that does this is called the Arithmetic and Logic Unit (ALU).

Processing devices

(i) The Central Processing Unit - CPU

The CPU (Central Processing Unit) controls the processing of instructions. The CPU produces electronic pulses at a predetermined and constant rate. This is called the clock speed. Clock speed is generally measured in megahertz, that is, millions of cycles per second.

It consists of:

- Control Unit (CU) – The electronic circuitry of the control unit accesses programme instructions, decodes them and coordinates instruction execution in the CPU.
- Arithmetic and Logic Unit (ALU) – Performs mathematical calculations and logical comparisons.
- Registers – These are high-speed storage circuitry that holds the instruction and the data while the processor is executing the instruction.
- Bus – This is a highway connecting internal components to one another.

(ii) Main Memory

The primary storage, also called main memory, although not a part of the CPU, is closely related to the CPU. Main memory holds programme instructions and data before and after execution by the CPU. All instructions and data pass through main memory locations. Memory is located physically close to the CPU to decrease access time, that is, the time it takes the CPU to retrieve data from memory. Although the overall trend has increased memory access time, memory has not advanced as quickly as processors. Memory access time is often measured in milliseconds, or one thousandths of a second.

e) Output

Results are taken from main storage and fed to an output device. This may be a printer, in which case the information is automatically converted to a printed form called hard copy or to a monitor screen for a soft copy of data or information.

Output devices

Output is human-readable information. Input (data) is processed inside the computer's CPU into meaningful output (information). Output devices translate the machine-readable information into human-readable information.

- Punched cards: characters are coded onto an 80-column card in columns by combining punches in different locations; a special card reader reads the cards and translates them into transactions for the computer. These are now used only for older applications.
- Paper tape punch

Printers

Output printouts on paper, often referred to as hard-copy output.

Categorised according to:

(i) Printing capacity

- Character printers – Print one character at a time.
- Line printers – Print one line at a time.
- Page printers – Print a whole page at a time.

(ii) Mode of printing

- Dot matrix printers
  Forms images via pins striking a ribbon against a paper. The print head typically have 9 or 24 pins. The images are relatively of poor quality since dots are visible upon close inspection. Though inexpensive compared to other types, they are noisy and low-end models are slow (speed varies with price).
- Ink jet printers
  Forms images by "shooting" tiny droplets of ink on paper. They offer relatively good image quality with so many small dots that they are not noticeable, even upon close inspection. They are relatively quiet compared to dot matrix and most can print colour images.
- Laser jet printers
  Form images using copier technology – a laser/LED (Light Emitting Diode) lights up dots to be blackened and toner sticks to these dot positions on the paper. They have excellent image quality – so many small dots that they are not noticeable, even upon close inspection. They are quieter than ink jet printers.
- Thermal Printers
  Form images using heat elements and heat–sensitive paper. It is very quiet and not widely used by home PC users. Some very expensive colour models are available. "Ink" in these computers is wax crayons.

Plotters

Plotters are typically used for design output. They are special-purpose output devices used to produce charts, maps, architectural drawings and three-dimensional representations. They can produce high-quality multi-colour documents or larger size documents. Plotters produce documents such as blueprints or schematics.

Monitors

Output device for soft-copy output (temporal screen display of output, which lasts as long as the monitor's power is on). They are the most frequently used output devices. Some are used on the desktop; others are portable. Two important characteristics of the monitor are size and clarity.

Voice-output devices

- Voice-output devices make sounds that resemble human speech.
- Voice-output devices use prerecorded vocalised sounds to produce output.
- The computer "speaks" synthesised words.
- Voice output is not as difficult to create as voice input.
- Most widely used voice-output devices are stereo speakers and headphones.
- Devices are connected to a sound card in the system unit.
- Sound card is used to capture sound as well as play it back.

Examples of voice output uses:

- Soft-drink machines, telephone, and in cars.
- Voice output can be used as a tool for learning.
- Can help students study a foreign language.
- Used in supermarkets at the checkout counter to confirm purchases.
- Most powerful capability is to assist the physically challenged.

Auxiliary/Secondary Storage devices

Secondary storage devices store a larger amount of data or instructions than does main memory, on a more permanent basis. On a per megabyte basis, secondary storage is also cheaper than primary storage. Secondary storage is also infinitely extendable, unlike main memory, which is finite. Secondary storage is not volatile. Secondary storage is also more portable than primary storage – that is, it is possible to remove it from a computer and use the device and its contents in another.

Types of secondary storage devices

- **Magnetic disks –** Stores bits as magnetic spots. Magnetic disks are similar to magnetic tapes in that areas are magnetised to represent bits. However, the disks' read/write head can go directly to the desired record, allowing fast data retrieval. Magnetic disks can range from small and portable, such as diskettes with 1.44MB of storage capacity, to large capacity fixed hard disks, which are more expensive and less portable.

    - Floppy disks (diskettes)
        - 5 ¼ floppy disks
        - 3 ½ floppy disks – The most common size with a capacity of 1.44 MB. They are not very fast and durable.
    - Hard disks/Fixed disks – Also called hard drives. Their capacity range from 20 to 120 GB. They are fast and durable though not foolproof. Most are internal, but disks that use removable cartridge are available. Disk compression can be used to increase capacity but slows down performance.

- **Optical Disks –** Store bits as "pits" and "lands" on surface of disk that can be detected (read) by a laser beam.

    - CD-ROM (Compact-Disk Read Only Memory) – Only read and cannot be erased for rewriting. Has a capacity of 650 MB
    - CD-R (Compact-Disk Recordable) / WORM (Write Once, Read Many) – Usually blank at first and can be written only once. Has a capacity of 650 MB
    - CD-RW (Compact Disk ReWritable) – Can be written and read more than once. Has a capacity of 650 MB.
    - DVD-ROM (Digital Video Disks) – They are similar to CDs except that they have high quality sound and high-resolution video. Has a normal capacity of 4.7 GB and up to 17 GB if double-sided with double layering. Use laser technology. They are a relatively new technology usually used in the entertainment industry.

- **Magnetic Tapes –** Magnetic tape is similar in composition to the kind of tape found in videotapes and audiotapes. A plastic film is coated with iron oxide, which is magnetised to represent bits.

    - Tape cartridges – Used in personal computers. Has up to 20 GB per tape (probably even more).
    - Tape reels – Used in minicomputers and mainframes.

- **Other Backup Options**
    - Zip drive/disk – Uses special diskettes that hold 100 MB, 250 MB or 750 MB
    - SyQuest drive – Uses special cartridges that hold 200 MB

- **RAID** - RAID stands for Redundant Arrays of Independent or Inexpensive Disks. RAID technology is fault tolerant; that is, it allows data to be stored so that no data or transactions are lost in the event of disk failure. RAID involves using multiple hard disks in a special controller unit and storing data across all the disks in conjunction with extra reconstruction information that allows data to be recovered if a hard disk fails.

- **Storage Area Network (SAN) –** A storage area network connects servers and storage devices in a network to store large volumes of data. Data stored in a storage area network can be quickly retrieved and backed up. The use of storage area networks is likely to increase in the near future.

- **Computer Output Microfilm (COM) -** Companies that must store significant numbers of paper documents often use computer output microfilm. These devices transfer data directly from the computer onto the microfilm, thus eliminating the intermediate step of printing the document on paper. Newspapers and journals typically archive old issues in this manner, although some are now using optical storage devices.

Storage capacity abbreviations
- KB - kilobyte - 1000 (thousand)
- MB - megabyte - 1,000,000 (million)
- GB - gigabyte - 1,000,000,000 (billion)
- TB - terabyte - 1,000,000,000,000 (trillion)

Communication devices

- Modem - Modems allow computers (digital devices) to communicate via the phone system (based on analog technology). It turns the computers' digital data into analog, sends it over the phone line, and then another modem at the other end of the line turns the analog signal back into digital data.
- Fax/modem - basic digital/analog modem enhanced with fax transmission hardware that enables faxing of information from computer to another fax/modem or a fax machine *(NOTE: a separate scanner must be connected to the computer in order to use the fax/modem to transfer external documents)*

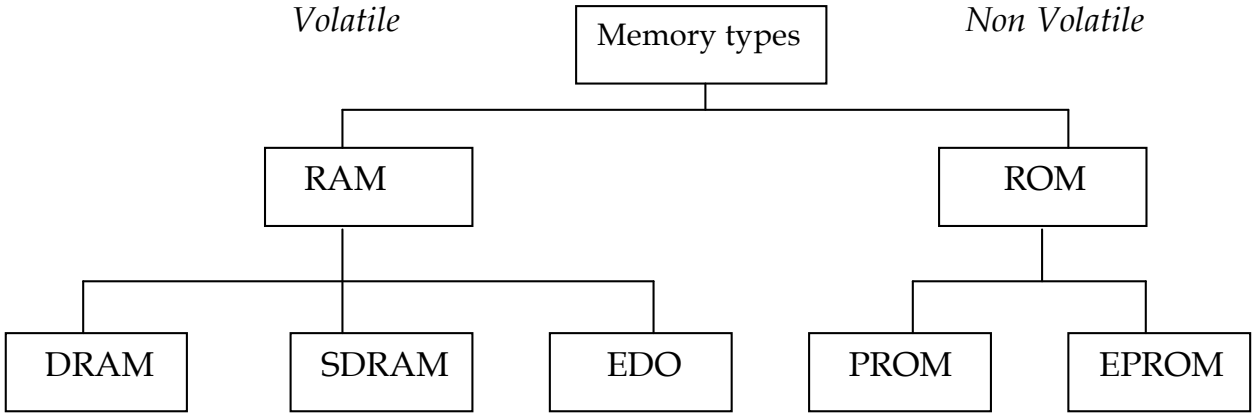
Computer Memory

Fast Forward: Although memory is technically any form of electronic storage, it is used most often to identify fast, temporary forms of storage.

Memory capability is one of the features that distinguish a computer from other electronic devices. Like the CPU, memory is made of silicon chips containing circuits holding data represented by on or off electrical states, or bits. Eight bits together form a byte. Memory is usually measured in megabytes or gigabytes.

A kilobyte is roughly 1,000 bytes. Specialised memories, such as cache memories, are typically measured in kilobytes. Often, both primary memory and secondary storage capacities today contain megabytes, or millions of bytes, of space.

Types of Memory



1. RAM (Random Access Memory) /RWM (Read Write Memory) – Also referred to as main memory, primary storage or internal memory. Its content can be read and can be changed and is the working area for the user. It is used to hold programmes and data during processing. RAM chips are volatile, that is, they loose their contents if power is disrupted. Typical sizes of RAM include 32MB, 64MB, 128MB, 256MB and 512MB.
    a. EDO – Extended Data Out
    b. DRAM – Dynamic RAM
    c. SDRAM – Synchronous

2. ROM (Read Only Memory) – Its contents can only be read and cannot be changed. ROM chips are non-volatile, so the contents aren't lost if the power is disrupted. ROM provides permanent storage for unchanging data and instructions, such as data from the computer maker. It is used to hold instructions for starting the computer called the bootstrap programme.

   ROM chips, the contents, or combination of electrical circuit states, are set by the manufacturer and cannot be changed. States are permanently manufactured into the chip.

   PROM: The settings must be programmed into the chip. After they are programmed, PROM behaves like ROM – the circuit states can't be changed. PROM is used when instructions will be permanent but they aren't produced in large enough quantities to make custom chip production (as in ROM) costeffective. PROM chips are, for example, used to store video game instructions.

   Instructions are also programmed into erasable programmable read-only memory. However, the contents of the chip can be erased and the chip can be reprogrammed. EPROM chips are used where data and instructions don't change often, but non-volatility and quickness are needed. The controller for a robot arm on an assembly line is an example of EPROM use.
    a. PROM (Programmable Read Only Memory) – It is written onto only once using special devices. Used mostly in electronic devices such as alarm systems.
    b. EPROM (Erasable Programmable Read Only Memory) – Can be written onto more than once.

3. Cache Memory - This is high-speed memory that a processor can access more quickly than RAM. Frequently used instructions are stored in cache since they can be retrieved more quickly, improving the overall performance of the computer. Level 1 (L1) cache is located on the processor; Level 2 (L2) cache is located between the processor and RAM.

8.2 Software

Software is detailed step-by-step sequence of instructions known as programme which guide computer hardware. A computer programme is a sequence of instructions that tell the computer hardware what to do. Programmes are written in (programming) languages, which consist of a set of symbols combined according to a given syntax.

A programme must be in main memory (RAM) to be executed. These invisible, intangible components of a computer that direct and control the operations of the hardware when processing data are referred to as software.

Software is classified into two major types: System and Application software.

System software

System software consists of programmes that coordinates the activities of hardware and other programs. System software is designed for a specific CPU and hardware class. The combination of a particular hardware configuration and operating system is called a computer platform. These programmes manage the “behind the scenes” operation of the computer.

Examples

- Operating systems
- Utility Programmes - Utility programmes often come installed in computer systems or packaged with operating systems. Utilities can also be purchased individually. Utility programmes perform useful tasks, such as virus detection, tracking computer jobs and compressing data.
- Language processors – Compilers and interpreters

Operating systems

The functions of an operating system include:

- Performing common hardware functions
  - Accepting input and store data on disks and send data to output devices
- Providing a user interface
- Providing hardware independence
- Managing system memory
- Managing processing
- Controlling access to system resources
  - Protection against unauthorised access

- Logins and passwords
- Managing files
  - Physical storage location
  - File permissions
  - File access

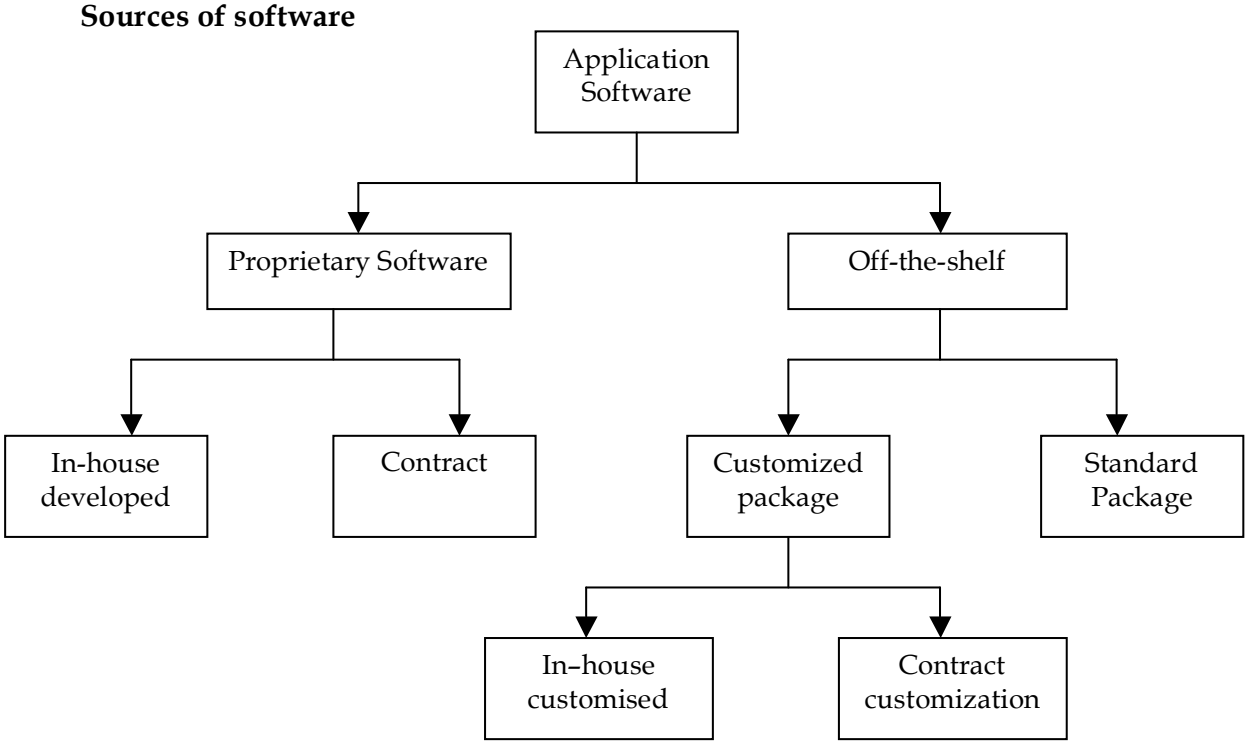
Examples of operating systems include:

- DOS – Disk Operating System
- Windows 3.1, 95, 98, NT, 2000, ME, XP
- Linux, Unix, MAC OS, System/7

Application software

Applications software include programmes designed to help end users solve particular problems using the computer or to perform specific tasks.

Sources of software



Proprietary Software

Is a computer software which is legal property of one party. The terms of use for other parties is defined by contracts or licensing agreements.

Advantages of proprietary software

- You can get exactly what you need in terms of reports, features etc.
- Being involved in development offers a further level in control over results.
- There is more flexibility in making modifications that may be required to counteract a new initiative by a competitor or to meet new supplier or customer requirements. A merger with another firm or an acquisition will also necessitate software changes to meet new business needs.

Disadvantages of proprietary software

- It can take a long time and significant resources to develop required features.
- Inhouse system development staff may become hard pressed to provide the required level of ongoing support and maintenance because of pressure to get on to other new projects.
- There is more risk concerning the features and performance of the software that has yet to be developed.

Off-the-Shelf Software

Off-the-shelf is a term for software or hardware, generally technology or computer products that are ready-made and available for sale, lease or license to the general public.

Advantages of off-the-shelf software

- The initial cost is lower since the software firm is able to spread the development costs over a large number of customers.
- There is lower risk that the software will fail to meet the basic business needs
- You can analyse existing features and performance of the package
- Package is likely to be of high quality since many customer firms have tested the software and helped identify many of its bugs.

Disadvantages of off-the-shelf software

- An organisation may have to pay for features that are not required or never used.
- The software may lack important features, thus requiring future modifications or customisation. This can be very expensive because users must adopt future releases of the software.
- Software may not match current work processes and data standards.

Application software is further classified into general-purpose software and applications which include:

- Word processing – Create, edit and print text documents, e.g. MS Word and Word Perfect.
- Spreadsheets – Provide a wide range of built-in functions for statistical, logical, financial, database, graphics, data and time calculations, e.g. Lotus 1-2-3, Excel and Quattro Pro.
- Database management systems (DBMS) – Store, manipulate and retrieve data. e.g. Access, FoxPro and dBase.
- Online Information Services – Obtain a broad range of information from commercial services. e.g. America Online and CompuServe
- Communications - Ms Outlook for email
- Browsers e.g Internet Explorer and Eudora
- Graphics – Develop graphs, illustrations and drawings. e.g. PaintShop, FreeHand and Corel
- Project Management – Plan, schedule, allocate and control people and resources needed to complete a project according to schedule. e.g. Project for Windows and Time Line.
- Financial Management – Provide income and expense tracking and reporting to monitor

and plan budgets, e.g. Quicken

- Desktop publishing - used to create high-quality printed output including text and graphics; various styles of pages can be laid out; art and text from other programmes can also be integrated into published pages, e.g. PageMaker and Publisher.
- Presentation packages like MS PowerPoint

Note: A software suite, such as Microsoft Office, offers a collection of powerful programmes including word processing, spreadsheet, database, graphics among others. The programmes in a software suite are designed to be used together. In addition, the commands, t icons and procedures are the same for all programmes in the suite.

Programming Languages

Programming languages are collections of commands, statements and words that are combined using a particular syntax, or rules, to write both systems and application software. This results in meaningful instructions to the CPU.

Generations of programming languages

Machine Language (1st Generation Languages)

A machine language consists of binary digit, that is, zeroes (0) and ones (1). Instructions and addresses are written in binary (0,1) code. Binary is the only "language" a CPU can understand. The CPU directly interprets and executes this language, therefore making its execution of instructions fast. Machine language programmes directly instructed the computer hardware, so they were not portable. That is, a programme written for computer model A could not be run on computer model B without being rewritten. All software in other languages must ultimately be translated down to machine language form. The translation process makes the other languages slower.

Advantage

- The only advantage is that programmes of machine languages run very fast because no translation programme is required for the CPU.

Disadvantages

- It is very difficult to programmes in machine language. The programmer has to know details of hardware to write the programme.
- The programmer has to remember a lot of codes to write a programme, which sometimes result in errors.
- It is difficult to debug a programme.

Assembly Language (2nd Generation Languages)

Uses symbols and codes instead of binary digits to represent programme instructions. It is a symbolic language meaning that instructions and addresses are written using alphanumeric labels that are meaningful to the programmer.

STUDY TEXT

The resulting programmes still directly instruct the computer hardware. For example, an assembly language instruction might move a piece of data stored at a particular location in RAM into a particular location on the CPU. Therefore, like their first generation counterparts, second generation programmes were not easily portable.

Assembly languages were designed to run in a small amount of RAM. Furthermore, they are low-level languages; that is the instructions directly manipulate the hardware. Therefore, programmes written in assembly language execute efficiently and quickly. As a result, more systems software is still written using assembly languages.

The language has a one-to-one mapping with machine instructions but has macros added to it. A macro is a group of multiple machine instructions, which are considered as one instruction in assembly language. A macro performs a specific task, for example adding and subtracting. A one-to-one mapping means that for every assembly instruction, there is corresponding single or multiple instructions in machine language.

An assembler is used to translate the assembly language statements into machine language.

Advantages:

- The symbolic programming of Assembly Language is easier to understand and saves a lot of time and effort of the programmer.
- It is easier to correct errors and modify programme instructions.
- Assembly Language has the same efficiency of execution as the machine level language This is because this is a one-to-one translator between assembly language programme and its corresponding machine language programme.

Disadvantages:

- One of the major disadvantages is that assembly language is machine dependent. A programme written for one computer might not run in other computers with a different hardware configuration.

High-level languages (3rd Generation Languages)

Third generation languages are easier to learn and use than were earlier generations. Thus programmers are more productive when using third generation languages. For most applications, this increased productivity and compensates for the decrease in speed and efficiency of the resulting programmes. Furthermore, programmes written in third generation languages are portable, that is, a program written to run on a particular type of computer can be run with little or no modification on another type of computer. Portability is possible because third generation languages are “high-level languages”; that is, instructions do not directly manipulate the computer hardware.

Third generation languages are sometimes referred to as “procedural” languages since programme instructions, must give the computer detailed instructions of how to reach the desired result.

High-level languages incorporated greater use of symbolic code. Its statements are more English–like, for example print, get and while. They are easier to learn but the resulting programme is slower in execution. Examples include Basic, Cobol, C and Fortran. They have first to be compiled (translated into corresponding machine language statements) through the use of compilers.

Advantages of High Level Languages

- Higher level languages have a major advantage over machine and assembly languages since they hig are easy to learn and use.
- Are portable

Fourth Generation Languages (4GLs)

Fourth generation languages are even easier to use, and more English-like, than are third generation languages. Fourth generation languages are sometimes referred to as "non-procedural", since programmes tell the computer what it needs to accomplish, but do not provide detailed instructions as to how it should accomplish it. Since fourth generation languages concentrate on the output, not procedural details, they are more easily used by people who are not computer specialists, that is, by end users.

Many of the first fourth generation languages were connected with particular database management systems. These languages were called Query Languages since they allow people to retrieve information from databases. Structured query language, SQL, is a current fourth generation language used to access many databases. There are also some statistical fourth generation languages, such as SAS and SPSS.

Some fourth generation languages, such as Visual C++, Visual Basic, or PowerBuilder are targeted to more knowledgeable users, since they are more complex to use. Visual programming languages, such as visual basic, use windows, icons, and pull down menus to make programming easier and more intuitive.

Object Oriented Programming

First, second, third and fourth generation programming languages were used to construct programmes that contained procedures to perform operations, such as draw or display, on data elements defined in a file.

Object oriented programmes consist of objects, such as a time card, that include descriptions of the data relevant to the object, as well as the operations that can be done on that data. For example, included in the time card object, would be descriptions of such data such as employee name, hourly rate, start time and. The time card object would also contain descriptions of such operations as calculating total hours worked or calculating total pay.

Language translators

Although machine language is the only language the CPU understands, it is rarely used anymore since it is so difficult to use. Every programme that is not written in machine language must be translated into machine language before it can be executed. This is done by a category of system software called language translation software. These are programmes that convert the code originally written by the programmer, called source code, into its equivalent machine language programme, called object code.

There are two main types of language translators: interpreters and compilers.

Interpreters

While a programme is running, interpreters read, translate, and execute one statement of the programme at a time. The interpreter displays any errors immediately on the monitor. Interpreters

are very useful for people learning how to programme or debugging a programme. However, the line-by-line translation adds significant overhead to the programme execution time leading to slow execution.

Compilers

A compiler uses a language translation programme that converts the entire source programme into object code, known as an object module, at one time. The object module is stored and it is the module that executes when the programme runs. The programme does not have to be compiled again until changes are made in the source code.

Software trends and issues

Open source software coming to the scene: This is software that is freely available to anyone and can be easily modified. The use of open source software has increased dramatically due to the World Wide Web. Users can download the source code from web sites. Open source software is often more reliable than commercial software because there are many users collaborating to fix problems. The biggest problem with open source software is the lack of formal technical support. However, some companies that package open source software with various add-ons and sell it with support are addressing this. An example of this is Red Hat Linux operating system.

9. Data resources

Data

Data, the raw materials for information are defined as groups of non-random symbols that represent quantities, actions, objects, etc. In information systems, data items are formed from characters that may be alphabetical, numeric or special symbols. Data items are organised for processing purposes into data structures, file structures and databases. Data relevant to information processing and decision-making may also be in the form of text, images or voice.

Information

Information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or prospective actions or decisions. It is important to note that data for one level of an information system may be information for another. For example, data input to the management level is information output of a lower level of the system such as operations level. Information resources are reusable. When retrieved and used, it does not lose value: it may indeed gain value through the credibility added by use.

The value of information is described most meaningfully in the context of making a decision. If there were no current or future choices or decisions to be made, information would be unnecessary. The value of information in decision-making is the value of change in decision behaviour caused by the information less the cost of obtaining the information. Decisions, however, are sometimes made without the “right” information. The reasons are:

- The needed information is unavailable
- The effort to acquire the information is too great or too costly.
- There is no knowledge of the availability of the information.
- The information is not available in the form needed.

Much of the information that organisations or individuals prepare has value other than in decision-making. The information may also be prepared for motivation and background building.

Desirable qualities of information

- Availability – It should be available and accessible to those who need it.
- Comprehensible – It should be understandable to those who use it.
- Relevance – Information should be applicable to the situations and performance of organizational functions. Relevant information is important to the decision maker.
- Secure – It should be secure from access by unauthorized users.
- Usefulness – It should be available in a form that is usable.
- Timeliness - Information should be available when it is needed.
- Reliability – Reliable information can be depended on. In many cases, reliability of information depends on the reliability of the data collection method use. In other instances, reliability depends on the source of information.
- Accuracy – It should be correct, precise and without error. In some cases, inaccurate information is generated because inaccurate data is fed into the transformation process (this is commonly called garbage in garbage out, GIGO).
- Consistency – It should not be self-contradictory.
- Completeness – Complete information contains all the important facts. For example an investment report that does not contain all the costs is not complete.
- Economical – Information should always be relatively economical to produce. Decision makers must always balance the value of information and the cost of producing it.
- Flexibility – Flexible information can be used for a variety of purposes.

Data Processing

Data processing may be defined as those activities, which are concerned with the systematic recording, arranging, filing, processing and dissemination of facts relating to the physical events occurring in the business. Data processing can also be described as the activity of manipulating the raw facts to generate a set or an assembly of meaningful data(information). Data processing activities include data collection, classification, sorting, adding, merging, summarising, storing, retrieval and dissemination.

The black box model is an extremely simple principle of a machine, that is, irrespective of how a machine operates internally, it takes an input, operates on it and then produces an output.

Processing

In dealing with digital computers, this data consists of: numerical data, character data and special (control) characters.

Use of computers for data processing involves four stages:

- Data input – This is the process of capturing data into the computer system for processing. Input devices are used.
- Storage – This is an intermediary stage where input data is stored within the computer system or on secondary storage awaiting processing or output after processing.

Programme instructions to operate on the data are also stored in the computer.

- Processing – The central processing unit of the computer manipulates data using arithmetic and logical operations.
- Data output – The results of the processing function are output by the computer using a variety of output devices.

Data processing activities

The basic processing activities include:

- Recording – bring facts into a processing system in usable form
- Classifying – data with similar characteristics are placed in the same category, or group.
- Sorting – arrangement of data items in a desired sequence
- Calculating – apply arithmetic functions to data
- Summarizing – to condense data or to put it in a briefer form
- Comparing – perform an evaluation in relation to some known measures
- Communicating – the process of sharing information
- Storing – to hold processed data for continuing or later use.
- Retrieving – to recover data previously stored

Information processing

This is the process of turning data into information by making it useful to some person or process.

Computer files

A file is a collection of related data or information that is normally maintained on a secondary storage device. The purpose of a file is to keep data in a convenient location where they can be located and retrieved as needed. The term computer file suggests organised retention on the computer that facilitates rapid, convenient storage and retrieval.

As defined by their functions, two general types of files are used in computer information systems: master files and transaction files.

Master files

Master files contain information to be retained over a relatively period of long time. Information in master files is updated continuously to represent the current status of the business.

An example is an accounts receivable file. This file is maintained by companies that sell to customers on credit. Each account record will contain such information as account number, customer name and address, credit limit amount, the current balance owed, and fields indicating the dates and amounts of purchases during the current reporting period. This file is updated each time the customer makes a purchase. When a new purchase is made, a new account balance is computed and compared with the credit limit. If the new balance exceeds the credit limit, an exception report may be issued and the order may be held up pending management approval.

Transaction files

Transaction files contain records reflecting current business activities. Records in transaction files are used to update master files.

To continue with the illustration, records containing data on customer orders are entered into transaction files. These transaction files are then processed to update the master files. This is known as posting transaction data to master file. For each customer transaction record, the corresponding master record is accessed and updated to reflect the last transaction and the new balance. At this point, the master file is said to be current.

Accessing Files

Files can be accessed:

- Sequentially - start from the first record and read one record after another until the end of file or when desired record is found
  - known as “sequential access”
  - only possible access for serial storage devices
- Directly - read desired record directly
  - known as “random access” or “direct access”

File Organisation

Files need to be properly arranged and organised to facilitate easy access and retrieval of the information. Types of file organisation (physical method of storage) include:

- Serial
- Sequential
- Indexed-Sequential
- Random

All file organisation types apply to direct access storage media (disk, drum etc.)

A file on a serial storage media (e.g. tape) can only be organised serially

Serial Organisation

- Each record is placed in turn in the next available storage space
- A serial file must be accessed sequentially implying
  - good use of space
  - high access time
- Usually used for temporary files, e.g. transaction files, work files and spool files
  Note: The method of accessing the data on the file is different to its organisation
  - E.g. sequential access of a randomly organised file
  - E.g. direct access of a sequential file

Sequential organisation

- Records are organised in ascending sequence according to a certain key
- Sequential files are accessed sequentially, one record after the other
- Suitable:
  - for master files in a batch processing environment
  - where a large percentage of records (high hit-rate) are to be accessed
- Not suitable for online access that requires a fast response as file needs to be accessed sequentially

Indexed-Sequential

- Most commonly used methods of file organisation

- File is organised sequentially and contains an index
- Used on direct access devices
- Used in applications that require sequential processing of large numbers of records but occasional direct access of individual records
- Increases processing overheads with maintenance of the indices

Random organisation

- Records are stored in a specific location determined by a randomising algorithm
  - *function (key) = record location (address)*
- Records can be accessed directly without regard to physical location
- Used to provide fast access to any individual record
  e.g. airline reservations and online banking

Problems of traditional file- based approach

Each function in an organisation develops specific applications in isolation from other divisions with each application using its own data files. This leads to the following problems:

- Data redundancy
  - duplicate data in multiple data files
- Redundancy leads to inconsistencies
  - in data representation e.g. refer to the same person as client or customer
  - values of data items across multiple files▪
- Data isolation — multiple files and formats
- Programme-data dependence
  - tight relationship between data files and specific programs used to maintain files
- Lack of flexibility
  - Need to write a new programme to carry out each new task▪ .
- Lack of data sharing and availability
- Integrity problems
  - Integrity constraints (e.g. account balance > 0) become part of programme code
  - Hard to add new constraints or change existing ones
- Concurrent access by multiple users difficult
  - Concurrent access needed for performance
  - Uncontrolled concurrent access can lead to inconsistencies
  - E.g. two people reading a balance and updating it at the same time
- Security problems

Data files and databases

A data file is a structured collection of data (information). The data are related in some manner. It is organised so that relationships within the data are revealed (revealable). A data file stores several (many) pieces of information about many data objects. The simplest and most efficient metaphor of how data is organised in a data file is as a table of rows and columns, like a spreadsheet but without the linkages between individual cells. A data file is made up of a number of records; each row in a table is a separate record. Each record is made up of all the data about a particular entity in the file.

A record includes many data items, each of which is a separate cell in the table. Each column in the table is a field; it is a set of values for a particular variable, and is made up of all the data items for that variable. Examples include phone book, library catalogue, hospital patient records and species information.

A database is an organised collection of (one or more) related data file(s). The way the database organises data depends on the type of database, called its data model, which, may be hierarchical, network and relational models.

Benefits of the database approach

- Provide Data Independence
  - separating the physical (how) and logical (what) aspects of the system
- Physical data independence
  - protects the application programmes from changes in the physical placement, of the files
  - the ability to modify the physical schema without changing the logical schema
- Logical data independence
  - Modify logical schema without changing application programmes
- Reduce redundancy
  - reduce duplicate data items
  - some redundancy may be necessary for business or technical reasons - DBA must ensure updates are propagated (a change to one is automatically applied to the other).
- Avoid inconsistency (by reducing redundancy)
  - if it is necessary - propagate updates
- Maintain integrity - i.e. ensure the data is accurate by:
  - reducing redundancy
  - implementing integrity rules, e.g. through foreign keys
- Share data
  - among existing applications
  - used in new applications
- Allow implementation of security restrictions
  - establish rules for different types of users for different types of update to database
- Enforce standards for
  - data representation - useful for migrating data between systems
  - data naming & documentation - aids data sharing and understandability
- Balance conflicting requirements
  - structure the corporate data in a way that is best for the organisation

Database Management Systems (DBMS)

DBMSs are system software that aid in organising, controlling and using the data needed by application programmes. A DBMS provides the facility to create and maintain a well-organised database. It also provides functions such as normalisation to reduce data redundancy, decrease access time and establish basic security measures over sensitive data.

DBMS can control user access at the following levels:

- User and the database
- Programme and the database
- Transaction and the database
- Programme and data field
- User and transaction
- User and data field

STUDY TEXT

The following are some of the advantages of DBMS:

- Data independence for application systems
- Ease of support and flexibility in meeting changing data requirements
- Transaction processing efficiency
- Reduction of data redundancy (similar data being held at more than one point – utilises more resources) – have one copy of the data and avail it to all users and applications
- Maximises data consistency – users have same view of data even after an update
- Minimises maintenance costs through data sharing
- Opportunity to enforce data/programming standards
- Opportunity to enforce data security
- Availability of stored data integrity checks
- Facilitates terminal users ad hoc access to data, especially designed query languages/ application generators

Most DBMS have internal security features that interface with the operating system access control mechanism/package, unless it was implemented in a raw device. A combination of the DBMS security features and security package functions is often used to cover all required security functions. This dual security approach, however, introduces complexity and opportunity for security lapses.

DBMS architecture

Data elements required to define a database are called metadata. There are three types of metadata: conceptual schema metadata, external schema metadata and internal schema metadata. If any one of these elements is missing from the data definition maintained within the DBMS, the DBMS may not be adequate to meet users' needs. A Data Definition Language (DDL) is a component used for creating the schema representation necessary for interpreting and responding to the users' requests.

Data Dictionary and Directory Systems (DD/DS) have been developed to define and store in source and object forms all data definitions for external schemas, conceptual schemas, the internal schema and all associated mappings. The data dictionary contains an index and description of all the items stored in the database. The directory describes the location of the data and access method. Some of the benefits of using DD/DS include:

- Enhancing documentation
- Providing common validation criteria
- Facilitating programming by reducing the needs for data definition
- Standardising programming methods

Database structure

The common database models are:

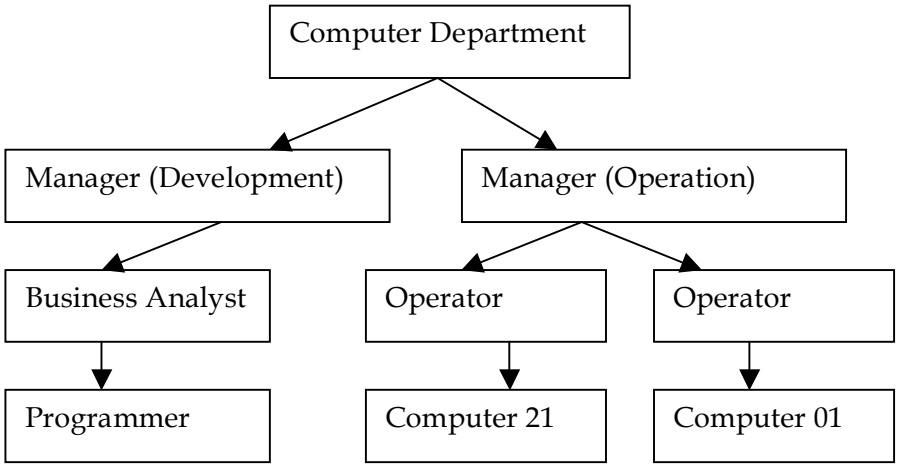
- Hierarchical database model
- Network database model
- Relational database model
- Object–oriented model

Hierarchical database model

This model allows the data to be structured in a parent/child relationship (each parent may have many children, but each child would be restricted to having only one parent). Under this model, it

is difficult to express relationships when children need to relate to more than one parent. When the data relationships are hierarchical, the database is easy to implement, modify and search.

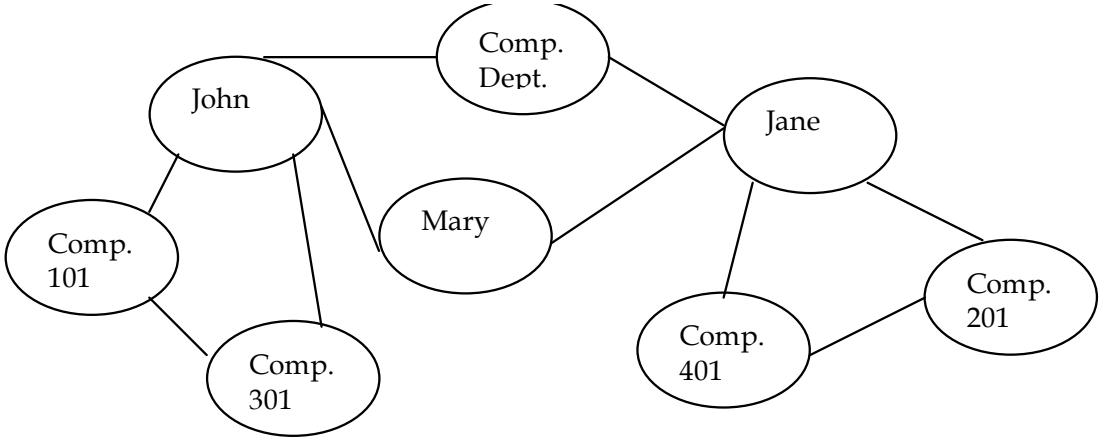
A hierarchical structure has only one root. Each parent can have numerous children, but a child can have only one parent. Subordinate segments are retrieved through the parent segment. Reverse pointers are not allowed. Pointers can be set only for nodes on a lower level; they cannot be set to a node on a predetermined access path.



Network Database Model

This model allows children to relate to more than one parent. A disadvantage to the network model is that such structure can be extremely complex and difficult to comprehend, modify or reconstruct in case of failure. The network structure is effective in stable environments where the complex interdependencies of the requirements have been clearly defined.

The network structure is more flexible, yet more complex, than the hierarchical structure. Data records are related through logical entities called sets. Within a network, any data element can be connected to any item. Because networks allow reverse pointers, an item can be an owner and a member of the same set of data. Members are grouped together to form records, and records are linked together to form a set. A set can have only one owner record but several member records.

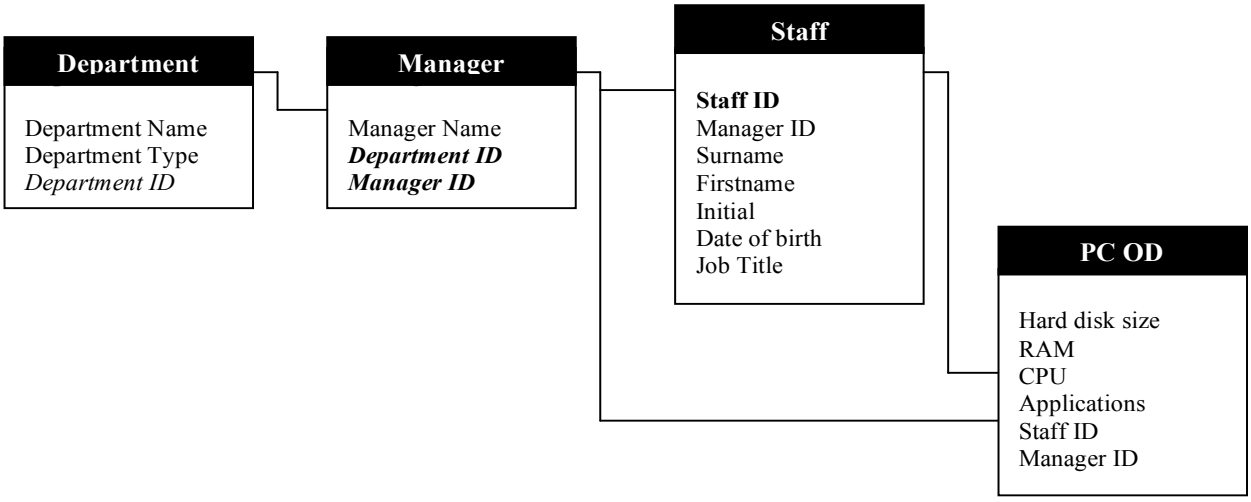


Relational Database Model

This model is independent from the physical implementation of the data structure. The relational database organisation has many advantages over the hierarchical and network database models. They are:

- Easier for users to understand and implement in a physical database system
- Easier to convert from other database structures
- Projection and joint operations (referencing groups of related data elements not stored together) are easier to implement and creation of new relations for applications is easier to do.
- Access control over sensitive data is easy to implement
- Faster in data search
- Easier to modify than hierarchical or network structures

Relational database technology separates data from the application and uses a simplified data model. Based on set theory and relational calculations, a relational database models information in a table structure with columns and rows. Columns, called domains or attributes, correspond to fields. Rows or tuples are equal to records in a conventional file structure. Relational databases use normalization rules to minimise the amount of information needed in tables to satisfy users' structured and unstructured queries to the database.



Relational keys not clear in the diagrams

Database administrator

Coordinates the activities of the database system. Duties include:

- Schema definition
- Storage structure and access method definition
- Schema and physical organisation modification
- Granting user authority to access the database
- Specifying integrity constraints
- Acting as liaison with users
- Monitoring performance and responding to changes in requirements
- Security definitions

Database Security, Integrity and Control

Security is the protection of data from accidental or deliberate threats, which might cause unauthorised modification, disclosure or destruction of data and the protection of the information

system from the degradation or non-availability of service. Data integrity in the context of security is when data are the same as in source documents and have not been accidentally or intentionally altered, destroyed or disclosed. Security in database systems is important because:

- Large volumes of data are concentrated into files that are physically very small
- The processing capabilities of a computer are extensive, and enormous quantities of data are processed without human intervention.
- Easy to lose data in a database from equipment malfunction, corrupt files, loss during copying of files and data files are susceptible to theft, floods etc.
- Unauthorised people can gain access to data files and read classified data on files
- Information on a computer file can be changed without leaving any physical trace of change
- Database systems are critical in competitive advantage to an organisation

Some of the controls that can be put in place include:

1) Administrative controls – controls by non-computer based measures. They include:
   a. Personnel controls e.g. selection of personnel and division of responsibilities
   b. Secure positioning of equipment
   c. Physical access controls
   d. Building controls
   e. Contingency plans
2) PC controls
   a. Keyboard lock
   b. Password
   c. Locking disks
   d. Training
   e. Virus scanning
   f. Policies and procedures on software copying
3) Database controls – a number of controls have been embedded into DBMS, these include:
   a. Authorisation – granting of privileges and ownership, authentication
   b. Provision of different views for different categories of users
   c. Backup and recovery procedures
   d. Checkpoints – the point of synchronisation between database and transaction log files. All buffers are force written to storage.
   e. Integrity checks e.g. relationships, lookup tables, validations
   f. Encryption – coding of data by special algorithm that renders them unreadable without decryption
   g. Journaling – maintaining log files of all changes made
   h. Database repair
4) Development controls – when a database is being developed, there should be controls over the design, development and testing e.g.
   a. Testing
   b. Formal technical review
   c. Control over changes
   d. Controls over file conversion
5) Document standards – standards are required for documentation such as:
   a. Requirement specification
   b. Programme specification
   c. Operations manual

d. User manual

6) Legal issues
   a. Escrow agreements – legal contracts concerning software
   b. Maintenance agreements
   c. Copyrights
   d. Licenses
   e. Privacy
7) Other controls include
   a. Hardware controls such as device interlocks which prevent input or output of data from being interrupted or terminated, once begun
   b. Data communication controls e.g. error detection and correction.
   Database recovery is the process of restoring the database to a correct state in the event of failure.

Some of the techniques include:

1) Backups
2) Mirroring – two complete copies of the database are maintained online on different stable storage devices.
3) Restart procedures – no transactions are accepted until the database has been repaired
4) Undo/redo – undoing and redoing a transaction after failure.

A distributed database system exists where logically related data is physically distributed between a number of separate processors linked by a communication network.

A multi-database system is a distributed system designed to integrate data and provide access to a collection of pre-existing local databases managed by heterogeneous database systems such as oracle.

CHAPTER SUMMARY

Advantages of computers:

- *Speed*
- *Accuracy*
- *Consistency*
- *Memory capability*
- *Processing capability*

Some of the areas that computers are used include:

- Communication
- Banking
- Organizational management
- Science, research and engineering
- Education
- Management of information materials
- Manufacturing and production
- Entertainment
- Retailing
- Home appliances

- Reservation systems
- Health care and medicine

Computers can be classified in different ways as shown below:

By processing - This is based on how the computer represents and processes the data.

a) Digital computers
b) Analog computers
c) Hybrid computers

By purpose - This is a classification based on the use to which the computer is put.

d) Special purpose
e) General-purpose

Classification by generation - This is a time-based classification coinciding with technological advances.

f) First generation.
g) Second generation.
h) Third generation.
i) Fourth generation.
j) Fifth generation.

Classification by power and size/ configuration

k) Supercomputers.
l) Mainframe computers.
m) Minicomputers.
n) Microcomputers.

CHAPTER QUIZ

1. A .....is an information-processing machine.
2. Computers are prone to errors.
   - True
   - False
3. Invention of the telephone enables both ..... and ..... communication in real time.
4. DBMS stands for?
5. Which one is odd one out among PC controls?
   a. Keyboard lock
   b. Password
   c. Locking disks
   d. Encryption
   e. Training

ANSWERS TO CHAPTER QUIZ

1. Computer
2. False
3. Wide Area Networks (WAN) and Local Area Networks (LAN)
4. Database Management Systems
5. d. Encryption - it's a Database control

EXAM QUESTIONS

1. Briefly list some important features which may be achieved by the use of a DBMS
2. Briefly discuss the problems which may be faced when using database systems.
3. The choice of file organisation should be based on the system type and purpose. Name FOUR types of file organisation giving an example of an application for which each type of file may be used.
4. Briefly explain four of some of the areas that computers are used.
5. Outline the classification by power and size/ configuration of computers.

CHAPTER TWO

SYSTEMS THEORY AND ORGANIZATIONS

CHAPTER TWO

SYSTEMS THEORY AND ORGANIZATIONS

▶ OBJECTIVES

When you have completed this chapter, you should be able to:

1. Define and classify information systems in organisations.
2. Describe features of systems theory
3. Describe Organisational theories
4. Describe organisational hierarchy

▶ INTRODUCTION

Information is a key resource within an organisation. Information resource provides a way of evidencing the nature and content of the transactions that allows organisations to monitor levels of resource availability and usage. It enables firms to identify revenues and costs and good record keeping.

▶ DEFINITION OF KEY TERMS

A **system** is a set of interacting components that work together to accomplish specific goals.

A **subsystem** is a unit within a system that shares some, or all, of the characteristics of that system.

Feedback - involves measuring the output of the system, comparing the output with a standard.

Entropy - This is the tendency towards disorder (chaos) in a system.

Synergy - It refers to cases where more than one system work together to produce more and better results than each would achieve independently.

Interfaces - Points where two systems meet and share inputs and outputs.

▶ EXAM CONTEXT

Most of the questions from this chapter are application questions in relation to organisations. The student will be required to have an open-minded approach when handling questions from this chapter. An in-depth knowledge of organisations operations will be an added advantage to a student attempting these questions. However, the theories outlined in this chapter form the basis to adequately answer the questions.

▶ INDUSTRY CONTEXT

The central concept to system dynamics is the need to understand how all parts of a system interact with one another. In this context, we can see organisations as systems, complex and chaotic ones. The various parts and people in an organisational system interact through "feedback" loops, where a change in one, over time, affects others, which in turn affects the original etc.

Fast Forward: Systems Thinking focuses on the interrelationship and dynamics among system components. Cause and effect are separated in time and space.

1. Systems concepts

A system is a set of interacting components that work together to accomplish specific goals. For example, a business is organised to accomplish a set of specific functions. Any situations, which involve the handling or manipulation of materials or resources of any kind whether human, financial or informative, may be structured and represented in the form of a system.

1.1 Characteristics of a System

a) **Purpose** – Systems exist to fulfil some objective or satisfy a need. A system may accomplish more than one task. The purpose of a system is closely tied to its rationale.
b) **Rationale** – This is the justification for a system's existence.
c) **Efficiency** – This is how well a system utilises its resources, that is, doing things right using the least amount of resources.
d) **Effectiveness** – How well a system fulfils its purpose, assuming that its purpose is the right one. Involves a system doing the right things.
e) **Inputs** – Entities that enter the system to produce output or furnish information.
f) **Outputs** – Entities that exit from the system either as interfaces or for end-user activities. They may be used to evaluate system's efficiency and effectiveness.
g) **Transformation rules** – They specify how the input is processed to produce output.
h) **Throughput** – Measures the quantity of work a system accomplishes. Does not consider the quality of the output.
i) **Boundary** – Artificially delimits a system for study or discussion purposes. System designers can only control those system components within the boundary.
j) **Environment** – That which impacts the system but is outside the system's boundary. The system cannot control events in the environment.
k) **Interfaces** – Points where two systems meet and share inputs and outputs. Interfaces belong to the environment although they may be inside the system boundary.
l) **Feedback** – Recycles outputs as subsequent inputs, or measures outputs to assess effectiveness.

1.2 Classification of systems

Each system can be characterised along a wide range of characteristics.

Physical systems Vs Abstract systems

A physical system consists of a set of elements, which are coordinated and operate as a whole entity to achieve a certain objective. This system may also be called a concrete system.

An abstract system is an orderly arrangement of conceptual items or components.

Simple systems Vs Complex systems

A simple system has few components, and the relationship or interaction between elements is uncomplicated and straightforward.

A complex system has many elements that are highly related and interconnected.

Open systems Vs Closed systems

An open system interacts with its environment. It is a system with a feedback mechanism that promotes the free exchange of information between the system and the external entities. Organisations are open systems.

A closed system has no interaction with the environment. This is a system that neither transmits information to the outside world nor receives any information from the outside world. It is mainly a scientific concept (e.g. physics experiments).

Open loop systems Vs closed loop systems

An open-loop system is one which does not act in a controlled manner, that is, there is no feedback loop, and so it has no measure of performance against standards.

A closed-loop system is one that functions in a controlled manner. Such a system accepts inputs, works upon them according to some predefined processing rules and produces outputs. Such a system is controlled via a feedback loop.

Stable/Static systems Vs Dynamic systems

A stable system undergoes very little change over time. A dynamic system undergoes rapid and constant change over time.

Adaptive systems Vs Non-adaptive systems

An adaptive system is able to change in response to changes in the environment. These systems can also be described as cybernetic or self-organising systems.

A non-adaptive system is not able to change in response to changes in the environment.

Deterministic systems Vs Probabilistic systems

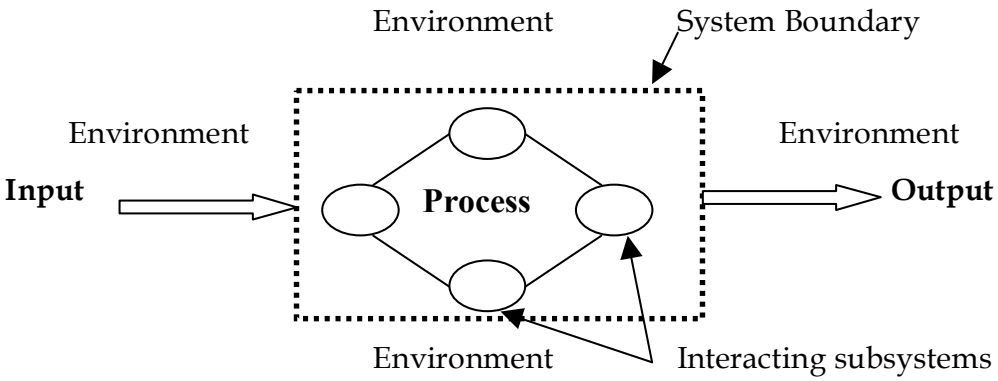
Deterministic systems operate in a predictable manner. For example, thermostats and computer programmes. In probabilistic systems, however, it is not possible to determine the next state of the system. These systems depend on probability distribution.

Permanent systems Vs Temporary systems

A permanent system exists for a relatively long period of time.

A temporary system exists for a relatively short period of time.

1.3 Components of systems



Inputs

These provide the system with what it needs to operate. It may include machines, manpower, raw materials, money or time.

Processes

Include policies, procedures, and operations that convert inputs into outputs.

Outputs

These are the results of processing and may include information in the right format, conveyed at the right time and place, to the right person.

Systems Boundary

A system boundary defines the system and distinguishes it from its environment.

Subsystems

A subsystem is a unit within a system that shares some or all of the characteristics of that system. Subsystems are smaller systems that make up a super-system / supra-system. All systems are part of larger systems

.

Environment

This is the world surrounding the system, which the system is a subsystem of.

Objectives and application of systems approach

Fast Forward: There are multiple levels of explanation for any complex situation. All may be true but their usefulness is different.

Features of systems theory

1. All systems are composed of inter-related parts or sub-systems and the system can only be explained as a whole. This is known as *holism* or *synergy*. The systems view is that the whole is more than just some of its parts and those vital interrelationships will be ignored and misunderstood if the separate parts are studied in isolation.
2. Systems are hierarchical, that is, the parts and sub-systems are made up of other smaller parts. For example, a payroll system is a subsystem of the Accounting System, which is a sub of the whole organisation. One system is a sub of another.
3. The parts of a system constitute an indissoluble whole so that no part can be altered without affecting other parts. Many organisational problems arise once this principle is flouted or ignored. Changes to one department could create untold adverse effects on others - ripple effects: e.g. changing a procedure in one department could affect others e.g. admissions - faculty ,type of data captured, process, etc.
4. The sub-systems should work towards the goals of their higher systems and should not pursue their own objectives independently. When subsystems pursue their own objectives, a condition of *sub-optimality* arises, and with this the falling of the organisation is close at hand!
   Information systems designers should seek to avoid the sub-optimality problem!
5. Organisational systems contain both hard and soft properties. Hard properties are those that can be assessed in some objective way e.g. the amount of PAYE tax with tax code, size of product-quantifiable

   Soft properties - constitute individual taste. They cannot be assessed by any objective standard or measuring process e.g. appearance of a product, suitability of a person for job and any problem containing a *political* element.

Importance of systems theory:

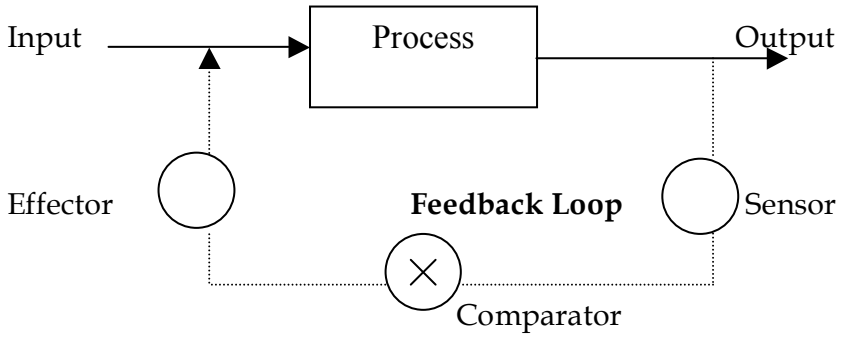
a) It provides a theoretical framework for study of performance of businesses
b) It stresses the fact that all organisations are made up of subsystems, which must work together harmoniously in order that goals of the overall system can be achieved.
c) It recognises the fact that conflicts can arise within a system, and that such conflicts can lead to sub-optimisation and that, ultimately, can even mean that an organisation does not achieve its goals.
d) It allows the individual to recognize that he/she is a subsystem within a larger system, and that the considerations of systems concept apply to him/her, also.
e) Given the above factors, it is clear that information-producing systems must be designed

to support the goals of the total system, and that this must be borne in mind throughout their development.

Systems theory concepts

- Entropy – This is the tendency towards disorder (chaos) in a system. The more closed a system is, the greater the entropy.

- Feedback – This is a control mechanism in open systems. Feedback involves measuring the output of the system, comparing the output with a standard and using any difference to modify subsequent input to ensure that the outputs conform to the required standards.



Elements of control include:

- Goal: This is the expected performance, plan or results.
- Sensor: Measures actual performance.
- Comparator: Compares expected results to actual results obtained.
- Effector: Reports deviation and initiates the response which may lead to a redirection of activity, revision of the expectation or changing the plan.

- Feed-forward – It means to take steps that make some adjustments to the system in advance in order to face any expected deviations in future. Feedback monitors the past results whereas feed-forward deals with future outcomes.
- Functional Decomposition – This involves factoring a system to its constituent subsystems. The subsystems are also decomposed further into manageable sizes resulting in a hierarchy structure of a system. Decomposition is used to analyse the existing system, to design and finally implement a new system.
- Functional cohesion – Involves dividing into subsystems by grouping activities that logically go together.
- Coupling – Occurs when two systems are highly interrelated.
- Decoupling – This is a process in which the subsystems are given autonomy and independence. The subsystems operate independently thereby pursuing own objectives and enhancing flexibility.
- Synergy – The whole is greater than the sum of its parts. At this point the focus is on global system needs, not local issues. It means that more than one system working together produce more and better results than each would achieve independently.
- Optimisation – It is possible to achieve the best solution.

- Sub-optimisation – It is an occurrence that occurs when the objectives of one element or subsystem conflicts with the objectives of the whole system.
- Equifinality – Certain results may be achieved with different initial conditions and in different ways. In open systems, the same final state can be reached from several starting points, one result can have different causes, or through different methods, there is more than one way to achieve the objective.
- Goal-seeking – systems attempt to stabilise at a certain point.
- Holism – the analysis of a system is considered from the point of view of the whole system and not on individual subsystems. Subsystems are studied in the context of the entire system.

3. Organisations

An organization is a group created and maintained to achieve specific objectives.

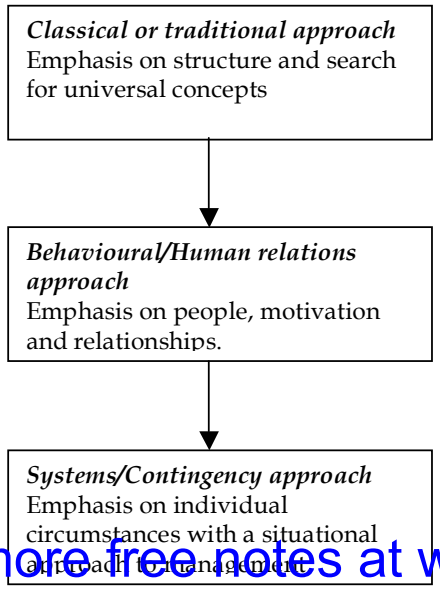
- A hospital with objectives dealing with human care.
- A local authority with objectives of providing services to the local community.
- A commercial company with objectives including earning profits, providing a return for shareholders and so on.

Features that describe organisations would be accepted by most people.

- Goal oriented i.e. people with a purpose.
- Social systems i.e. people working in groups.
- Technical systems i.e. people using knowledge, techniques and machines.
- The integration of structured activities i.e. people co-coordinating their efforts.

3.1 Organisational theories

Organizational theory is the body of knowledge relating to the philosophical basis of the structure, functioning and performance of organisations. Such theory is derived from historical schools of thought stating the point of view of a number of early pioneers of management. A broad chronological sequence of the three main schools of thought, which have contributed to an understanding of the nature of organisations and management is shown in the figure below:



Classical or Empirical Approach

Also known as the traditional approach. The classical or management process approach to management was evolved in the early part of the 20th century. This theory is based on contributions from a number of sources including:

- Scientific management (from Taylor, Gant, Gilbert and others)
- Administrative Management Theorists (Fayol, Urwick, Brech and others)
- Bureaucracy/Academics (notably from Weber)

Whilst not completely ignoring the behavioural aspects of organisation, the traditional emphasis was on the structure of organisations, the management of structures and control of production methods. All organisations were treated similarly and there was a search for universal principles, which could be applied to any organisation and on the whole took a relatively mechanistic view of organisations with a tendency to treat them as closed systems.

(i) Scientific management or Taylorism

In the late 1890's, Fredrick Taylor introduced the concept of scientific management. Taylor's approach focused on the effective use of human beings in organizations; it is a rational engineering approach of work based on time and motion studies. His pioneering work was refined and developed by others. There are four main principles to scientific management:

a) Develop the best or ideal method of doing a task and determine a standard scientifically. The worker should be paid an incentive for exceeding this standard.
b) Select the best person for the job and train him or her in the way to accomplish the task.
c) Combine the scientific method with well selected and trained people (workers will not resist improved method, since they receive more money because of them).
d) Take all responsibility for planning and give it to the management. The worker is only responsible for the actual job performance. Scientific management and intensive study of the activities of individual employees answered many questions on human engineering.

Benefits and drawbacks of scientific management

Benefits

a) The improvement in working methods resulted in enormous gains in productivity.
b) The measurement and analysis of tasks provided factual information on which to base improvements in methods and equipment.
c) It provided a rational basis for piecework and incentive schemes, which became more widely used.
d) There were considerable improvements in working conditions.
e) Management became more involved with production activities and was thus encouraged to show positive leadership.

Drawbacks

a) Jobs became more boring and repetitive.

b) Planning, design and control became divorced from performance thus de-skilling tasks.
c) Workers became more virtual adjuncts to machines with management having a monopoly of knowledge and control.
d) De-skilling, excessive specialisation, repetition and so on, causes workers to become alienated and frustrated.

(i) Departmental Approach

A number of theorists, including Gulick, Urwick and Fayol have described organisations based on groupings of various activities into departments. These theorists looked at the organisation as divided into departments. These theorists looked at the organisation as a giant machine and tried to develop principles or universal laws that govern the machine's activities. The general problem addressed in their writing is that given an organisation, how do you identify the unit tasks and how do you organise these tasks into the individual jobs? Then how are the jobs organised into administrative units, and finally how are top-level departments established? The result of this analysis is the structuring of departments within the organisation, each department contains a set of tasks to be performed by workers in that department.

Example:

- Finance department: For providing funds and ensuring effective use.
- Production department: Provides and maintains equipment to convert raw materials into finished products and ensure control of the production process.
- Marketing department
- Supply department
- Research and development department

(ii) Weber's Bureaucratic Organisation

Unlike other contributors to the classical view of organisations, Weber was not a practicing manager, but an academic sociologist. He is the one who first coined the term bureaucracy to describe a particular organisational form, which exists to some extent in every large enterprise whether in public or private sector.

In Weber's view the bureaucratic organisation was a logical rational organisation which was technically superior to all other forms. The key elements in the ideal bureaucratic organisation were as follows:

- A well defined hierarchy of legitimate authority.
- A division of labour based on functional specialisation.
- A clear statement of the rights and duties of personnel.
- Rules and procedures in writing should exist to deal with all decisions to be made and situations to be handled.
- Promotion and selection based on technical competence.

In Weber's view a de-personalised form of organisation would minimise the effect of human unpredictability. Weber concentrated on the structural aspects of organisations and in consequence took a rather mechanistic impersonal standpoint.

Weaknesses of the bureaucratic model

- Adaptability and change are made more difficult because of standardised rules, procedures and types of decisions.
- Rules tend to become important in their own right rather than as a means of promoting efficiency.

The contribution of the classical theorists can be summarised as follows:

- They introduced the idea that management was a suitable subject for intellectual analysis.
- They provided a foundation of ideas on which subsequent theorists have built.
- Criticism of their work has stimulated empirical studies of actual organisational behaviour.

Human Relation School

The human relations school of organisations studied human individuals in the organisation from a psychological point of view. The approach was based on a series of experiments conducted in the 1920's at the Hawthorne Western electric plant by Mayo. The experiment revealed that an organisation was more than a formal structure or arrangement of functions. The results of his research focused attention on the behavioural approach to management and he concluded that an organisation is a social system, a system of cliques, grapevines, informal status systems, rituals and a mixture of logical and non-logical behaviour.

Concepts of the human relations approach

Some of the concepts which Mayo and other workers in the human relations field developed after studying the role of individuals, informal groups, inter-group relationships and the formal relationship with the organisation are as follows:

a) People are not motivated by financial factors but by a variety of social and psychological factors.
b) Informal work groups have important roles in determining the attitudes and performance of individuals.
c) Management requires social skills as well as technical ones.
d) An organisation is a social system as well as technical/economic system.
e) Traditional authoritarian leadership patterns should be modified substantially to consider psychological and social factors and should become more 'democratic' in nature.
f) Participation in work organisation, planning and policy formulation is an important element in organisations. This meant establishing effective communications between the various levels in the hierarchy to ensure a free flow of information. The following are some of the individuals who carried on motivation research together with their theories:

(i) Abraham Maslow

Maslow developed the theory that people are motivated by a desire to satisfy their specific needs and that they tend to satisfy their needs progressively, starting with the basic psychological needs and moving up the hierarchy. He suggested five levels of human needs as follows:

Level 1 – Physiological needs e.g. self-satisfaction of sleep, hunger, thirst, etc.
Level 2 – Security needs: protection against threats and danger.

Level 3 – Affiliation needs: needs for love and acceptance by others.
Level 4: Esteem needs: needs for respect, status and recognition.
Level 5: Self-actualisation needs: needs for self-fulfilment and self-development.

Thus according to Maslow's hierarchy of needs, once a need from lower levels upwards is satisfied it ceases to be a motivator.

(ii) Douglas McGregor

Maslow and the need hierarchy influenced McGregor when he developed his theory of management. He described theory X as the approach that governs most current thinking about work. The following is a summary of assumptions in theory X:

a) Average man is inherently lazy.
b) He lacks ambition, dislikes responsibility and must be led.
c) He is resistant to change and is indifferent to organisational needs.
d) Coercion and close control is required.

If theory X is adopted, management must direct, persuade and control activities of people and management must seek to coerce and modify people's behaviour to fit the needs of the organisation. Later, McGregor rejected the assumptions of theory X and proposed an alternative called theory Y. Some elements of theory Y are as follows:

a) To the average man, work is as natural as rest or play.
b) Motivation, potential for development, imagination and ingenuity are present in all people given proper conditions.
c) Coercion and close control are not required.
d) Given proper conditions people will seek out responsibility.

The implication of this theory in management if adopted is that, management tries to harness qualities of people by arranging conditions and methods of operations so that people can achieve their own goals best by directing their efforts towards organisational objectives. Cooperation rather than coercion is required.

(iii) Schein

Schein has combined a number of the different models and assumptions about individuals in organisations into a model he calls 'complex man'. His model suggests that the individual is both complex and highly variable, and has many motives that may change over time. A person can learn new motives and will become productively involved in an organisation for a number of different reasons, responding in different ways to different managerial strategies. The result of this view is that mangers need to adopt and vary their behaviour in accordance with the motivational needs of particular individuals and groups and the task in hand.

(iv) Fredrick Herzberg

From his research Herzberg concluded that certain factors are helpful to job satisfaction, which he termed motivators, while certain factors which he called hygiene factors could lead to dissatisfaction. The following is a summary of the major factors found in the two groups:

Hygiene factors	Motivators
Policies and administration Supervision Working conditions Money Job security Relationship with peers and subordinates	Achievement Recognition Responsibility Growth Development and growth

Note that the motivators are related to the content of the job whilst the hygiene factors are more related to the environment of the work and not intrinsic to the job itself. The two sets of factors are not opposite. Hygiene factors do not induce job satisfaction by themselves. To promote positive satisfaction motivators are needed. For example, in production, hygiene factors maintain production while motivators increase output.

(v) Rensis Likert

From his research, Likert found that successful managers built their successes on tightly knit groups of staff whose cooperation had been obtained by close attention to a range of lower and higher order motivational factors. Participation was arranged and supportive relationship within and between groups was fostered.

System Contingency Approach

These theories developed from two main sources:

- The classic school with its somewhat mechanistic emphasis on structures, which could be imposed on people.
- Human relations school whose laudable concentration on the needs of the individual to an extent obscured study of the organisation as a whole.

Modern theorists attempted to develop from these earlier ideas a more comprehensive view of organisation. One major approach they developed is a system approach, which sees the organization as a total system of interconnected and interactive subsystems. The organisation was found to respond to numerous independent variables of which the following are important:

- People
- Tasks
- Organisational structure
- Environment

In contrast with earlier approaches which considered variable in isolation, system theorists study the relationship between several of them. System theorists have suggested that there is no one best way of designing organizations, and because of volatility and change the best way is dependent (or contingent) upon prevailing conditions. Thus the development of the contingency approach.

Contingency Theory

This is the most current school and it sees each organisation as a unique system resulting from an interaction of subsystems with the environment. The motto of contingency theory is 'it all depends'. Both system and contingency approaches recognise organisations as a complex structure with many interacting elements, which must continually adapt to uncertain and changing environment. Some of the major contributors to this approach are:

1. Lawrence and Lorsch

The two studied the operations of a number of firms to assess the effects on the tasks and attitudes of managers in various functions operating with different structures and environment. Some of the major contributors to this approach are:

a) The more volatile and diverse the environment, the more task differentiation, and consequent integration, is required to achieve a successful organization.
b) More stable environment does not require much differentiation but still requires substantial integration within the functions that exist.
c) It is more difficult to resolve conflict in organisations with a high degree of differentiation between the functions that exist.
d) Better methods of conflict resolution result in higher performance and lead to types of differentiation and integration that suit the organisations environment.
e) In a predictable environment, integration is achieved through the management hierarchy, particular at higher levels and through rules, procedures, budgets etc. In an uncertain environment, integration is achieved at lower levels mainly through personal interrelationship with only a moderate use of administrative methods.

In spite of some criticism, the Lawrence and Lorsch study received, it played an important role in development of organisations theory, which took account of change, uncertainty and the interaction of key variables.

2. Burns and Stalker

These two carried out a study in a number of electronic firms to see how they adapted to changes in their environment, particularly with regard to changes in the market and technical conditions. The result of their study was a classification of organisation into mechanistic and organic systems.

Properties of mechanistic systems

a) Stable environment with high certainty and predictability.
b) High functional specialisation.
c) Detailed differentiation of duties and responsibilities.
d) Hierarchical control, authority and communications with largely vertical interactions.
e) Authorisation style with clear superior subordinate relationships and emphasis on loyalty and obedience.
f) Low rate of innovation.

Properties of organic systems

a) Uncertain environment, low predictability.

b) Low functional specialisation.
c) Less structured management with more adjustment and re-definition roles.
d) More consultation with information and advice being communicated rather than decisions and instructions.
e) High rate of innovation.

Examples of mechanistic organisation system

Traditional industries such as steel, textiles and ship building where management controls and methods are based on well-defined rules and procedures which experience little change.

Examples of organic systems

Industries facing rapidly changing environment such as computers and pharmaceuticals.

3. Joan Woodward

She carried out a study of manufacturing firms where she observed that many organisational characteristics were already related to the technology used. She categorised organisation on the basis of technology as follows:

a) Small batch or individual item production.
b) Large batch or mass production including assembly line production.
c) Continuous process production including refinery, chemical and gas production.

Based on this categorizsation, Woodward found that there were clear patterns relating to things like the span of control, chain of command and system of management. A summary of the various features are illustrated in the figure below.

Categories of technology

Types of management systems

	Small batch/ individual items	Large batch/mass production	Continuous production
Number of levels in chain command	Few	Medium	Numerous
Span of control – Top Management	Small	Medium	Large
Span of control – middle management	Large	Medium	Small
Ratio of management /operatives	Low	Medium	High
Typesof management system	Mainly organic system with fewer rules and close personal interrelationship	Mainly mechanistic with clear-cut procedures and more rules and impersonal relationships.	Mainly organic with fewer rules and close personal relationships.
Communication	Mainly verbal with little paperwork.	Mainly written with considerable paperwork.	Mainly verbal with little paperwork.

Woodward concluded that the method of production was an important factor affecting organization structure and that there was a particular type of structure and management style suitable for each of the types of production.

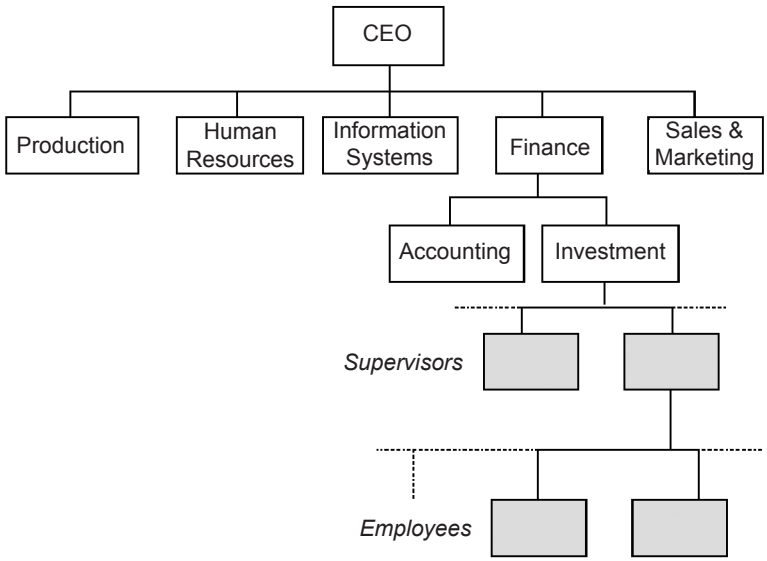
4. Aston University group led by Gareth

The group continued on the work of Woodward and found that size was an important factor in determining structure as well as the technology used. As firms grow, they become more formally structured and the study found that a large size tends to lead to:

a) More standardisation
b) More of structures, procedures and decision rules.
c) More specialisation of tasks and functions.
d) Less centralisation, that is, concentration of authority.

3.2 Organizational structures

- Traditional management organisation is essentially *hierarchical*



- Characterised by
  - strong *line management* structure, emphasised through reporting and responsibility
  - 'top' management is responsible to board of directors and shareholders
  - departmental structure is usually based on functions (sales, production, finance etc.)
  - management of information systems is usually the responsibility of a specific IS department
  - there is limited scope for cross-departmental operations
- Managers at each level in the organisation are responsible for
  a) planning development
  b) organising resources
  c) staffing

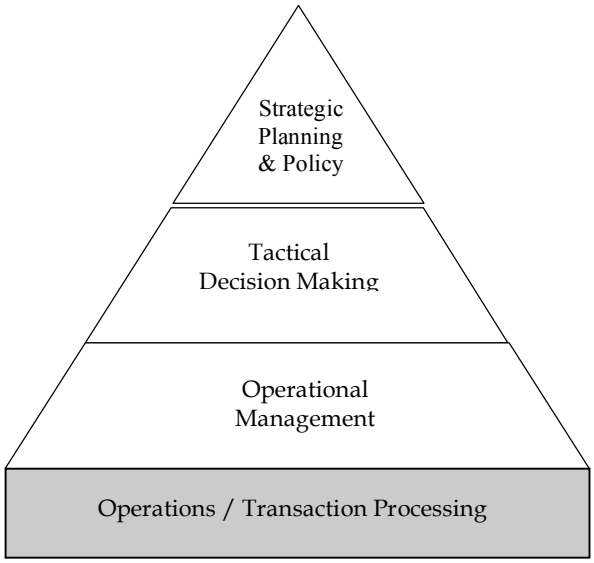
STUDY TEXT

d) directing employees
e) controlling operations

- Managers at different levels in the hierarchy place different emphasis on these functions:
  - top-level managers deal mainly with *strategic* decision-making (long-term planning)
  - 'middle-level' managers focus on *tactical* decisions, which are primarily to do with organising and staffing
  - 'low-level' managers deals with the day-to-day running of the organisation, and are mostly involved in *directing* and *controlling*

- the major impact of computers on organisations that have this structure has been to 'flatten' this hierarchy, largely by reducing the role of middle (and to some extent low) management
- the traditional system provides *processed* information on the functioning of the organisation to the higher levels
- with centralised computer systems, data collected by the various departments was fed to the IS department, where it was processed ready for analysis by management
- extensive use of distributed computing allows the processed information to be supplied directly to higher levels of management
- this is almost always based on the use of some form of *information system*; these are generally termed *management information systems* (MIS)

3.3 Organisational hierarchy



Fast Forward: Managers are organizational members who are responsible for the work performance of other organizational members.

In an organisation, information flows vertically (up and down) among management levels and horizontally (across) among departmental levels. There are five basic functions found in an organisation:

a) Accounting: Keeps track of all financial activities.
b) Manufacturing/Production: Makes the company's product.
c) Marketing: Advertises, promotes and sells the product.
d) Human resources: Finds and hires people and handles personnel matters.
e) Research: Does product research and relates new discoveries.

There are three management levels in most organisations:

i. Supervisors

Supervisors manage and monitor the employees or workers. They are responsible for the day-to-day operational matters. An example of a supervisor's responsibility would be to monitor workers and materials needed to build the product.

Supervisors get information from middle managers above them and workers below them (primarily vertical). They need internal information for operational planning. They need detailed, current day-to-day information.

ii. Middle Management

Middle managers deal with control planning, tactical planning and decision-making. They implement long-term goals of the organisation. An example of a middle manager's responsibility would be to set sales goals for several regions.

Middle-level managers get information from among all departments (horizontally) and from all levels of management (vertically). They need historical internal information for tactical planning. They need summarised information such as weekly or monthly reports. An example of a middle-level manager information need would be to develop production goals with concurrent information from top-level managers and supervisors.

iii. Top Management

Top managers are concerned with long-range strategic planning. They need information to help them plan future growth and direction of the organisation. An example of a top manager's responsibility would be to determine the demand for current products and the sales strategies for new products.

Top-level managers get information from outside the organisation and from all departments (horizontally and vertically). They need future-oriented internal and external information for strategic planning. They need information that reveals the overall condition of the business in a summarised form. An example of a top-level manager information need would be to plan for new facilities.

SUMMARY

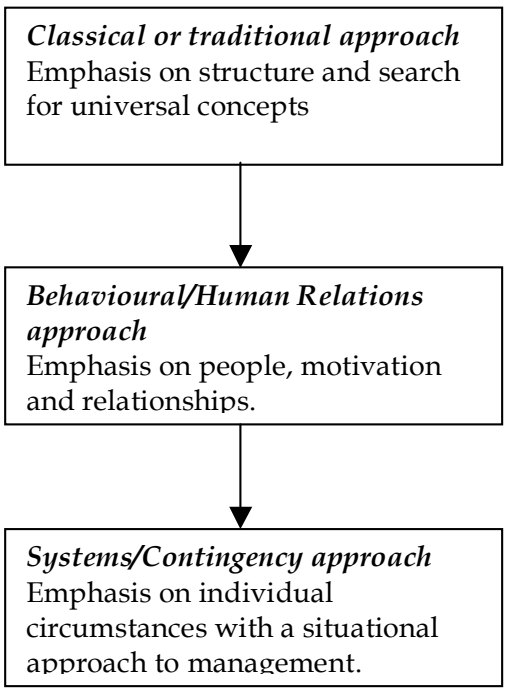
Components of systems

- Inputs
- Processes
- Outputs
- Systems Boundary
- Subsystems
- Environment

Elements of control include:

- Goal: This is the expected performance, plan or results.
- Sensor: Measures actual performance.
- Comparator: Compares expected results to actual results obtained.
- Effector: Reports deviation and initiates the response which may lead to a redirection of activity, revision of the expectation or changing the plan.

Organisational theories



PAST PAPER ANALYSIS

12/00, 6/01, 12/01, 12/02, 6/03, 12/04, 6/05, 6/07

CHAPTER QUIZ

1. Which one is not a characteristic of a system?

   a. Purpose
   b. Rationale
   c. Synergy
   d. Effectiveness

2. ..... provide the system with what it needs to operate

3. Coupling occurs when two systems are highly interrelated.

   a. True
   b. False

4. An ..... is a group created and maintained to achieve specific objectives

5. Which one is not an organisation approach?

   a. Classical
   b. Behavioural
   c. Abraham Maslow
   d. Systems

ANSWERS TO CHAPTER QUIZ

1. c. Synergy
2. Inputs
3. a. True
4. organisation
5. c. Abraham Maslow

EXAM QUESTIONS

1. At a macro level, the organisation itself may be viewed as a system comprising a number of levels of subsystems. List and briefly describe the five levels of the system hierarchy which may be found in a large commercial organisation.
2. The reliability of the interface between systems depends upon the effectiveness and robustness of the communications. List and briefly discuss four factors, which largely determine the quality of integration and interaction between systems.
3. A model of an information system can be produced by applying the elements from the general systems approach. Briefly list the components of an information system and apply to them the contribution of the general systems approach.
4. A system is a set of interacting components that work together to accomplish specific goals. Outline the importance of systems theory.
5. Describe the contribution of Lawrence and Lorsch to the Contigency Theory on organisations.

CHAPTER THREE

INTRODUCTION TO SYSTEMS DEVELOPMENT

CHAPTER THREE

INTRODUCTION TO SYSTEMS DEVELOPMENT

▶ OBJECTIVES

When you have completed this chapter, you should be able to:

1. Manage a project from its inception to completion via all the requisite stages.
2. Describe system development life cycle.
3. Identify the critical path of a project and realise the significance of the critical path.
4. Draw and interpret flow charts.
5. Describe the alternative development methodologies.

▶ INTRODUCTION

System analysis and design is a series of processes for analysing and designing computer-based information systems. Systems design allows a development team to roughly see what and how their system will look like. An important result of systems analysis and design is an application software, that is, software designed to support a specific organizational function or process.

▶ DEFINITION OF KEY TERMS

Critical path is the longest-duration path through the network.

Activity is a task that must be performed.

Event is a milestone marking the completion of one or more activities.

Programme Evaluation and Review Technique (PERT) is a network model that allows for randomness in activity completion times.

Structured walkthrough - It is a planned review of system by people not involved in its development effort.

▶ EXAM CONTEXT

Most of the questions from this chapter are direct. This, therefore, means that the student will be required to understand all concepts in this chapter fully. Emphasis is usually laid on feasibility study and project development.

▶ INDUSTRY CONTEXT

Practitioners of systems analysis are often called up to dissect systems that have grown haphazardly to determine the current components of the system. This was shown during the year 2000 re-engineering effort as business and manufacturing processes were examined and simplified as part of the Y2K automation upgrades. Current employment titles utilising systems analysis include, but are not limited to, Systems Analyst, Business Analyst, Manufacturing Engineer, Enterprise Architect, etc.

While practitioners of systems analysis can be called upon to create entirely new systems their skills are more often used to modify, expand or document existing systems (processes, procedures and methods).

Fast Forward: System Analysis, Design and Integration addresses the activities, methodsand tools required to transform an operational need into a description of system performance parameters and a preferred system configuration

1. Object-Oriented Programming (OOP)

This is a revolutionary concept that changed the rules in computer programme developmentOOP is organized around "objects" rather than "actions," data rather than logic. Historically, a programme has been viewed as a logical procedure that takes input data, processes it, and produces output data. The programming challenge was seen as how to write the logic, not how to define the data. OOP takes the view that what we really care about are the objects we want to manipulate rather than the logic required to manipulate them. Examples of objects range from human beings (described by name, address, and so forth) to buildings and floors (whose properties can be described and managed) down to the little widgets on your computer desktop (such as buttons and scroll bars).

The first step in OOP is to identify all the objects you want to manipulate and how they relate to each other, an exercise often known as data modelling. Once you've identified an object, you generalise it as a class of objects and define the kind of data it contains and any logic sequences that can manipulate it. Each distinct logic sequence is known as a method. A real instance of a class is called an "object" or, in some environments, an "instance of a class." The object or class instance is what you run in the computer. Its methods provide computer instructions and the class object characteristics provide relevant data. You communicate with objects - and they communicate with each other - with well-defined interfaces called messages. .

C++ and Java are the most popular object-oriented languages today. The Java programming language is designed especially for use in distributed applications on corporate networks and the Internet.

Companies often commit significant resources to development, acquisition and continued maintenance of application systems. These systems often control an organisation's assets and may in themselves be considered an asset that needs to be protected and controlled.

One or more of the following situations will initiate an individual application or project:

a) A new opportunity that relates to a new or existing business process.
b) A problem that relates to an actual business process.
c) A new opportunity that will enable the organisation to take advantage of technology.
d) A problem with the current technology.
e) Organisational growth
f) Merger or acquisition
g) Revisions in government regulations

System development projects should be initiated using well-defined procedures to communicate business needs to management. These procedures often require detailed documentation identifying the need or problem, specifying the desired solution and relating the potential benefits to the organisation.

Aids in system analysis and design include:

§ Methodologies – Comprehensive, multi-step approaches to systems development that guide the work and influence the quality of the final product.
§ Techniques – Particular processes that an analyst will follow to ensure that the work is well thought-out, complete and comprehensible to others on the project team.

§ Tools – Computer programmes that make it easy to use and benefit from the techniques and to faithfully follow the guidelines of the overall development methodology.

To create new systems or to modify existing ones, information systems professionals follow several steps:

a) Investigation – the process of understanding a problem or opportunity.
b) Analysis – the process of defining what the system should accomplish.
c) Design – the process of determining how the system will accomplish its purpose.
d) Implementation – involves creating the system and putting it into use.
e) Maintenance – involves monitoring and changing an information system throughout its life.

System analysts use the system analysis and design process to develop new systems. They study the organisation's present systems and suggest actions to be taken after doing preliminary investigations.

2. Project Management

A project can be defined as a temporary sequence of unique, complex and connected activities having one goal or purpose and that must be completed by specific time, within budget and according to specification. It is a planned undertaking that has a beginning and an end and that produces a predetermined result or product. Every project is constrained by its scope, time goals and cost goals.

Projects have the following characteristics:

a) Unique purpose – a project is undertaken to fulfil a specific objective
b) Temporary – projects exist for a limited duration of time; often not perpetual
c) Require resources – such as money, manpower and machine resources
d) Should have a primary sponsor – usually an organisation, a department or individual
e) Involves uncertainty – a great deal of the project implementation is unknown the need for planning and management.

The key competencies that project managers must develop are known as knowledge areas and include:

- Scope management
- Time management
- Cost management
- Quality management
- Human resources management
- Communications management
- Risk management
- Procurement management and
- Integration management

The project stakeholders are the people involved in or are affected by project activities (including project sponsor, project team, support staff, customers, users, suppliers and even opponents to the project).

A project life cycle is a collection of project phases, which includes:

1. Concept
2. Development
3. Implementation
4. Close-out

The first two phases relate to project feasibility awhile the last two phases focus on delivering the work and are often called project acquisition.

It is important not to confuse project life cycle with product life cycle. The project life cycle applies to all projects regardless of the products being produced. On the other hand product life cycle models vary considerably based on the nature of the product. For information systems a systems development life cycle (SDLC) is used. SDLC is a framework for describing the phases involved in developing and maintaining information systems.

2.1 Measures of project success

A project is successful when:

- The resulting information system is acceptable to the customer.
- May need to specifically mention the importance of functionality of the delivered system
- The system is delivered on time
- The system is delivered within budget

The system development process has a minimal impact on ongoing business operations.

2.2 Causes of project failures

- Failure to establish top-management commitment to the project
- Lack of organisation's commitment to the system development methodology
- Taking shortcuts through or around the system development methodology
- Poor expectations management
- Premature commitment to a fixed budget and schedule
- Poor estimating techniques
- Over-optimism
- Inadequate people management skills
- Failure to adapt to business changes
- Insufficient resources
- Failure to manage the plan

2.3 Systems Planning

Involves:

(i) Project identification and selection i.e. high level planning
(ii) Project initiation and planning i.e. low level planning

Project identification and selection

(i) Identify potential development projects

Sources of projects include:

- Management and business units
- Managers who want to make a system more efficient or less costly
- Formal planning groups

Projects are identified by:

- Steering committees
- Top management
- User departments
- Development group or senior information systems staff

Top-down identification focuses on global needs of the organisation and is usually done by top management or steering committees. Bottom-up identification is usually done by business unit or information system group and doesn't reflect overall goals of the organisation.

(ii) Classify and rank projects

This process is performed by top management, steering committee, business units or information systems development group. Value chain analysis is often used. This is a method to analyse an organisation's activities to determine where value is added and costs are incurred.

(iii) Select projects

This is the process of considering short and long-term projects. Projects most likely to achieve business objectives are selected. Decision requires consideration of:

- Perceived and real needs
- Potential and ongoing projects
- Current organisational environment
- Existing and available resources
- Evaluation criteria
- Outcomes

Project Initiation and Planning

Project planning and initiation involves:

- Team organisation
- Establishing management procedures
- Identifying scope – Scope defines the boundaries of a project – what part of the business is to be studied, analysed, designed, constructed, implemented and ultimately improved?
- Identifying alternatives
- Feasibility/risk analysis and strategic assessment
  Feasibility is the measure of how beneficial or practical the development of an information system will be to an organisation. Feasibility analysis is the process by which feasibility is measured.

Risk analysis helps understand and manage uncertainty. There is need to assess probability, assess impact and establish contingency plan.

- Estimation – Estimation of resources, such as human effort, time and cost. Estimation is extremely difficult and (usually) inaccurate.
- Cost/benefit analysis
  - Costs
    - Development costs are one-time costs that will not recur after the project has been completed e.g. systems development, hardware/software, user training, site preparation and data conversion.
    - Operating costs are costs that tend to recur throughout the lifetime of the system. e.g. expenses on maintenance, data storage, communicationsand software licenses. Such costs can be classified as:
      - Fixed costs – occur at regular intervals but at relatively fixed rates
      - Variable costs – occur in proportion to some usage factor
  - Benefits
    - Tangible benefits are those that can easily be quantified e.g. cost reduction, error reduction and increased sales
    - Intangible benefits are those benefits that are difficult or impossible to quantify e.g. improved planning and control, improved employee morale and improved decision making
  - Constraints
    - Schedule e.g. project must be completed before a certain set date
    - Costs e.g. the system cannot cost more than 1m
    - Technology e.g. the system must be online, use MS Access database and run on a Windows platform
    - Policy e.g. the system must use double-entry accounting
- Scheduling – Usually use of Gantt charts and PERT/CPM methods (Performance Evaluation and Review Technique/ Critical Path Method). The tools are not mutually exclusive (especially when PERT is based on “activity on node” conventions). That is why most project management software tools maintain both views simultaneously.

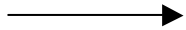
PERT (Program Evaluation and Review Technique) and CPM (Critical Path Method)

Fast Forward: PERT chart can be much more difficult to interpret, especially on complex projects.

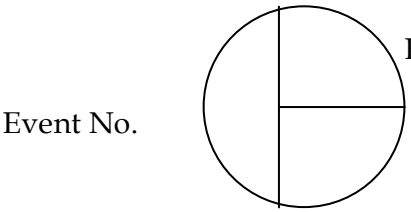
A PERT chart is a graphical network model that depicts a project’s tasks and the relationships between those tasks. It was developed in the late 1950’s to plan and control large weapons development projects for the US Navy. It is a project management tool used to schedule, organise, and coordinate tasks within a project. PERT depicts task, duration, and dependency information.

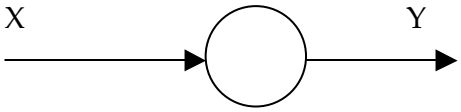
Critical Path Method (CPM), which was developed for project management in the private sector at about the same time, has become synonymous with PERT, so that the technique is known by any variation on the names: PERT, CPM, or CPM/PERT.

Diagram Symbols

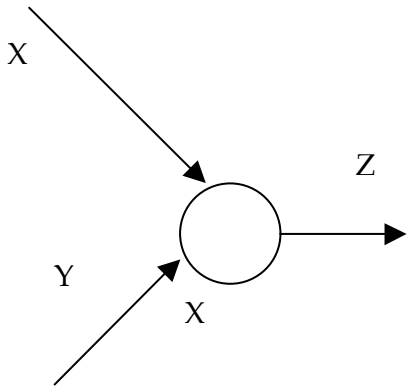


Activity (task to be carried out in the project)

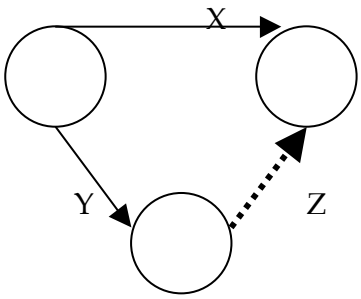




Task X must be completed before task Y can start



Tasks X and Y must be completed before Z can start



Z is a dummy activity; it is represented by a dotted line, it is required to avoid activities having the same head and tail events.

CPM

CPM provides the following benefits:

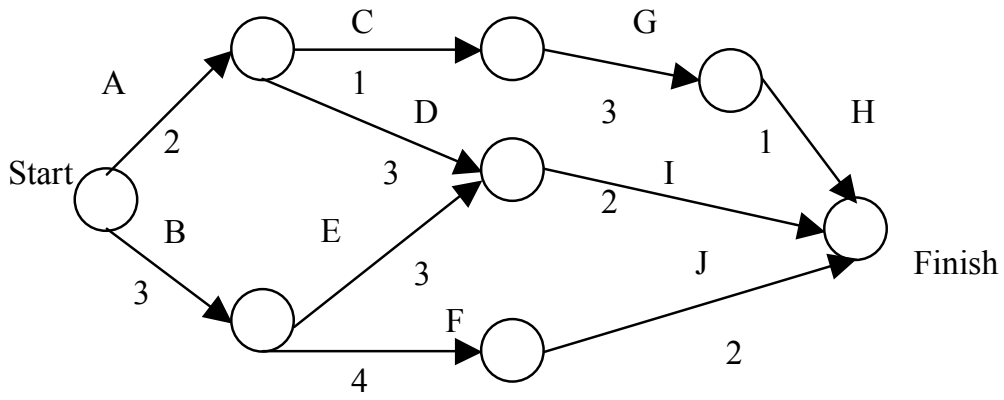
- Provides a graphical view of the project.
- Predicts the time required to complete the project.
- Shows which activities are critical to maintaining the schedule and which are not.

CPM models the activities and events of a project as a network. Activities are depicted as nodes on the network and events that signify the beginning or ending of activities are depicted as arcs or lines between the nodes. The following is an example of a CPM network diagram:

Activity Listing

Activity	Precedence	Duration (Weeks)
A	-	2
B	-	3
C	A	1
D	A	3
E	B	3
F	B	4
G	C	3
H	G	1
I	D, E	2
J	F	2

Network Diagram



Steps in CPM Project Planning

1. Specify the individual activities.
2. Determine the sequence of those activities.
3. Draw a network diagram.
4. Estimate the completion time for each activity.
5. Identify the critical path (longest path through the network)
6. Update the CPM diagram as the project progresses.

>> 1. Specify the Individual Activities

From a work breakdown structure, a listing can be made of all the activities in the project. This listing can be used as the basis for adding sequence and duration information in later steps.

>> 2. Determine the Sequence of the Activities

Some activities are dependent on the completion of others. A listing of the immediate predecessors

of each activity is useful for constructing the CPM network diagram.

>> 3. Draw the Network Diagram

Once the activities and their sequencing have been defined, the CPM diagram can be drawn. CPM was originally developed as an *activity on node* (AON) network, but some project planners prefer to specify the activities on the arcs.

>> 4. Estimate Activity Completion Time

The time required to complete each activity can be estimated using past experience or the estimates of knowledgeable persons. CPM is a deterministic model that does not take into account variation in the completion time; so only one number is used for an activity's time estimate.

>> 5. Identify the Critical Path

The critical path is the longest-duration path through the network. The significance of the critical path is that the activities that lie on it cannot be delayed without delaying the project. Because of its impact on the entire project, critical path analysis is an important aspect of project planning.

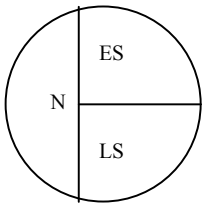
The critical path can be identified by determining the following four parameters for each activity:

- EST - earliest start time: the earliest time at which the activity can start given that its precedent activities must be completed first.
- EFT - earliest finish time, equal to the earliest start time for the activity plus the time required to complete the activity.
- LFT - latest finish time: the latest time at which the activity can be completed without delaying the project.
- LST - latest start time, equal to the latest finish time minus the time required to complete the activity.

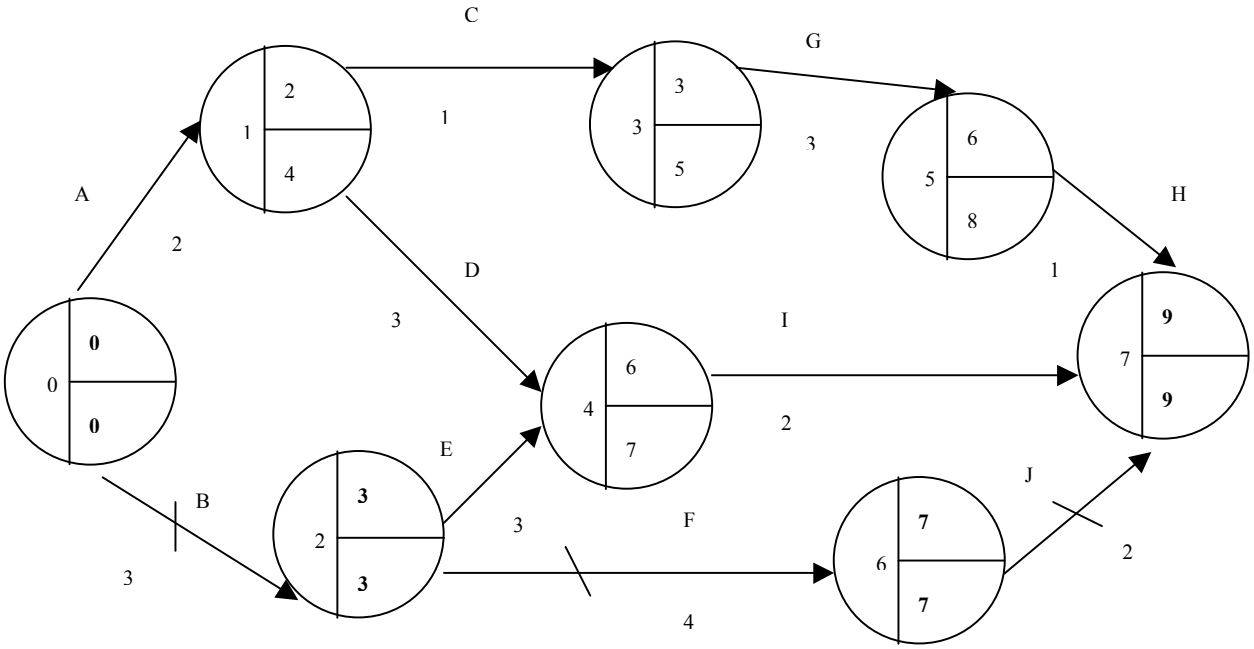
Slack is the amount of time that an activity can be delayed past its earliest start or earliest finish without delaying the project. The *slack time* for an activity is the time between its earliest and latest start time, or between its earliest and latest finish time.

The critical path is the path through the project network in which none of the activities have slack, that is, the path for which EST=LST and EFT=LFT for all activities in the path. A delay in the critical path delays the project. Similarly, to accelerate the project it is necessary to reduce the total time required for the activities in the critical path.

Convention:



Where N is node (activity) number
ES – Earliest Event Start Time
LS – Latest Event Start Time



Critical Path: BFJ

>> 6. Update CPM Diagram

As the project progresses, the actual task completion times will be known and the network diagram can be updated to include this information. A new critical path may emerge, and structural changes may be made in the network if project requirements change.

CPM Limitations

a) CPM was developed for complex but fairly routine projects with minimal uncertainty in the project completion times. For less routine projects, there is more uncertainty in the completion times, and this uncertainty limits the usefulness of the deterministic CPM model. An alternative to CPM is the PERT project-planning model, which allows a range of durations to be specified for each activity.

Complex projects require a series of activities, some of which must be performed sequentially and others that can be performed in parallel with other activities. This collection of series and parallel tasks can be modeled as a network.
In 1957, the Critical Path Method (CPM) was developed as a network model for project management. CPM is a deterministic method that uses a fixed time estimate for each activity.

b) While CPM is easy to understand and use, it does not consider the time variations that can have a great impact on the completion time of a complex project.

The *Program Evaluation and Review Technique* (PERT) is a network model that allows for randomness in activity completion times. PERT was developed in the late 1950's for the U.S. Navy's Polaris project having thousands of contractors. It has the potential to reduce both the time and cost required to complete a project.

The Network Diagram

In a project, an activity is a task that must be performed and an event is a milestone marking the completion of one or more activities. Before an activity can begin, all of its predecessor activities must be completed. Project network models represent activities and milestones by arcs and nodes. PERT originally was an *activity on arc* network, in which the activities were represented on the lines and milestones on the nodes. Over time, some people began to use PERT as an *activity on node* network. For this discussion, we will use the original form of activity on arc.

The PERT chart may have multiple pages with many sub-tasks.

The milestones generally are numbered so that the ending node of an activity has a higher number than the beginning node. Incrementing the numbers by 10 allows for new ones to be inserted without modifying the numbering of the entire diagram. The activities in the above diagram are labeled with letters along with the expected time required to complete the activity.

Steps in the PERT Planning Process

PERT planning involves the following steps:

1. Identify the specific activities and milestones.
2. Determine the proper sequence of the activities.
3. Construct a network diagram.
4. Estimate the time required for each activity.
5. Determine the *critical path*.
6. Update the PERT chart as the project progresses.

>> 1. Identify Activities and Milestones

The activities are the tasks required to complete the project. The milestones are the events marking the beginning and ending of one or more activities. It is helpful to list the tasks in a table that, in later, steps can be expanded to include information on sequence and duration.

>> 2. Determine Activity Sequence

This step may be combined with the activity identification step since the activity sequence is evident for some tasks. Other tasks may require more analysis to determine the exact order in which they must be performed.

>> 3. Construct the Network Diagram

Using the activity sequence information, a network diagram can be drawn showing the sequence

of the serial and parallel activities. For the original activity-on-arc model, the activities are depicted by arrowed lines and milestones are depicted by circles or “bubbles”.

If done manually, several drafts may be required to correctly portray the relationships among activities. Software packages simplify this step by automatically converting tabular activity information into a network diagram.

>> 4. Estimate Activity Times

Weeks are a commonly used unit of time for activity completion, but any consistent unit of time can be used.

A distinguishing feature of PERT is its ability to deal with uncertainty in activity completion times. For each activity, the model usually includes three time estimates:

- *Optimistic time* - generally the shortest time in which the activity can be completed. It is common practice to specify optimistic times to be three standard deviations from the mean so that there is approximately a 1% chance that the activity will be completed within the optimistic time.
- *Most likely time* - the completion time having the highest probability. Note that this time is different from the *expected time*.
- *Pessimistic time* - the longest time that an activity might require. Three standard deviations from the mean are commonly used for the pessimistic time.

PERT assumes a beta probability distribution for the time estimates. For a beta distribution, the expected time for each activity can be approximated using the following weighted average:

Expected time = (Optimistic + 4 x Most likely + Pessimistic) / 6

This expected time may be displayed on the network diagram.

To calculate the variance for each activity completion time, if three standard deviation times were selected for the optimistic and pessimistic times, then there are six standard deviations between them, so the variance is given by:

$[(\text{Pessimistic} - \text{Optimistic}) / 6]^2$

>> 5. Determine the Critical Path

The critical path is determined by adding the times for the activities in each sequence and determining the longest path in the project. The critical path determines the total calendar time required for the project.

If activities outside the critical path speed up or slow down (within limits), the total project time does not change. The amount of time that a non-critical path activity can be delayed without delaying the project is referred to as *slack time*.

If the critical path is not immediately obvious, it may be helpful to determine the following four quantities for each activity:

- EST - Earliest Start time
- EFT - Earliest Finish time
- LST - Latest Start time
- LFT - Latest Finish time

These times are calculated using the expected time for the relevant activities. The earliest start

and finish times of each activity are determined by working forward through the network and determining the earliest time at which an activity can start and finish considering its predecessor activities. The latest start and finish times are the latest times that an activity can start and finish without delaying the project. LS and LF are found by working backward through the network. The difference in the latest and earliest finish of each activity is that activity's slack. The critical path then is the path through the network in which none of the activities have slack.

The variance in the project completion time can be calculated by summing up the variances in the completion times of the activities in the critical path. Given this variance, one can calculate the probability that the project will be completed by a certain date assuming a normal probability distribution for the critical path. The normal distribution assumption holds if the number of activities in the path is large enough for the central limit theorem to be applied.

Since the critical path determines the completion date of the project, the project can be accelerated by adding the resources required to decrease the time for the activities in the critical path. Such a shortening of the project sometimes is referred to as *project crashing*.

>> 6. Update as Project Progresses

Make adjustments in the PERT chart as the project progresses. As the project unfolds, the estimated times can be replaced with actual times. In cases where there are delays, additional resources may be needed to stay on schedule and the PERT chart may be modified to reflect the new situation.

Benefits of PERT

PERT is useful because it provides the following information:

- Expected project completion time.
- Probability of completion before a specified date.
- The critical path activities that directly impact on the completion time.
- The activities that have slack time and that can lend resources to critical path activities.
- Activity start and end dates.

Limitations

The following are some of PERT's weaknesses:

- The activity time estimates are somewhat subjective and depend on individual group judgment. In cases where there is little experience in performing an activity, the numbers may be only a guess. In other cases, if the person or group performing the activity estimates the time,there may be bias in the estimate.
- Even if the activity times are well estimated, PERT assumes a beta distribution for these time estimates, but the actual distribution may be different.
- Even if the beta distribution assumption holds, PERT assumes that the probability distribution of the project completion time is the same as that of the critical path. Because other paths can become the critical path if their associated activities are delayed, PERT consistently underestimates the expected project completion time.

The underestimation of the project completion time due to alternate paths becoming critical is perhaps the most serious of these issues. To overcome this limitation, Monte Carlo simulations can be performed on the network to eliminate this optimistic bias in the expected project completion time.

Gantt Chart

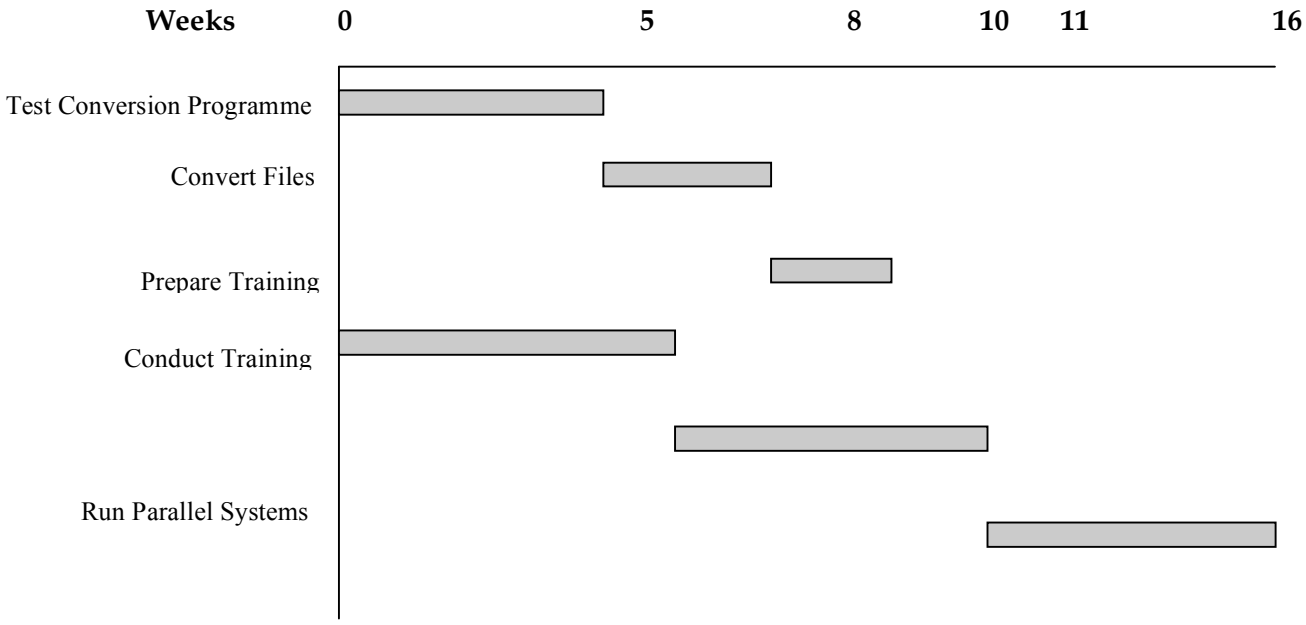
A Gantt chart is a simple horizontal bar chart that depicts project tasks against a calendar. Each bar represents a named project task. The tasks are listed vertically in the left hand column. The horizontal axis is a calendar timeline. The Gantt chart was first conceived by Henry L. Gantt in 1917, and is the most commonly used project scheduling and progress evaluation tool.

Gantt charts give a clear, pictorial model of the project. They are simple and require very little training to be understand and used. They show progress and can be used for resource planning. They also show interrelationships and critical path.

Gantt Chart Methodology

- List vertically all tasks to be performed
- Tasks identified by number and name
- Horizontally indicate duration, resources and any other relevant information
- Graphical part shows horizontal bar for each task connecting start and end duration
- Relationships can be shown by lines joining tasks – can make diagram

Example of a Gantt Chart (File conversion)



Different approaches to system development are:

1. System Development Life Cycle (SDLC)
2. Structured Systems Analysis Design Methodology (SSADM) – Data driven methodology
3. Prototyping Method – User driven method
4. Rapid Application Development (RAD)

3. System Development Life Cycle

This is also known as traditional system development method or function driven method or process driven method. The method requires the analyst to follow a sequence of phases during the development and implementation of an information system. This involves people and is described as information system development project. The following are the system development cycle phases or stages:

1. Preliminary survey/study
2. Feasibility study
3. Facts finding and recording
4. Analysis
5. System design
6. System development
7. System implementation

3.1 Preliminary study

This stage involves determination of whether there is need to change the existing system or business procedures. It may require management requests for a change of the existing system to give an organisation a competitive advantage or to improve the staff morale. The user department should be involved during the definition of the problem. The problem to be solved should be very specific, clear and precise. It should not be too broad to cause ambiguities in its solution.

Objectives of the preliminary study are:

- To understand organisational characteristics and its objectives.
- To understand organisational structure.
- To identify organizational mission and collect relevant data or document regarding organizational information.
- To develop a brief and accurate problem statement usually known as system terms of reference (TOR).

Terms of reference

It is a documentation prepared by the steering committee to act as a reference document throughout system development stages. Its contents include:

- Project title

- Subject of study
- Purpose of study
- Personnel
- Departments
- Sections affected or involved in the system implementation.
- Available resources and constraints, the analyst, the project leader should consider
- The projects estimated duration and schedule.

The importance of terms of reference is:

i. Provides information about the proposed system
ii. It may act as a reference document throughout the system development process
iii. It acts as an authorisation document to the project development team by the management
iv. It gives the scope and extent of the proposed system project, thus setting out systems limitation and capability.
v. It sets out the objectives of the proposed system

Steering committee

It is formed by two or three people to oversee the system development project from its initiation to its completion. It comprises the system analyst as the project leader and a representative of the user department. They should understand all the processing objectives and procedures within the affected department. A management representative and accountant or auditors may be incorporated to advise initially on financial aspects of the project.

The roles of the steering committee are:

a) To study the current processing procedures that may require to be improved.
b) To prepare problem statement in form of terms of reference.
c) To coordinate system development activities throughout the development life cycle.
d) To interface the project development team with organisational management.
e) To resolve conflict that may arise during system development.
f) To direct, control and monitor the system development progress.

3.2 Feasibility study

Fast Forward: The Feasibility Study is based on the Functional Brief findings and outcomes.

This is a more detailed study carried out by a feasibility study team. Its purpose is to define the problem and decide whether or not a new system to replace the existing one is viable or feasible. During the study, the analyst should assess the magnitude of the problem and attempt to restrict or at least identify the scope of the project. The analyst must list precisely the problems of the current system and also indicate what would be required of the new system. He must identify alternative solutions to the problems and recommend the most cost effective solution.

Feasibility study activities include:

- Identification of main characteristics of the existing system

- Determination of the main output requirements
- Considerations of alternative ways of meeting similar requirements.
- Preparation of gross estimates of developments, implementation and operation costs for each probable alternative solution.
- Documentation of the study i.e. writing of feasibility study report.
- Preparation of gross estimates of possible direct and indirect benefits for each probable alternative.

The following are the areas of feasibility study:

a) Technical Feasibility
b) Social Feasibility
c) Economical Feasibility
d) Legal Feasibility

Technical Feasibility

Technical questions are those that deal with equipment and software e.g. determination of whether the new system can be developed using the current computer facilities within the company. Technical feasibility is thus aimed at evaluation one or more of the following:

i. The hardware required for the new system
ii. The software required for the new system
iii. Determination of whether the current facilities are adequate or inadequate for the new system after implementation.
iv. Evaluation of the current technology and how applicable it is to the new system
v. Determination of the need for telecommunication equipment in the new system to improve both data capture and preparation activities.
vi. The inputs, outputs, files and procedures that the proposed system should have as compared to the outputs, files and procedures for the current system.
vii. Determination of whether training is necessary for the employees before the new system is implemented and the relevant skills required.
viii. Suggesting a suitable method of developing the new system, methods of running it when it becomes operational and ways of implementing it.

Social Feasibility

This is also known as operational feasibility. It mostly deals with the effect of the system on the current society within the company. It is carried out on the following areas:

i. The reaction of individuals both inside and outside the company as a result of the new system.
ii. The effect of the system on the existing organisational structure.
iii. The effect of the system on the current working practices and management levels i.e. whether there would be any change required and if so the cost of the change socially.
iv. Redundancy or retrenchment, implication to the company as a result of the new system.
v. Implication of the system on existing staff development programmes.

The social feasibility is carried out along with technical feasibility such that the social implications of every alternative technical solution to the problem that emerges are evaluated. Areas to

consider include:

- Group relationships
- Salary levels
- Job titles and job descriptions
- Social costs to be evaluated e.g. cost of user training, consultancy that may be engaged during development of the new system, job improvements and salary changes.

Legal Feasibility

The new system's legal implications should be evaluated e.g. if it requires that the computer should be insured or whether the stored data should be registered with the government registrar before use. The copyright implication for restriction should be assessed before the new system is implemented. Generally, any legal aspects associated with the new system should be assessed, and adequate measures taken to protect the interest of the user company.

Economic Feasibility

Economic feasibility is aimed at determining of whether or not to continue with the project, depending on whether it is economically viable. The systems benefits and estimated implementation cost should be determined before any further resources can be spent on the project.

A cost benefit analysis (CBA) is carried out to determine whether the new system is economically viable.

Cost Benefit Analysis (CBA)

Benefit Analysis: Is obtained through comparison of the new system with the existing one. Benefits of the new system fall under two categories i.e. direct and indirect benefits as well as tangible and intangible benefits.

i. Direct (Tangible)–fall under two categories: measurable benefits and direct savings.

Measurable benefits are those that can be quantified in monetary terms e.g. increase in working capital as a result of purchasing of computer systems or reduction of delays in decision making which is obtained through improved procedures e.g. invoicing procedures and credit control procedures.

Direct savings are those costs, reduced or eliminated as a result of introduction of computerised system. They include reduction or elimination of clerical personnel and elimination of some specific costs e.g. stationery costs. Like measurable benefits direct savings can be quantified in monetary terms.

ii. Intangible benefits – they are benefits that cannot be quantified in monetary terms or those that are difficult or impossible to quantify in monetary terms.

They are clearly desirable but very difficult to evaluate in terms of money value e.g. improved customer satisfaction, better information, improved organisational image, increased staff morale and a competitive advantage to an organisation.

Cost Analysis: Costs are expenses or expenditure, which are incurred by a system. These may include equipment cost, development cost, operation cost and software cost. During cost

analysis, one should consider both the new and the existing system. The cost of retaining and operating the existing system should be compared to the cost of introducing and running the computerised information system.

These costs fall under the following categories:

a) The cost of running the existing system. This is calculated from the past records. The items to consider include:

   i. Man power cost – which is extracted from the budgets and payroll reports
   ii. Material cost – which includes consumables e.g. stationery, work in progress and current stock
   iii. Operational cost e.g. the equipment cost expressed in terms of unit rate. Others to consider include the duration the project takes to be completed and initial replacement cost.
   iv. Overhead costs – which are direct expenses incurred by the company on behalf of all departments e.g. rent, electricity, telephone bill etc. These can easily be extracted from departments or centres to which they are allocated.
   v. The intangible cost of existing system e.g. loss of sales or cost of sales as a result of inappropriate stock levels or loss of interest in bank as a result of improper credit control system.

b) The cost of operating the proposed system – this is likely to include all the areas covered above i.e. manpower, materials, overheads and the intangible costs. However, there are additional costs associated with computerised systems e.g. service contracts for the computer system, insurance of the computer system, cost of data transmission, cost of consumables like printer cartridges, ribbons etc. All these costs should be evaluated or estimated as accurately as possible.

c) The cost of new system development – Includes the cost incurred for any consultancy services that may have been hired during development. Allowances given to the system development team members fall under this category. Overall effects of the system development and implementation should be determined and any cost associated established. These estimates are based on both time and activities involved in the project. Staff training cost, recruitment costs and retrenchment costs should be considered under system development cost.

Cost benefit analysis should be conducted on each alternative solution to the problem. This enables the analyst to make recommendation is on a suitable cost-effective alternative solution to the problem.

Cost benefit analysis techniques

The techniques used in economical evaluation of a computer based information system are the same used in investment appraisal in other areas of commercial world. These techniques tend to produce contradictory results and none of them is universally accepted. These techniques are based on either marginal costing methods or life cycle costing method. Marginal costing methods deal with snapshots of systems performance at a given point in time. Life cycle costing methods deal with measuring system performance over its working life.

These techniques include:

- The ARR (Accounting Rate of Return)
- Pay Back Period
- Discounted Cash flow – Net Present Value (NPV)
- Internal Rate of Return (IRR)

Some of the limitations of CBA are:

- Difficult to consider all factors that might contribute to costs or benefits.
- Difficult to quantify some costs and benefits.

Feasibility study report

After the feasibility study and the cost benefit appraisal, a report is prepared that gives recommendations on whether or not to commit any further resources on the project.

The contents of the feasibility study report include:

- Introduction – It gives general description of the existing system, the people contacted during the study and purpose of the report.
- Description of the alternative proposed systems in terms of the inputs, outputs, file processed, response time, etc.
- Quantification to justify the cost of running the proposed system
- The recommendation by the analyst on the most cost effective alternative solution.
- The author of the report
- System analyst is recommendations on the new system indicating whether to commit further resources.
- If the decision is to continue with the project, its development plan should be given.

The report is submitted to the management for approval. After approval, a more detailed survey is conducted on the existing system mostly to establish its weaknesses and strengths. This is called fact-finding or fact gathering.

3.3 Fact finding/investigation

This involves collection of information about the existing system on which to base analysis in order to determine whether users current needs are being met. The following are some of the activities that are looked at:

a) Functional requirement – the requirements should be established
b) Determination of the proposed system requirements – this is necessary as it may suggest a change in the existing system requirement.
c) Establish any weaknesses or problems associated with the present system, working methods and procedures.
d) Determination of organisational growth rate – this will assist in determination of the growth of the volume of transactions to be processed.
e) Determination of the organisation structure, objective and the cost associated with the present system.

Fact-finding comprises of the following activities:

i. Fact-gathering
ii. Fact-recording
iii. Fact-evaluation

Fact-finding techniques

a) Use of questionnaires

A questionnaire is a special document that allows the analyst to ask a number of standard prepared questions set to be asked to a large number of people in order to gather information from them. It is suitable for use when:

- the system analyst is located at a considerably long distance from the respondent
- there is a large number of respondents such that interviewing them will be limited by time
- the questions to be asked are simple and straight forward and require direct answers
- limited information is required from a large number of people
- it is used as a means to verify facts found using other methods.

Advantages of using questionnaires are:

- They provide a cheap means of gathering information/data from a large number of people.
- They encourage individuals to provide response without fear, intimidation or victimization.
- The respondents can complete the questionnaire at their own convenience with minimal or limited interruption from their work.
- Questions are presented consistently to all without bias.

Disadvantages of using questionnaires are:

- Response is often too slow since the respondents complete and return the form at their own convenience.
- They don't provide an opportunity for respondents to obtain clarification of questions, which may appear vague or ambiguous.
- Do not provide an opportunity for the analyst to observe respondents' reactions.
- The design of questionnaires requires an expert who may charge expensively and may not be economical when administered to a small group of respondents.
- All forms may not be returned and also not all questions may be answered, which leads to incomplete data for analysis.

Requirements for preparing a questionnaire include:

- Questions should be simple and clear.
- Questions should be objectively oriented and one should avoid leading questions.
- Questions should be logically organised.
- The form should be neat.

b) Interviewing

This is a face-to-face conversation between the system analyst (the interviewer) and users

(interviewees). He obtains answers to questions he asks the interviewee. He gets the interviewee's suggestions and recommendations that may assist during the design of the proposed system.

Interviews serve the following purposes:

- Act as a method of fact-finding to gather information/responses about the existing system.
- Used for verifying facts gathered through other methods.
- Used for clarifying facts gathered through other methods.
- Used to get the user involved in the development of the new system.

Interviews are used in the following circumstances:

- When the respondents are few e.g. corporate managers
- When the respondents are physically available and accessible
- When the main emphasis of the system investigation is people
- When the analyst wishes to seek direct answers, opinions, suggestions and detailed information
- When the analyst wishes to verify validity of facts collected through other techniques
- When immediate response is required

Interviews have the following advantages:

- The analyst can frame questions differently to individuals depending on their level of understanding. Thus it allows detailed facts to be gathered.
- The analyst can observe non-verbal communication from the respondents or interviewees
- The response rate tends to be high
- Provides immediate response
- The analyst can get detailed facts from each respondent

Disadvantages of interviews are:

- Costly and time consuming when used on a large number of people
- Success highly depends on the analysts human relation skills, expertise and experience.
- May not be practical due to location of respondents.
- May make respondents to feel that they are being summoned or grilled by theanalyst
- Interviews can fail due to:
  - Ambiguous questions being asked
  - Personal questions being asked
  - Inadequate time allocation for the exercise
  - Lack of earlier preparation by both parties
  - When the analyst is biased on using technical jargon

c) Observation

Observation is the most effective fact-finding technique but requires the analyst to participate in performing some activities carried out by the user. He may choose to watch them as they perform their activities and gather the facts intended.

This method is best used in the following circumstances:

- When the validity of facts gathered through other methods is questionable
- When complexity of certain aspects of a system prevent a clear explanation by the respondents or the user
- Used to confirm that the procedures specified in the manuals are being followed.
- When one needs to obtain first hand and reliable information

Guidelines when using the observation method include:

- There should be permission from concerned authorities before the exercise
- Gathered facts should be recorded
- Those to be observed should be notified and the purpose of the exercise explained
- The analyst should be objective and avoid personal opinion. He should have an open mind
- The analyst should also record ordinary events

Advantages of observation method include:

- Data gathered is highly reliable thus the method can be used to verify facts collected through other methods
- The analyst can see what is being done clearly including the tasks, which are difficult to explain clearly in writing or in words
- Inaccuracy or inaccurately described tasks can easily be identified
- It allows the analyst to easily compare gathered facts through other methods and what actually happened on the ground
- Relatively cheap compared to other methods

Disadvantages of observation method are:

- People feel uncomfortable when being observed and behave abnormally thus influence the analyst's conclusions/Hawthone effect
- The exercise may take place at odd times thus inconveniencing those involved
- The analyst may observe exceptional activities, leaving some critical areas. His patience and expertise play a great role
- The tasks being observed may be interrupted and the analyst may gather wrong facts

d) Record inspection/Document review

This method involves perusing through literature or documents to gain a better understanding about the existing system. Examples of documents that are perused include sales orders, job descriptions, existing systems documentation, management reports, procedure manuals, organised structure charts, trade journals, etc.

This method is best used when:

- The analyst needs to have a quick overview of the existing system
- The information required cannot be obtained through any other techniques

STUDY TEXT

Advantages of this method are:

- It is relatively cheap compared to other techniques
- It is a faster method of fact finding especially when documents to be considered are few

Disadvantages of this method are:

- Time consuming if the documents are many or if they are not within the same locality.
- Unavailability of relevant documents makes this method unreliable.
- Its success depends on the expertise of the analyst.
- Most of the documents or information obtained may be outdated.

e) Sampling

Sampling is the systematic selection of representative elements of a population. The selected elements are examined closely and the results assumed to reveal useful information about the entire population.

This method is used when the target population:

- Is too large and it is impractical to study every element of the population
- Contains homogenous elements (those with similar characteristics)

Advantages of sampling are:

- It reduces cost e.g. by avoiding to examine every document or talking to everyone in the organisation to gather facts
- It speeds up the fact-finding process.
- It improves effectiveness since one can concentrate on a few people and fewer documents to get adequate and accurate information.
- May reduce biases, if a representative sample is taken. All the elements of the population stand a chance of being selected.

Disadvantages include:

- The sample may not be representative enough, which may lead to incorrect and bias conclusions
- The expertise of the analyst is required since sampling involves a lot of mathematical computation

3.4 Analysis

A system analysis involves evaluation of the current system using the gathered facts or information. One should evaluate whether the current and projected user needs are being met. If not, he should give a recommendation of what is to be done. Analysis involves detailed assessment of the components of the existing system and the requirements of the system.

The objectives/aims of system analysis are:

- To determine information needs of an organisation and the users of that information
- Determination of the current activities of the system i.e. functions involved in conversion of inputs to outputs
- Determination of the intended systems output
- Determination of the resources required for the intended system
- Determine capabilities required in the system to meet information needs of the organisation.

System analysis activities are:

i) Analysis of the organisation environment. The analyst should evaluate in details information needs of the organisation environment e.g. information needs of the consumers, suppliers, competitors, government departments, etc.

ii) Analysis of the present system. The analyst should study the current system and identify its weaknesses and its strengths. He should establish the ability of current system in meeting the stated information needs. This guides a decision to be made on whether the existing system stands to be improved, changed or done away with altogether. Some aspects of the existing system that are examined include input transactions, outputs or results, existing controls, files, user interaction, methods, procedures, functions and existing hardware and software.

iii) Requirement analysis – involves determination of user requirements e.g. task performed, output expected, proposed system development cycle and user goals. The following are also determined:
- Maximum, minimum and average level of activities.
- Duplicate procedures e.g. two people entering the same transaction at different times.
- Labour intensive tasks – the tasks that are manual and can easily be computerised.
- Activities or tasks that involve complex or repetitive computation
- Procedures that have become obsolete.

Once all the facts are analysed and documented, a formal report is written called statement of requirements.

The contents of statement of requirements are:

i) Description of the initial system goals and whether or not they are met and are still applicable

ii) Description of the existing system's cost effectiveness.

iii) Description of whether the output produced is adequate, timely and well controlled.

iv) Description of whether files held are suitable for supporting current organization requirements.

v) Description of current system inputs and whether or not they support current file maintenance activities.

vi) Description of the existing system workflow efficiency.

vii) Description of any constraints within the system.

viii) Description of any existing system equipment, procedures and controls that can be transferred to the new system.

The importance of system analysis includes:

- It helps the analyst or system developer to gain understanding of the existing system.
- It allows the analyst or system developer to record existing system information in a standard form to aid design of a new system. It also facilitates understanding of the system by the user staff.
- Enables the analyst or developer to define existing system procedure into a logical model.
- Helps the analyst to write or produce statement of requirements, which guides the development team throughout subsequent stages of the development life cycle.

3.5 System design

The objective of system design is to put a logical structure of the real system in a form that can be interpreted by other people apart from the designer. The analyst should derive a logical model of the way the existing system works. There is an assumption that the existing system provides a good guide to what is required of a new system. It should be different from how the new system is to achieve the given requirement.

Limitations of system design include:

- There could be some requirements of the new systems that are not currently being satisfied by the current system. These requirements should not be taken into account.
- Inefficiency in the current system may be translated into a logical model and these will be transferred to the new system. Ideally, the models should reveal the logic of an efficient system and should be amended accordingly.
- It is likely that physical aspects of the existing system may be transferred to the logical analysis. The analysts should guard against that.

The above limitations can be dealt thus:

- Treatment of the new requirement: The new requirement can be estimated through interviews with management and users. It is important that the logical model be amended to reflect the new requirements. They are likely to lead to new processes that are added to higher-level design.
- Treatment of inefficiencies: The model should be adjusted through the decomposition of top level design tools e.g. DFDs. The lower level data flow diagram (DFD) tends to be determined partly by what is done in existing system to fulfil a function.
- Treatment of physical aspects: Certain physical considerations may have shifted into a logical model e.g. a data store or file may contain extra information which may require amendment e.g. to incorporate separate files.

There are two types of design: logical design and physical design.

Logical Design

A logical design produces specifications of major features of the new system, which meets the system's objectives. The delivered product of the logical design is a blueprint of the new system.

It includes the requirements of existing system components:

- Outputs (reports, displays, timings, frequencies, etc)
- Inputs (dialogs, forms, screens, etc)
- Storage (requirement for data to be stored in databases)
- Procedures (to collect, transform and output data)
- Controls (requirements for data integrity, security, data recovery procedures)

Note: Logical design of the system is viewed in terms of what process i.e. procedures, inputs, outputs, storage and control that the new system should have.

Physical Design

It takes the logical design blueprint and produces the programme specification, physical files or database and user interface for the selected or targeted hardware and software. Physical design is mostly concerned with how the current system or future system works in terms of how the programmes are written, files organised in storage media and how tasks are carried out for user interface with the system.

System design objectives

The designed system should meet the following criteria:

- User needs are met as cost effectively as possible
- One that is within the constraints laid down in the terms of reference
- Produce correct outputs by processing data accurately and efficiently
- Simple to operate i.e. easy to use
- One with sufficient built in controls and provide feedback to its user
- Should be reliable
- Should be functional

System design constraints

- The budget: A well-designed system incurs greater expenses. The total system cost of meeting the objectives must be considered in the light of the available budget.
- Time: Time taken to produce a very usable system would increase development cost and delay system delivery.
- Integration with other existing system: Existing and planned system may limit option and available features of the system.
- Skills: Limitation may arise from the range of skills and level of competence in both the design team and the system users.
- Standards: Standards may drive the design tasks in a specified direction.

Input and output design

The input and output design of a new system starts by choice of input and output media.

Factors to consider include:

- Input and output contents
- Contents layout
- Nature of the system

Some factors are considered during output design although such other factors as the following are considered:

- How the information will be used
- The timings and frequency of the output, and
- The complexity of the information contained in the report

Printed output design

There are two types i.e. pre-printed forms and computer generated reports.

The pre-printed output design begins by drafting copies, which are then passed on to an expert graphic designer to create necessary documents. They are then printed on a continuous basis.

Examples include: a purchase order, invoices and statements. A programmer then writes a programme, which controls a specific type of print and fills up the variable data on the document. The computer generated report format is influenced by user organisation standards. The user and the management should participate in the original design draft and also approve the final printed reports or outputs. This may be done through the use of a prototype.

Screen design

In order to produce an effective screen dialogue, several factors should be considered:

i) The hardware in which the interface will be implemented e.g. a VDU, mini computers etc. These should include the hardware ability to use graphics, colour or touch sensitive panels.
ii) The software pre-loaded on hardware e.g. the pre-loaded operating system, whether it is DOS-based or windows-based.
iii) Memory capacity i.e. RAM and hard disk in order to determine the size of the application to be developed

Interface techniques

It is important to consider the characteristics of the proposed system of input and output interface design. Modern screen dialogue interface will always apply three types of combination i.e. form filling, menu selection and WIMP interface.

Form filling

It is an effective form of interface where verification involves data capture. Some of the guidelines to form filling include:

- Forms should be easy to fill
- Information should be logically organised or grouped e.g. headings identification, instructions, body, totals and any comments
- Should be clear and attractive
- Should ensure accurate completion

Menu interface (selection)

It is designed to allow an operator to select increasingly detailed options or choices with each menu screen covering a different function. This is made clear by use of colour screen and WIMP

interface. The bottom option is usually reserved for the error message or for help facility.

WIMP (Windows Icon Mouse and Pull-down menu)

It is not created by the system team but it is an environment that allows computer users to manipulate the operating system as well as application programmes. WIMP tends to be used in PCs but can also be used in multi-user system workstation. They have to allow users to generate screen dialogue by prototyping. Prototyping is used to allow the user to see the interface on the screen and also simulate menu operations, cursor movements and screen changes in form-filling techniques.

Programme design

A programme can also be referred to as a module, process, unit, routine, procedure, function, macro, segment or fragment depending on its size and the scope of operation.

The following are some important aspects of a programme:

- One function: A program should carry out only one task. If several interrelated programmes are linked together, they form a system, which is easy to maintain for it comprises of several units.
- Size: A programme should be small enough so that it is easy to maintain, can take less memory and make optional use of the CPU.
- Cohesion: This measures the strength of relation within a programme. This implies that what happens in one sub-routine affects the other sub-routine or other programmes. A programme that performs more than one function has a low cohesion. A high degree of cohesion within a programme results in low coupling between programmes.
- Coupling: Is a measure of the strength of the bond between programmes. Ideally, programme should have little dependencies on other programmes in the system. This is so that any amendment to it should have little or no impact on other programmes in the system. Programmes should thus be developed in modules.

Systems are broken down into modules because smaller programmes (modules) are easier to specify, test and modify than larger programmes. Therefore, errors of the impact of a change are confined within fewer lines of code when modules are used. Programmers can also choose the area of the system that interests them to code, which is motivating to them. A large number of small programmes make rescheduling work easier i.e. same programmes can be assigned to someone else to write if the first programmer is taking longer than estimated for a particular programme.

For a system to be broken down into modules, a good system specification should be prepared.

System specification

It is a document prepared at the design stage of system development life cycle. It represents the conceptual system or logical system. This is a system in paper form. Its contents are:

i) Introduction of existing system i.e. details of its objectives and a brief description of how

these objectives are met.

ii) Description of the proposed system i.e. details of its objectives and a description of how the objectives are to be met.

iii) Justification of proposed system as a solution to the problem specified in terms of reference. Costs and benefits justification for the proposed system should be shown.

iv) Comparison of both existing and proposed system in terms of inputs and outputs i.e. specification of frequency, volume, timings, etc.

v) Proposed system file descriptions: This should include file names, organisation methods, access methods, nature of the system, storage media, record structures and file activities.

vi) Proposed system control specifications i.e. error handling procedures, recovery procedures, in built controls both hardware and software related.

6.6 System development

This involves programming, testing and documentation activities.

(a) Programming

This activity involves translation of system specification into programme code. A programmer should integrate user requirements into the computer system. Programming standards should be adhered to e.g. use of a standard programming language. Decomposition of a programme into smaller units or modules should be implemented as per the design specifications. It is important that the programming team work in cooperation to improve the quality of programmes produced.

The contents of a good programme specification are:

- Document details: This includes title, programme identifier i.e. name, author, version number, reviewer of the program, etc.
- Introduction: contains a brief summary of what the program does in business application area
- Assumption and restriction: this lists any constraints on the program or information that affects the logic of the problem.
- Attributes: this outlines the programme environment e.g. hardware, operating system, programming language etc.
- Data: inputs and outputs of the programme.
- Functional description: the processing or tasks carried out to convert programme input into meaningful outputs.
- Detailed processing requirement: indicates functional description i.e. low level detailed view of the processing paths.
- Operation consideration: Describes how operations interact with the programme in the normal running and how he can recover to save state or restore the programme if anything goes wrong
- Sub-routines: these are modules or segments used by the programme as well as their input parameters.
- Messages: identifies message sent and received by the programme and their purpose
- Print layout: Describes print or screen dialogue or layout of the programme.

(b) Testing

Generally all programmes should be tested before system conversion. There are two major program-testing techniques: white box and black box testing.

White box testing

It concentrates on internal construction of a programme. It is carried out on the following:

i. Cyclomatic complexity - are measures of logical complexity of a program
ii. Graph matrix - are used for condition testing
iii. Data flow testing – commonly associated with SSADM. It is used to select paths of a programme according to location and definition of variables.
iv. The loop testing – it focuses on exclusive validity of loops within a program

Black box testing

It focuses on functional requirements of software. It attempts to find errors in the following categories:

- Incorrect or missing functions
- Interface errors
- Data structure errors
- Performance errors
- Initialisation and termination errors

These methods are based on the input and output to and from a programme. They do not emphasize on the internal structure of a program.

Software testing is conducted on the following aspects or stages:

(i) Unit testing: testing of programme segments that do specific functions. It emphasises on the local data structure, boundaries, interfaces etc.
(ii) Module testing: involves testing of interrelated units within a programme, which perform a specific task. It emphasizes on local data structure, error handling and independent programme parts. A module is a segment of an entire system that does a specific task. Debugging and correction of errors during each individual program segment could be part of module testing.
(iii) Integration testing: Also known as verification or programme construction testing. It involves moving downwards through a control hierarchy i.e. from subordinate modules it can either be top-down integration or bottom-up integration. Top-down integration verifies major control and decision points early in the testing process. Bottom-up integration uses drivers to coordinate a test case.
(iv) System testing: involves linking all modules of a suite to test whether they are interfacing properly. Its primary purpose is to fully test functionality of a computer- based system. Integration testing is testing of modules during the time they are being linked up or combined together into a suite.
(v) Alpha and Beta testing: Alpha testing is testing that is conducted at the software developer's site by both the developer and the user or customer. Beta testing is testing a system at the user's or customer's site. It is conducted by the end user of the system.
(vi) Configuration review: It is conducted to ensure that each element of the software is properly developed i.e. to ensure that each module's configuration is proper.

(vii) Recovery testing: Is conducted to force software to fail in a number of ways and verify that recovery is properly performed.
(viii) Security testing: It attempts to verify that protection mechanism built into the system works.
(ix) Stress testing: Designed to confront a programme with abnormal structure and abnormal quantity of resources e.g. a large volume of transaction inputs to see how the programme can cope up with such abnormally.
(x) Performance testing: Conducted to evaluate the software performance e.g. run time, response time, quality of output, etc.
(xi) Acceptance testing: This is carried out by software users and management representation for the following reasons:
- To discover software errors not yet detected
- To discover the actual and exact demands of the system
- To discover if any major changes required by the system can be adopted.

Structured walkthrough (peer review)

It is a planned review of system by people not involved in its development effort. It is carried out to establish areas where improvement can be made in the system or its development process. The review is done by between 5-10 people as a software quality assurance measure. Types of walkthrough include:

(i) Requirement review – It is conducted to examine a proposed system as formulated by the system analyst. If there are any inconsistencies between the requirements stated by the users and those that the analyst is proposing, the walkthrough should be able to uncover such inconsistencies so that they can be dealt with early enough.
(ii) Design review – Its purpose is to determine whether the proposed design will meet the requirements of the system and user. If the review team finds any discrepancies between the design and the requirement, they should give solutions to such discrepancies.
(iii) Programme review – This is conducted to examine the programme development along with its documentation. The programmes are compared with their specific design specifications to determine whether the specifications are being satisfied. Any programming errors are detected and dealt with.
(iv) Testing review – It assists in development of test data that can be used to detect system design errors. The system testing strategy is not to prove programmer correctness but to assess reliability and suitability of the system through detecting critical system errors.

Walkthrough team members include:

i. Chairman – He controls the overall direction of a walkthrough and ensures that its agenda is adhered to. He gives approval by formally signing the project milestones when users are satisfied at each development stage.
ii. Author – He is the creator or designer of the system. He presents and explains the materials that are being walked through.
iii. Recorder – Acts as the secretary of the team and ensures that all agreed actions pointed out are noted and followed up.
iv. Reviewers – They get in advance the materials being walked through as a working model. They walk through the proposed system and check whether it falls short of required quality.

v. User representative – Approve their understanding and satisfaction of what they will do with the system when it becomes operational. The representatives may be senior managers, auditors, etc.

A structured walkthrough is important because:

- It identifies errors, omissions and inconsistencies in a system
- It focuses on quality of and good practices in system operation generally
- It involves the users and gives them an opportunity to give a feedback on critical appraisal of their work.
- It avoids description about who is responsible for what role thus encouraging team work
- It reduces user resistance since they are incorporated and recognised by the development team.

(c) Documentation

Software documentation is a description of software or system after its development. Software product therefore comprises of code and documentation. Documentation includes a wide range of technical and non-technical manuals, books, descriptions and diagrams relating to the use and operation of produced software. It is vital for software engineering to allocate adequate time to the software engineering particularly documentation throughout its development.

Documentation is produced for:

- System developer – who will depend on documentation from previous life cycle stages to guide continued development and subsequent maintenance of software or system.
- Management – who use documentation from past projects to plan and understand current projects
- System users – who learn how to use software or system from its narrative description or documentation.

Objectives of good documentation

The following factors should be considered when preparing a good documentation:

- Completeness – This implies that all known aspects or components of documents should be included.
- Consistency – Inconsistency will destroy the reader's confidence in the documentation. The biggest challenge is not consistency in the original documentation but maintaining consistency through all the changes the software may undergo.
- Documentation should be targeted at the right levels – i.e. for its intended audience e.g. a training manual demands as much from its readers as design documentation to the programmer.

There are two major reasons why software engineers dislike producing documentation:

(i) They do not see the need for it because it may indicate that one is new to the profession and has not yet had time to appreciate the benefits of documentation. It may indicate also that one is so wrapped up in pressure of the moment that long-range goals have become absurd.

(ii) They do not feel capable of doing it. Although sometimes the feeling of inadequacy derives from inability to talk about technical subjects with non-technical people.

Importance of system documentation

(i) It guides the development team at various stages of the development life cycle
(ii) Can be used as a system backup copy to recover the system should something happen to its implementation.
(iii) It aids or assists during system maintenance since it guides in identification of system modules to be changed.
(iv) It can effectively provide a checklist of items to be covered during subsequent system audit or system maintenance.
(v) It guides against loss of system understanding particularly when the author leaves the company or dies.
(vi) It may act as a training guide or document to new programmers, analysts or users who may join after system implementation.

Contents of system documentation

(i) Table of contents – acts as a document index.
(ii) Introduction – indicates the system capabilities and constraints or limitations
(iii) System specification – it specifies the conceptual system in terms of process, data structures, files, etc.
(iv) A list of files to be used by the system – used for reference should something go wrong when the system is live.
(v) Test data – shows the data used to evaluate system functionality.
(vi) Recover procedures – guides the user on how to recover the system should something go wrong when the system is running.
(vii) Samples of input and output data – these help the user to identify errors when they occur during system live-running.
(viii) Back-up procedures – it advises the reader on how to make security copies of files for use to recover the system in case something goes wrong during system live-running.
(ix) Contacts – Address or phone number to be used by the operator to seek help if other options fail.

System Documentation: Fact Recording tools and techniques

(1) Flowcharts

A flowchart is a diagrammatic representation that illustrates the sequence of operations performed to get to the solution of a problem. Flowcharts facilitate communication between system analysts, system designers and programmers.

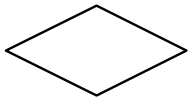
Guidelines for drawing a flowchart

Flowcharts are usually drawn using some standard symbols. Some standard symbols used in drawing flowcharts are shown on the opposite page:

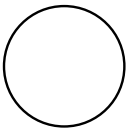

Start or end of the program - terminator

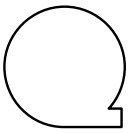

Process - Computational steps or program processing

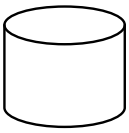

Alternate process

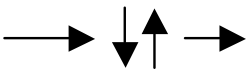

Decision making and branching

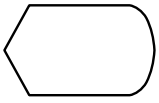

Data - Input or output operation


Connector or joining of two parts of program

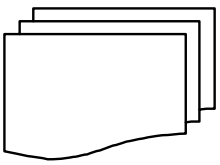

Magnetic tape


Magnetic disk


Flow lines


Display


Document

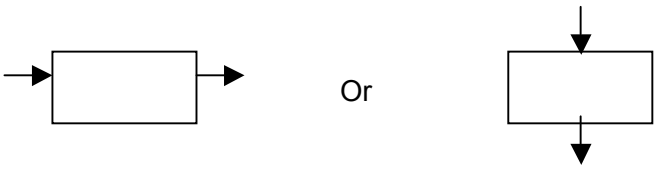

Multiple documents


Stored data

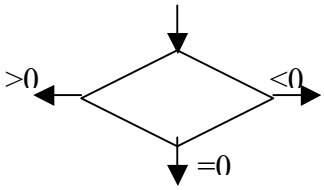
STUDY TEXT

The following are some guidelines in flowcharting:

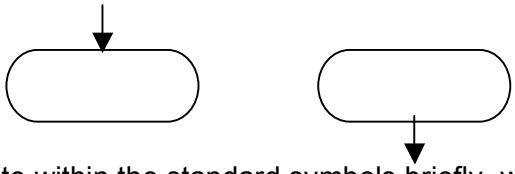
- In drawing a proper flowchart, all necessary requirements should be listed out in logical order
- The flowchart should be clear, neat and easy to follow. There should not be any room for ambiguity in understanding the flowchart
- The usual direction of the flow of a procedure or system is from left to right or top to bottom
- Only one flow line should come out from a process symbol



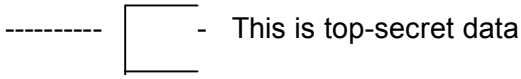
- Only one flow line should enter a decision symbol, but two or three flow lines, one for each possible answer, should leave the decision symbol



- Only one flow line is used in conjunction with the termination symbol



- Write within the standard symbols briefly. where necessary, you can use the annotation symbol to describe data or computational steps more clearly.



- If the flowchart becomes complex, it is better to use connector symbols to reduce the number of flow lines. Avoid the intersection of flow lines if you want to make it more effective and a better way of communication.
- Ensure that the flowchart has a logical start and finish
- It is useful to test the validity of the flowchart by passing through it with simple test data.

Types of flowcharts

Flowcharts are of three types:

- System flowcharts
- Run flowcharts
- Programme flowcharts

System Flowcharts

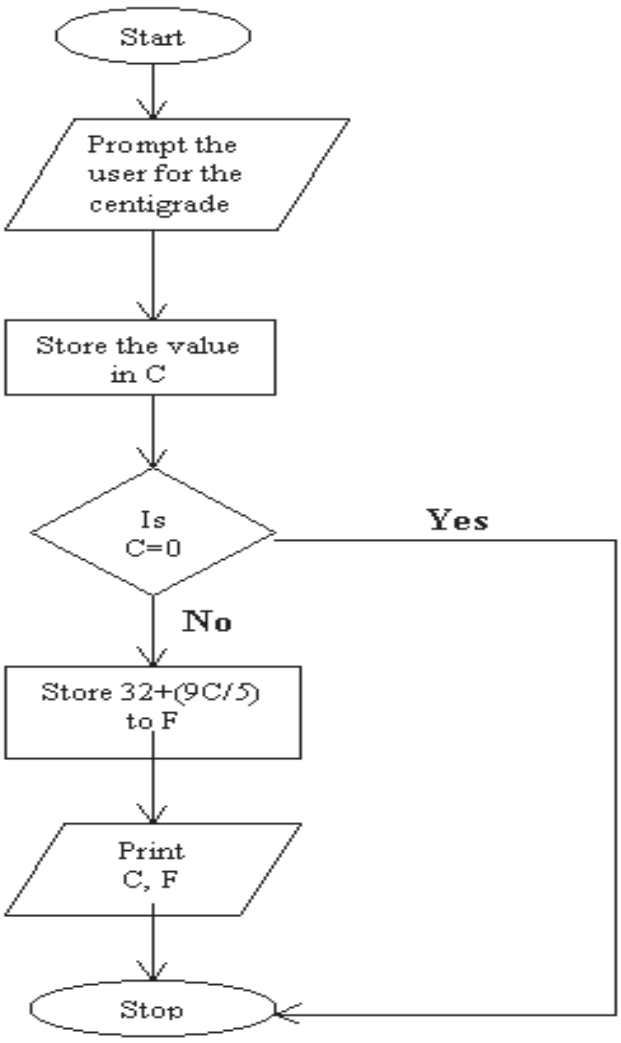
System flowchart describes the data flow for a data processing system. It provides a logical diagram of how the system operates. It represents the flow of documents, the operations performed in data processing system. It also reflects the relationship between inputs, processing and outputs. Following are the features of system flowcharts:

- The sources from which data is generated and device used for this purpose
- Various processing steps involved
- The intermediate and final output prepared and the devices used for their storage

The figure below is a sample of system flowchart for the following algorithm (step by step instructions on how to perform a certain task):

- Prompt the user for the centigrade temperature.
- Store the value in C
- Set F to 32+(9C/5)
- Print the value of C, F
- Stop

System Flowchart

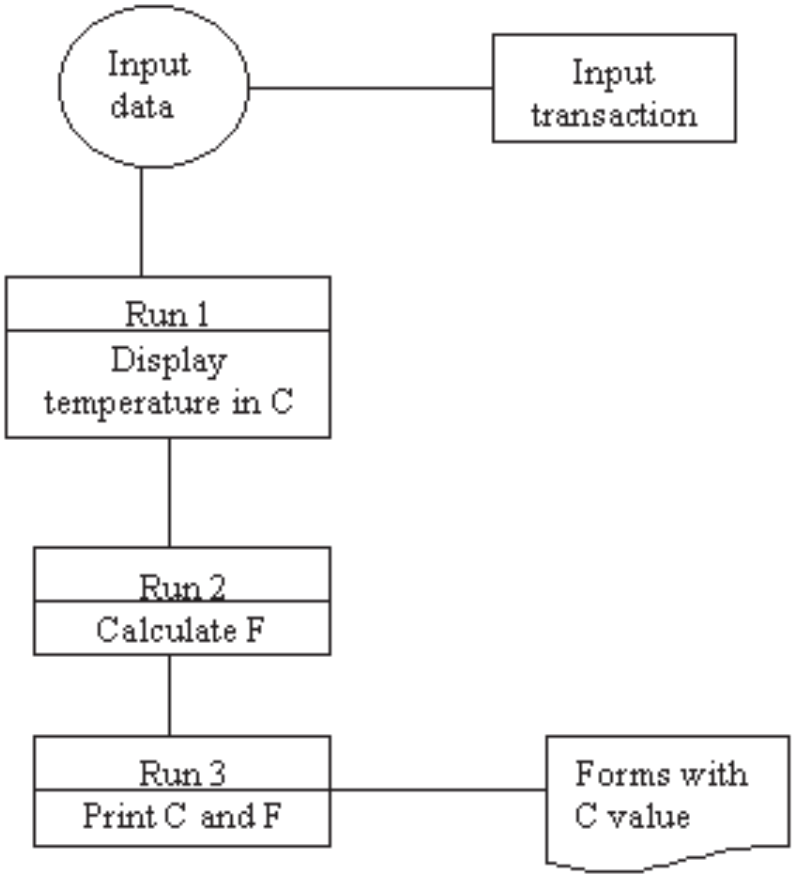


STUDY TEXT

Run Flowcharts

Run flowcharts are used to represent the logical relationship of computer routines along with inputs, master files transaction files and outputs.

The figure below illustrates a run flowchart.

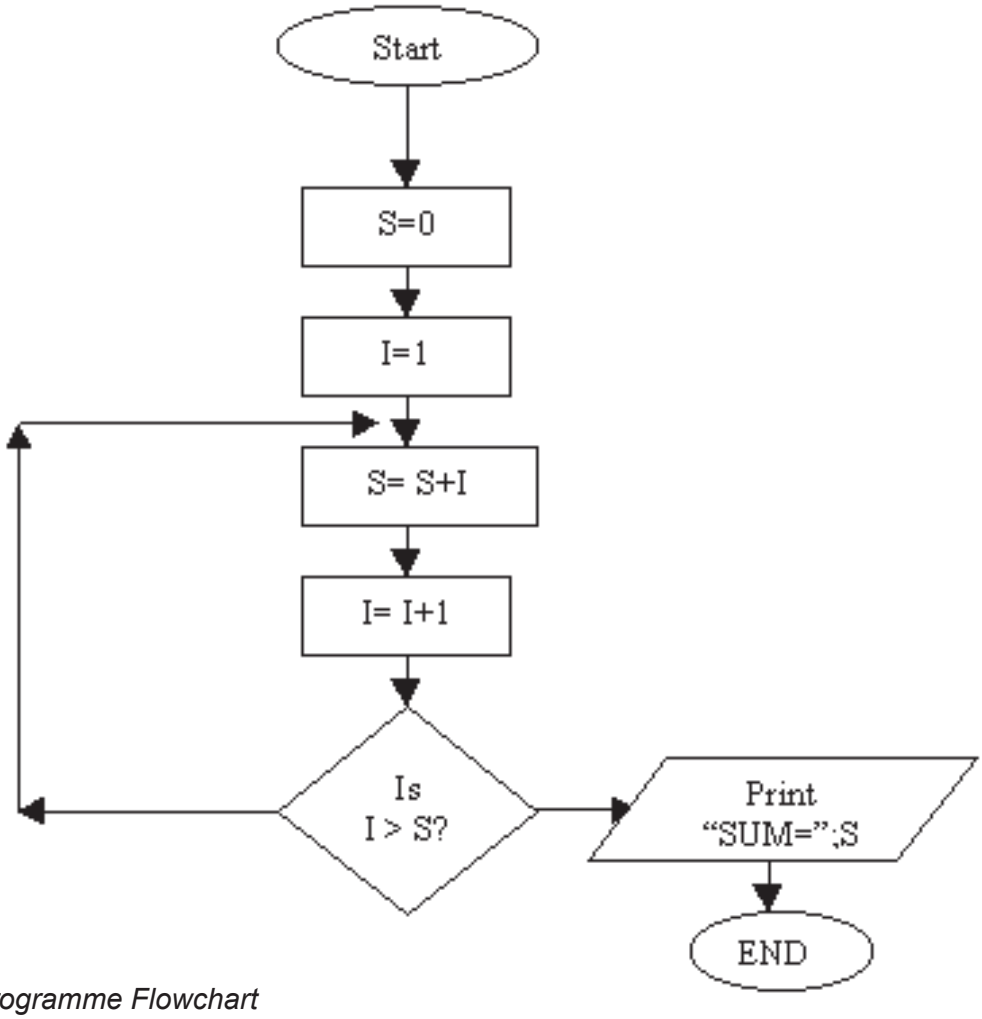


Run Flowchart

Programme Flowcharts

A programme flowchart represents, in detail, the various steps to be performed within the system for transforming the input into output. The various steps are logical/ arithmetic operations, algorithms, etc. It serves as the basis for discussions and communication between the system analysts and the programmers. Programme flowcharts are quite helpful to programmers in organising their programming efforts. These flowcharts constitute an important component of documentation for an application.

The figure represents a programme flowchart for finding the sum of first five natural numbers (i.e. 1,2,3,4,5).



Programme Flowchart

Advantages of using flowcharts

- Communication: Flowcharts are better ways of communicating the logic of a system to all concerned.
- Effective analysis: With the help of flowchart, problem can be analysed in more effective way.
- Proper documentation: Programme flowcharts serve as a good programme documentation, which is needed for various purposes
- Efficient coding: The flowcharts act as a guide or blueprint during the systems analysis and programme development phase.
- Proper debugging: The flowchart helps in the debugging process.
- Efficient program maintenance: The maintenance of operating programme becomes easy with the help of flowchart. It helps the programmer to put efforts more efficiently on that part.

Limitations of using flowcharts

- Complex logic: Sometimes, the programme logic is quite complicated. In that case, flowchart becomes complex and clumsy.
- Alterations and modifications: If alterations are required, the flowchart may require redrawing completely.

- The essentials of what is done can easily be lost in the technical details of how it is done.

(2) Data flow diagram

Data Flow Diagram (DFD) is a graphical representation of a system's data and how the processes transform the data. Unlike, flowcharts, DFDs do not give detailed descriptions of modules but graphically describe a system's data and how the data interact with the system.

Components of DFD

DFDs are constructed using four major components

- External entities
- Data stores
- Processes and
- Data flows

>> (i) External Entities

External entities represent the source of data as input to the system. They are also the destination of system data. External entities can be called data stores out side the system. These are represented by squares.

>> (ii) Data Stores

Data stores represent stores of data within the system. Examples: computer files or databases. An open-ended box represents a data/store – data at rest or a temporary repository of data.

>> (iii) Process

Process represents activities in which data is manipulated by being stored or retrieved or transferred in some way. In other words we can say that process transforms the input data into output data. Circles stand for a process that converts data into information.

>> (iv) Data Flows

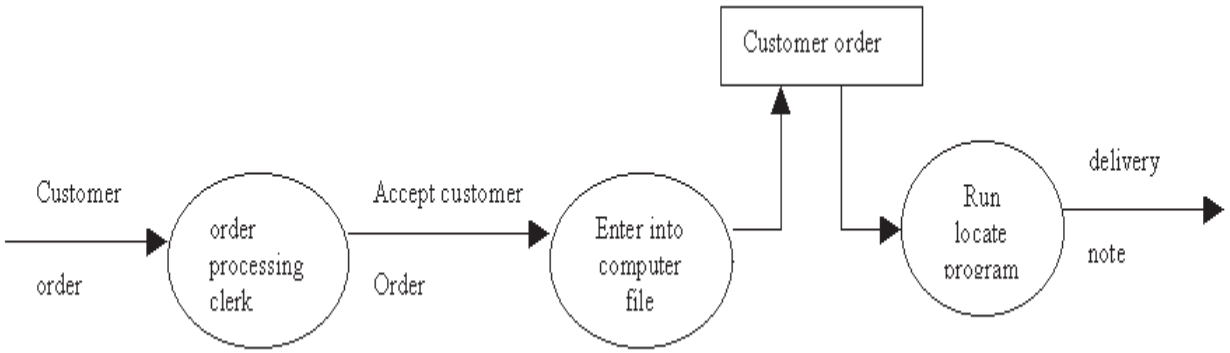
Data flow represents the movement of data from one component to the other. An arrow identifies data flow – data in motion. It is a pipeline through which information flows. Data flows are generally shown as one-way only. Data flows between external entities are shown as dotted lines.

Physical and Logical DFD

A **logical DFD** of any information system is one that models what occurs without showing how it occurs. An example is illustrated below.

It is clear from the figure that orders are placed, orders are received, the location of ordered parts is determined and delivery notes are dispatched along with the order. It does not however tell us how these things are done or who does them. Are they done by computers or manually and if manually who does them?

A **physical DFD** shows how the various functions are performed? Who does them? An example is illustrated below:



The figure is opposite to that of the logical DFD, it shows the actual devices that perform the functions. Thus there is an “order processing clerk”, an “entry into computer file” process and a “run locate program” process to locate the parts ordered. DFD(s) that shows how things happen, or the physical components are called physical DFD(s).

Typical processes that appear in physical DFDs are methods of data entry, specific data transfer or processing methods.

Difference between Flowcharts and DFD

The programme flowchart describes boxes that describe computations, decisions, interactions and loops. It is important to keep in mind that data flow diagrams are not programme flowcharts and should not include control elements. A good DFD should:

- Have no data flows that split up into a number of other data flows
- Have no crossing lines
- Not include flowchart loops of control elements
- Not include data flows that act as signals to activate processes.

(3) Decision Tables

This is a matrix representation of the logic of a decision. It specifies the possible conditions and the resulting actions. It is best used for complicated decision logic. It consists of the following parts:

- Condition stubs
  - Lists condition relevant to decision
- Action stubs
  - Actions that result from a given set of conditions
- Rules
  - Specify which actions are to be followed for a given set of conditions

An indifferent condition is a condition whose value does not affect which action is taken for two or more rules.

The **Condition stub** contains a list of all the necessary tests in a decision table. In the lower left-hand corner of the decision table we find the action stub where one may note all the processes desired in a given module. Thus Action Stub contains a list of all the processes involved in a decision table.

The upper right corner provides the space for the condition entry - all possible permutations of yes and no responses related to the condition stub. The yes and no possibilities are arranged as a vertical column called rules. Rules are numbered 1,2,3 and so on. We can determine the rules in a decision table by the formula:

Number of rules = 2^N = 2^N where N represents the number of condition and ^ means exponentiation. Thus a decision table with four conditions has 16=(2^4 =2 X 2 X 2 X 2 = 16) rules. One with six conditions has 64 rules and eight conditions yielding 256 rules.

The **Condition entry** contains a list of all the yes/no permutations in a decision table. The lower right corner holds the action entry. X's or dots indicate whether an action should occur as a consequence of the yes/no entries under condition entry. X's indicate action; dots indicate no action.

Thus Action entry indicates via dot or X whether something should happen in a decision table

The standard procedure for creating decision tables involves:

(i) Name the condition and each values each condition can assume
(ii) Name all possible actions that can occur
(iii) List all the rules
(iv) Define the actions for each rule
(v) Simplify the table

Example: Complete decision table for payroll system

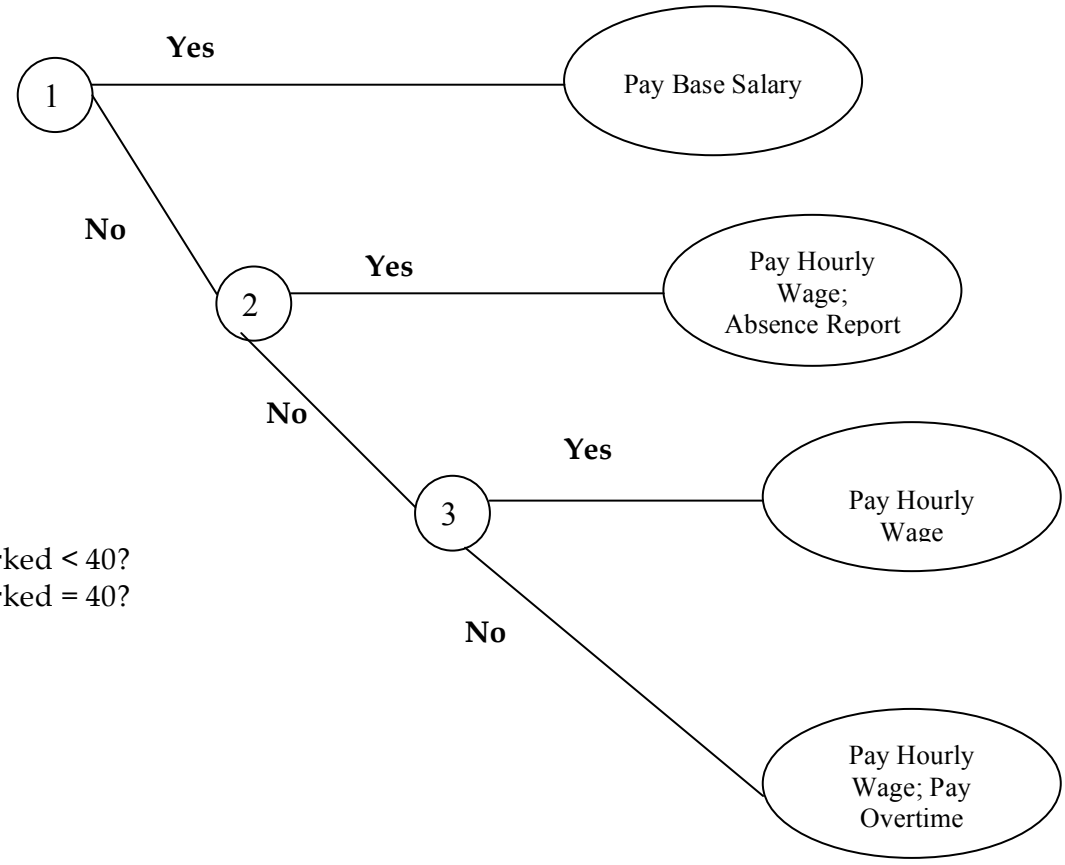
	Conditions / Courses of action	Rules					
		1	2	3	4	5	6
Condition Stubs	Employee Type	S	H	S	H	S	H
	Hours Worked	<40	<40	40	40	>40	>40
Action Stubs	Pay Basic Salary	X		X		X	
	Calculate Hourly wage		X		X		X
	Calculate Overtime						X
	Produce Absence Report		X				

(4) Decision Trees

This is a graphical representation of a decision situation. Decision situation points are connected together by arcs and terminate in ovals. The two main components are:

- Decision points represented by nodes
- Action represented by ovals

The decision tree defines the conditions as a sequence of left to right tests. A decision tree helps to show the paths that are possible in a design following an action or decision by the user. Decision tree turns a decision table into a diagram. This tool is read from left to right, decision results in a fork, and all branches end with an outcome. Each node corresponds to a numbered choice on the legend. All possible actions are listed on the far right.



Legend
1) Salaried?
2) Hours Worked < 40?
3) Hours Worked = 40?

(5)Structured English

This is a modified form of English used to specify the logic of information processes. It uses a subset of English.

- Action verbs
- Noun phrases
- No adjective or adverbs

There are no specific standards and is similar to programming languages.

- If conditions
- CASE statements

3.7 System implementation

This phase involves the following activities:

a) Hardware selection, acquisition and installation
b) User training
c) File conversion/creation
d) Changeover

Hardware and software acquisition

A user may acquire the hardware and software directly from a manufacturer and developer respectively. He may also purchase them from an intermediate supplier. Whichever way, carefully controlled purchasing procedures should be followed. The procedures should include invitation to tender and comparative analysis to determine the appropriate supplier of the required hardware and software.

Invitation to tender (ITT)

It is issued to a range of suppliers. ITT sets out specifications for the required equipment and software and should explore how the hardware will be used and the time scale for implementation. It sets the performance criteria required for the new system.

Contents of ITT

ITT includes background information about the companies together with an indication of the purpose of the system. This includes:

(i) The volume of data to be processed by the system. Complexity of the processing requirements and system interfaces should be stated.
(ii) The number of individuals who will want to access the computer system after installation and whether access needs to be instant or not
(iii) The speed of processing required or expected
(iv) Input and output desired
(v) The type of processing methods preferred
(vi) Estimated life of the system
(vii) Possible upgrades or expansion anticipated
(viii) Other general consideration include:

- Contact person in the company
- Overall financial constraints
- The form that submission is to take
- Closing date for submission of tender
- The address to which the tender is to be sent
- The reference person to which tender is to be addressed

While all the above features are necessary, it is important to decide on the financing methods.

These may include:

a) Purchasing – where the buyer acquires ownership of item after payment of an agreed amount
b) Leasing – involves formation of an agreement between lessee and lessor detailing the use of equipment, the length of time to use the equipment and the periodical payment
c) Renting – involves a single agreement where one party agrees to use another party's resources at certain periodical payments. The agreement is not as binding as that of a lease agreement.

Evaluation of a vendor proposal

(1) Benchmark tests – tests how long it takes for a machine to run through a particular set of programmes. It is carried out to compare performance of software/hardware against present criteria such as performance speed, response times and user friendliness of the equipment.

(2) Simulation tests – it uses synthetic programme written specifically for testing purposes. They are programs incorporated with routines designed to test a variety of situations. Other features or factors include:

i. Supplier's reliability – both financial stability and track record
ii. Cost – equipment cost, installation cost and training costs
iii. Utility software supported and preloaded in the hardware
iv. The warrant period, units and maintenance commitments
v. Software support upgrades and maintenance
vi. Training requirements, which includes timings, number of personnel, etc

Choosing hardware and software

Software factors

Factors influencing choice of software include:

(i) User requirements: the selected software or package should fit user requirement as closely as possible.
(ii) Processing time: these involves the response time e.g. if the response time is slow, the user might consider the software or package as unsuccessful
(iii) Documentation: the software should be accompanied by a manual, which is easy to understand by non-technical person. The manual should not contain technical jargon.
(iv) User friendliness: the package should be easier to use with clear on screen prompts, menu driven and extensive on screen help facility.
(v) Controls: the software should have in-built controls, which may include password options, validation checks, audit trails or trace facilities, etc.
(vi) Up-to-date: the software should be up-to-date e.g. should have changes or corrections in line with business procedures.
(vii) Modification: one should consider whether the user could freely change the software without violating copyright.
(viii) Success in the market: one should consider how many users are using the software and how long it has been in the market.

(ix) Compatibility of the software: how the software integrates with other software particularly the operating system and the user programmes.
(x) Portability: one should consider how the software runs on the user computer and whether there will be need for the user to upgrade his hardware
(xi) Cost: the user company should consider its financial position to establish whether it can afford the software required for efficient operations rather than the least cost package software available.

>>> *Software contracts*

Software contracts include the costs, purpose and capacity of the software. The following are covered in software contracts:

- Warrant terms
- Support available
- Arrangement for upgrades
- Maintenance arrangements
- Delivery period/time especially for written software
- Performance criteria
- Ownership

>>> *Software licensing*

Software licensing covers the following:

- Number of users that can install and use the software legally
- Whether the software can be copied without infringing copyrights
- Whether it can be altered without the developers consent
- Circumstances under which the licensing can be terminated
- Limitation of liability e.g. if the user commits fraud using the software
- Obligation to correct errors or bugs if they exist in the software

Hardware factors

Custom-built hardware is a rare necessity. Most hardware is standard, compatible, off-the-shelf components. It is cheaper, easy to maintain, and ensures compatibility with equipment in your organization and your partners and clients.

The system analysis and design should have precisely determined what sort of hardware is needed - down to the make and model.

The decision of hardware choice must consider many factors:

- Future needs - can the equipment be expanded or added to?
- Availability (is it only available overseas?)
- Capacity (e.g. is the hard disk big enough to hold all your data? Is it fast enough?)
- Reliability - can it be depended on?
- Cost - initial cost, running costs, upgrade costs, repair costs, training costs
- Compatibility - with your other equipment, and that of your partners and clients
- Warranty and support - in case of failure or problems
- Ease of use and installation
- Compliance with local conditions (e.g. power supplies must be 240V or compliant with telecommunication systems)

>>> *Choosing a supplier*

After choosing the hardware equipment and the equipment makers (manufacturers), one must choose a *supplier* or reseller (in other words, once you know what you want to buy, what shop will you choose?)

Factors to consider:

- Reputation for support (e.g. phone support, onsite visits, website help)
- Reputation for reliability, honesty, permanence (very important!)
- Knowledge of the equipment
- Geographic location - can you get to them easily if you need to?
- Ability to offer onsite support or repair
- Prices – cheap, affordable

>>> *Installation*

Software and hardware installation is done by supplier's technicians or the user organisation appointed person to avoid the risks associated with improper installation of the equipment. The system analyst and other development team members may be called to assist where appropriate.

User training

It is important that the system users be trained to familiarise themselves with the hardware and the system before the actual changeover.

The aims of user training are:

a) To reduce errors arising from learning through trial and error
b) To make the system more acceptable to the users
c) To improve security by reducing accidental destruction of data
d) To improve quality of operation and services to the users
e) To reduce the cost of maintenance by minimising accidental destruction of data or hardware
f) To ensure efficiency in system operation when it goes live

The people to be trained include system operators, senior managers, middle managers and all those affected by the system directly or indirectly. Training should cover current staff and recruited personnel.

>>> *Timing of users' training*

- Before the feasibility study when the users are given a general explanation of computer systems, their relevance in function application and reason for desire to introduce a computer in the specific functions
- Before investigation where users are explained about the impact of the new system and importance of their involvement in development. This may help gain user confidence and facilitate their acceptance of the system
- During fact finding so that they can cooperate and provide useful information to guide the system developer during the analysis stage of SDLC
- Before programming so that they can prepare themselves for specific roles at implementation stage. These may include testing activities or roles.

- Before implementation to enable the users to cooperate and play their roles as assigned to them
- After implementation in order to assist in evaluation of system performance

File conversion

This involves changing of existing form of files into a form suitable for the new system when it becomes operational. It may require that the analyst create the file from scratch if no computer-based files exist. In an event that computer-based files exist, they should be converted to a form relevant or sensible to the new system.

File conversion procedures

(i) Record manually the existing data i.e. the old master files
(ii) Transfer the recorded data to special form required by the new system
(iii) Insert any new data into the file i.e. update the file already in the new form (form should include data contents and their corresponding formats and layouts)
(iv) Transcribe the completed form into a medium or storage relevant for the new system
(v) Validate the file contents to ensure that they are free of error before they can be used in the new system

Problems associated with file creation or file conversion are:

- Records may be stored or located at different places or locations, thus may be difficult to gather them all
- Some records may require updating which may slow down the change over plan
- Records may be too numerous i.e. too large in volume which may slow down the change over plan since transcription will take long
- Some records may not exist at all e.g. a customer who makes an order through a phone call

File conversion methods include:

- Straight file conversion/creation
- Dummy file conversion/creation
- Phased file conversion/creation

Straight file conversion

This method requires that the new system files be created moments before the planned change over. It is important to note that it is only suitable for small size files. Otherwise, it may delay the system implementation plan. The actual data or real data would be used instead of dummy data. This implies that once created, files are already in the form suitable for the new system.

Dummy file conversion

It requires that files be created long before the planned changeover. Dummy records are used, which are replaced with the actual records immediately before change over. The method is ideal when dealing with large volumes of transaction files or master files. It enables file creation activities to be spread over a long period of time.

Phased file conversion

It requires that the files be converted on a bit-by-bit phases. This implies that instead of changing, for example, a whole department file, the file is changed on a section-by-section basis. It may suitably be applicable on a phased change over method.

System change-over

Involves changing or switching from existing system to the new developed system. The following methods may be used:

(i) Direct change-over
(ii) Parallel change-over
(iii) Phased change-over
(iv) Pilot change-over

>>> Direct change-over

The old system ceases its operation and the new system commences operation the next day. The old system is made redundant in all its aspects. The method is applicable in the following circumstances:

- When the new system is small and simple
- When both the new and old system are substantially different
- When extra staff to oversee or undertake parallel running of both systems are unavailable
- When the management has complete confidence that the new system will work

The advantages of a direct change-over are:

- Relatively cheap
- Prevents the weaknesses of the old system from being passed over to the new system
- Reduces system implementation duration

Its disadvantages are:

- It is very risky especially if the new system fails. The cost of switching back to the old system will be high
- If not properly planned, it may interrupt user organisation operations and bring confusion amongst staff members

>>> Parallel change-over

This is a method where new and old systems are allowed to run side by side or simultaneously until it is proved beyond reasonable doubt that the new system is working and all the benefits are realised. It is suitable when the new system is sophisticated and a very careful changeover is required or when the development team has little confidence in the new system and where there are more staff to cope with the operations of both systems running in parallel.

Its advantages are:

- Users become familiar with the new system prior to the actual changeover which may enhance their efficiency

- The organisation is exposed to less risks in case the new system fails
- There would be less interruption and inconveniences in the organisation's operations during the change-over period.

The disadvantages of this method are:

- It is an expensive method.
- It might delay system implementation schedule or period.

>>> Phased change-over

The method involves implementation of a system on a step-by-step approach. This implies that only a portion of the system is implemented initially. Other portions are implemented in phases. For example, if it has modules for finance, production and human resource management, then the finance module is implemented first, then the production and lastly the human resource management module.

>>> Pilot change-over

It involves installation of new system but using it only in one part of the organisation on an experimental basis. e.g. a bank wishing to computerise its operations may install a computerised system on one branch on an experimental basis. When the system is proved to be successful, it is transferred to another, branch and after some time to another etc until the entire bank is computerised. Any refinement that ought to be done on the system should be done before it is installed in the next branch.

NB: The whole system is implemented on a section of the organisation.

Both phased and pilot changeover methods have the following advantages and disadvantages.

Advantages are:

- Allow a new system to be implemented quickly with minimum costs
- Allow training of personnel on the new system during implementation
- They cause minimum interruption to company operations during system's implementation
- The peak demands are lighter on the end user and the operational environment
- They are less costly
- The risks associated with errors and system failure are minimised

The disadvantages include:

- Interfacing both the old and new system may usually bring problems
- There may be additional costs associated with running both systems at the same time

The change over plan should include the following:

(i) Time limit for the parallel run
(ii) Instructions on error handling procedures
(iii) Instruction on how to cope with major problems in the new system

3.8 Post implementation review

It is an important activity, which, like training and testing, is continuous. It involves measuring or assessment of system development stages and the final produced system. It may be carried out from the third to seventh month after changeover. The development team members, users, auditors, management representative and those affected by the system may take part in the exercise. This is to ensure that specified objectives are met and are justifiable in terms of cost, benefits and other performance criteria.

The review focuses on the following areas:

a) Comparison of the actual system performance against the anticipated performance objectives. This involves assessment of system running cost, benefits, etc as they compare with estimated or anticipated.
b) The staffing needs and whether they are more or less than anticipated costs.
c) Any delays in the processing and effects of such delays.
d) Effectiveness of the inbuilt security procedures in the system.
e) The error rates for input data.
f) The output i.e. whether it is correct, timely and distributed correctly to the relevant users.

Evaluation of a system should be carried out after completion of every stage of SDLC. There are three types of evaluation.

Formative (feedback) evaluation

It produces information that is fed back into the development cycle to improve the product under development. It serves the needs of those who are involved in the development process.

Summative evaluation

It is done after the system development project is completed. It provides information about efficiency of the product to the decision makers who adopt it.

Documentation evaluation

It is performed just before and after hardware and software installation and also after system change-over. It is carried out to assess general functionality of a system after settling down.

The benefits of a post-implementation review are:

- It improves system development practices and decisions to adopt, modify or discard an information system
- Ensures compliance with user objectives
- Enhances evaluation and training of personnel responsible for system development
- Improves effectiveness and productivity of subsequent system design
- Ensures realisation of cost saving operations by modifying the system

The aspects to be evaluated include:

- Systems output accuracy i.e. information produced by the system
- User satisfaction with information system
- The attitude towards the system by those directly affected by the system
- Effective systems of internal control
- Project schedule compliance

Other aspects/factors may include:

- The impact of the system on the organisation structure.
- The quality of programme produced.
- The operational cost of the system.
- The savings made as a result of the system.
- The impact of the system on users and their job.
- Quality and completeness of the system documentation.

The reasons why post implementation evaluation is carried out are:

- To verify that the installed system meets user requirements.
- To provide a feedback to the development personnel.
- To justify adoption, continuation or termination of installed system.
- To clarify and set priorities for any needed modification on the system.
- To transfer responsibility of the system from the development team to the users.

NB: System post-implementation review team writes a report that indicates specific areas within the system that need improvement. This report is called post-implementation review report. It acts as a reference document during system maintenance.

3.9 System maintenance

It involves changing part of the system according to the recommendations of the post-implementation review team.

Causes of system maintenance include:

- Defects in the system after its delivery. This involves any errors or bugs in the newly implemented system e.g. use of wrong formula within a system.
- Environment change e.g. a government tax policy may change, which would influence a change of payroll system.
- A change in user requirement. A business organisation exists in a changing environment, therefore the user requirements change e.g. a payslip in a payroll system may initially be required to show the employee corporate share amount. Employees may feel that such information should not appear in the payslips and thus influence a change of the system.
- Poor documentation of the system. It makes it difficult for one to understand the system, and also to change it should there be a need to do so. A system may be changed and its documentation rewritten in order to improve it is maintainability.

System maintenance is carried to improve the system adaptability and flexibility. Flexibility involves minor changes in a system in order to cope up with the growth in business transaction volume. Adaptability involves changing a system in order to benefit the user from advances in both software and hardware technology.

The process of the system maintenance should be controlled by the system analyst.

When a manager or a user suggests a change to the system regardless of the reasons:

a) The analyst should prepare diagrams and estimate the impact
b) The change control board decides whether or not to implement the change.
c) If change would take place, the analyst modifies all the documentation by merging the diagram and estimates into the existing problem and designs specification.
d) The programmers and testing teams are responsible for incorporating any change into the programs. They test the system to ensure that no errors or problems are introduced as a result of the change.
e) Once the change is satisfied as default free, the revised system is adopted immediately.

Types of system maintenance

a) Corrective maintenance
b) Perfective maintenance
c) Adaptive maintenance
d) Preventive maintenance
e) Replacive maintenance

>> a) Corrective maintenance

It is usually a change effected in a system in response to a detected problem or error. Its objective is to ensure that the system remains functional. It basically involves removal of errors on the already newly developed system.

>> b) Perfective maintenance

It is a change to perfect a system i.e. improve its performance in terms of response time to user request or to amend a system interface to make a system more user friendly.

>> c) Adaptive maintenance

Involves changing a system to take account of a change in its functional environment.

>> d) Preventive maintenance

Carried out on a system to ensure that it can withstand stress. It helps in ensuring data and software integrity.

>> e) Replacive maintenance

It is carried out on a system when a system becomes almost unmaintainable e.g. due to lack of documentation, poor design or age.

4. Alternative development methodologies

4.1 Data-Oriented System Development

Data-oriented system development (DOSD) focuses on and recognises the need for management and staff to have access to data to facilitate and support decisions. Users need and want data so they can derive information from it. Inherent in DOSD systems is the development of an accessible database of information that will provide the basis for *ad hoc* reporting.

The emphasis on data is not to be interpreted as the disappearance of operation-level transaction processing systems, rather it is recognition that most transaction systems have already been developed and that new systems are now addressing the users' need for more information.

4.2 Object-Oriented Technology

Object-oriented technology views the raw data and the procedures governing use of data as a single object. An object-oriented approach to data management defines the object in terms of its characteristics (for example, text, graphics, format specifications and printer information) and the procedures governing their use (how those characteristics are used to make a complete document).

The object is then stored as a resource that can be reused or modified.

The major advantages of an object-oriented approach to data management systems are:

a) Ability to manage an unrestricted variety of data types.
b) Provides a means to model complex relationships.
c) Capacity to meet the demands of a changing environment.
d) The user can manipulate object-oriented models easily.
e) Increased efficiency in programming through the ability to re-use elements of logic.
f) Ability to allow a user or an application to access only the needed information, since it stores objects independently of one another.

4.3 Prototyping

Prototyping, also known as heuristic development, is the process of creating a system through controlled trial and error. It is a method, primarily using faster development tools such as 4GLs that allows a user to see a high level view of the workings of the proposed system within a short period of time.

The initial emphasis during development of the prototype is usually placed on the reports and screens, which are the system aspects most used by the end users. This allows the end users to see a working model of the proposed system within a short time.

There are two basic methods or approaches to prototyping:

i. Build the model to create the design. Then, based on that model, develop the system with all the processing capabilities needed.
ii. Gradually build the actual system that will operate in production using a 4GL that has been determined to be appropriate for the system being built.

The problem with the first approach is that there can be considerable pressure to implement an early prototype. Often, users observing a working model cannot understand why the early prototype has to be refined further. The fact that the prototype has to be expanded to handle transaction volumes, terminal networks, backup and recovery procedures, as well as provide for auditability and control is not often understood.

Another disadvantage of prototyping is that it often leads to functions or extras being added to the system that are not included in the initial requirements document. All major enhancements beyond the initial requirements document should be reviewed to ensure that they meet the strategic needs of the organisation and are cost effective. Otherwise, the final system can end up being functionally rich but inefficient.

A potential risk with prototyped systems is that the finished system will have poor controls. By focusing mainly on what the user wants and what the user uses, system developers may miss some of the controls that come out of the traditional system development approach, such as: backup/recovery, security and audit trails.

Change control often becomes much more complicated with prototyped systems. Changes in designs and requirements happen so quickly that they are seldom documented or approved and can escalate to a point of being unmaintainable.

However, this method of system development can provide an organisation with significant time and cost savings.

4.4 Rapid Application Development (RAD)

RAD is a methodology that enables organisations to develop strategically important systems faster while reducing development costs and maintaining quality. This is achieved by using a series of proven application development techniques, within a well-defined methodology. These techniques include the use of:

- Small, well trained development teams
- Evolutionary prototypes
- Integrated power tools that support modelling, prototyping and component re-usability.
- A central repository
- Interactive requirements and design workshops.
- Rigid limits on development time frames.

RAD supports the analysis, design, development and implementation of individual application systems. However, RAD does not support the planning or analysis required to define the information needs of the enterprise as a whole or of a major business area of the enterprise. RAD provides a means for developing systems faster while reducing cost and increasing quality. This is done by: automating large portions of the system development life cycle, imposing rigid limits on development time frames and re-using existing components.

The RAD methodology has four major stages:

i. The concept definition stage defines the business functions and data subject areas that the system will support and determines the system scope.
ii. The functional design stage uses workshops to model the system's data and processes and to build a working prototype of critical system components.
iii. The development stage completes the construction of the physical database and application system, builds the conversion system and develops user aids and deployment work plans.
iv. The deployment stage includes final user testing and training, data conversion and the implementation of the application system.

4.5 Joint Application Design (JAD)

A structured process in which users, managers and analysts work together for several days in a series of intensive meetings to specify or review system requirements. Aims to develop a shared understanding of what the information system is supposed to do.

4.6 End-user development

End-user development refers to the development of information systems by end users with minimal or no assistance from professional systems analysts or programmers. This is accomplished through sophisticated "user-friendly" software tools and gives end-users direct control over their own computing.

Advantages:

- Improved requirements determination.
- Large productivity gains have been realised when developing certain types of applications.
- Enables end users to take a more active role in the systems development process.
- Many can be used for prototyping.
- Some have new functions such as graphics, modeling, and *ad hoc* information retrieval.

Disadvantages:

- It is not suited to large transaction-oriented applications or applications with complex updating requirements.
- Standards for testing and quality assurance may not be applied.
- Proliferation of uncontrolled data and "private" information systems.

End-user development is suited to solving some of the backlog problems because the end-users can develop their needed applications themselves. It is suited to developing low-transaction systems. End-user development is valuable for creating systems that access data for such purposes as analysis (including the use of graphics in that analysis) and reporting. It can also be used for developing simple data-entry applications.

4.7 Computer Aided Software Engineering (CASE)

This is the automation of the steps and methodologies for systems analysis and development. It reduces the repetitive work that developers do. Usually it has graphical tools for producing charts and diagrams. It may have any of the following tools: screen and report generators, data dictionaries, reporting facilities, code generators, and documentation generators. These tools can greatly increase the productivity of the systems analyst or designer by:

- Enforcing a standard.
- Improving communication between users and technical specialists.
- Organising and correlating design components and providing rapid access to them via a design repository or library.
- Automating the tedious and error-prone portions of analysis and design.
- Automating testing and version control.

5. Application Packages

An application software package is a set of prewritten, pre-coded application software programmes that is commercially available for sale or lease. Packages range from very simple programs to very large and complex systems encompassing hundreds of programmes. Packages are normally used for one of the following three reasons:

- Where functions are common to many companies. For example, payroll systems typically perform the same functions for most companies.
- Where data processing resources for in-house development are in short supply.
- When desktop microcomputer applications are being developed for end users. This approach is often followed because so many application packages have been developed for microcomputers.

Advantages of packages are:

- Design: The vendor has already established most of the design which may easily consume up to 50 percent of development time.
- Testing: Programmes are pre-tested, cutting down testing time and technical problems.
- Installation: The vendor often installs or assists in the installation of the package.
- Maintenance and support: Periodic enhancement or updates are supplied by the vendor. Vendors also maintain a permanent support staff well versed in the package, reducing the need for individual organisations to maintain such expertise in-house.
- Documentation: The vendor supplies documentation.

Disadvantages of packages:

- There are high conversion costs for systems that are sophisticated and already automated.
- Packages may require extensive customization or reprogramming if they can't easily meet unique requirements. This can inflate development costs.

- A system may not be able to perform many functions well in one package alone. For example, a human resources system may have a good compensation module but very little capacity for manpower planning or benefits administration.
- Impact if the vendor no longer supports/supplies the package. In case the vendor no longer supports or supplies the package, a firm maybe negatively affected, e.g. need to invest in other packages which maybe costly.

6. Software reengineering

Is a methodology that addresses the problem of aging or legacy software. It seeks to upgrade such software that works by extracting the logic of the system, thereby creating a new system without starting from scratch. The techniques involved are:

- Reverse engineering.
- Revision of design and programme specifications.
- Forward engineering.

7. Reverse engineering

Extracts the business specifications from older software. Reverse engineering tools analyse the existing programme code, file, and database descriptions to produce a structured specification of the system. This specification can be combined with new specifications to provide the basis of the new system.

SUMMARY

Projects have the following characteristics:

a) Unique purpose – a project is undertaken to fulfil a specific objective
b) Temporary – projects exist for a limited duration of time; often not perpetual
c) Requires resources – such as money, manpower and machine resources
d) Should have a primary sponsor – usually an organisation, a department or individual.
e) Involves uncertainty – a great deal of the project implementation is unknown therefore need for proper planning and management

Some of the factors influencing choice of software include:

(i) User requirements: the selected software or package should fit user requirement as closely as possible
(ii) Processing time: these involves the response time e.g. if the response time is slow the user might consider the software or package as unsuccessful
(iii) Documentation: the software should be accompanied by a manual, which is easy to understand by non-technical person. The manual should not contain technical jargon.
(iv) User friendliness: the package should be easier to use with clear on screen
(v) Portability: one should consider how the software runs on the user computer and

whether there will be need for the user to upgrade his hardware

(vi) Cost: the user company should consider its financial position to establish whether it can afford the software required for efficient operations rather than the least cost package software available.

The RAD methodology has four major stages:

i. The concept definition stage defines the business functions and data subject areas that the system will support and determines the system scope.
ii. The functional design stage uses workshops to model the system's data and processes and to build a working prototype of critical system components.
iii. The development stage completes the construction of the physical database and application system, builds the conversion system and develops user aids and deployment work plans.
iv. The deployment stage includes final user testing and training, data conversion and the implementation of the application system.

Packages are normally used for one of the following three reasons:

- Where functions are common to many companies. For example, payroll systems typically perform the same functions for most companies.
- Where data processing resources for in-house development are in short supply.
- When desktop microcomputer applications are being developed for end users. This approach is often followed because so many application packages have been developed for microcomputers.

PAST PAPER ANALYSIS

6/00, 12/00, 6/01, 12/01, 6/02, 12/02, 6/03, 12/03, 6/04, 12/04, 6/05, 12/05, 6/06, 12/06, 6/07, 12/07

CHAPTER QUIZ

1. ..... involves changing of existing form of files into a form suitable for the new system when it becomes operational.
2. ..... technology views the raw data and the procedures governing use of data as a single object.
3. *.....*The method involves implementation of a system on step-by-step approach.
4. Prototyping, also known as heuristic development
   a. True
   b. False
5. Parallel system change-over is where the old system ceases its operation and the new system commences operation the next day.
   a. True
   b. False

ANSWERS TO CHAPTER QUIZ

1. File conversion
2. Object oriented
3. Phased changeover
4. a. True
5. b. False – it's a direct changeover

EXAM QUESTIONS

1. A system project is regarded as having economic feasibility when its benefits exceed its costs. List and briefly describe the types of benefit and types of cost which may accrue from computerising a typical commercial application.

2. The economic evaluation of computer-based information systems depends on the selective application of investment appraisal techniques. Briefly describe THREE such techniques which are commonly applied and discuss their advantage and disadvantages.

3. In practice the project manager needs to manage simultaneously the elements of time, resources, cost and quality. These elements not only interact with each other but are continuously changing.

   (a). Briefly explain the role of each of these elements in the project management processes.

   (b). Give examples of the type of judgments and decisions which the project manager may be required to make.

4. There are a number of organisational structures which are used to perform management activities at different levels. List FOUR major components of these structures, and discuss their primary roles and responsibilities.

   Critical Path Analysis (CPA) is one of the main techniques applied in the planning and control of information systems projects. List and briefly explain the stages involved in the CPA approach.

CHAPTER FOUR

INFORMATION SYSTEMS IN AN ENTERPRISE

CHAPTER FOUR

INFORMATION SYSTEMS IN AN ENTERPRISE

▶ OBJECTIVES

When you have completed this chapter, you should be able to:

1. Describe the functions of an information system.
2. Describe the types of information systems.
3. Evaluate effectiveness of information systems.
4. Relate one system to another.

▶ INTRODUCTION

An information system is a set of interrelated components that collect, manipulate, process and transform data into information and provide feedback to meet a specified objective. A computer based information system is one that uses computer technology to perform input, processing and output activities. Due to the massive computerisation of manual information systems, computer based information systems are simply referred to as information systems. They are the subject of discussion in this chapter.

Common examples of information systems include: Automated Teller Machines (ATMs), Point of Sale (POS) terminals used by supermarket checkout clerks, airline reservation systems or flight schedule systems used by airlines, student registration systems used by colleges, etc.

▶ DEFINITION OF KEY TERMS

Computer Hardware – Refers to physical computer equipment and devices.

Computer Software – Refers to the instructions that direct the operation of the computer hardware.

Electronic Funds Transfer (EFT) - is the exchange of money via telecommunications without currency actually changing hands.

Databases – Contains all data utilised by application software.

▶ EXAM CONTEXT

Questions from this chapter are mostly application questions. The examiners would test students'

understanding of Information Systems in relation to commercial firms. Clear relation of the types of information systems outlined in this chapter to commercial firms is important. The student will be required to have an open mind as well as a wide general knowledge on information systems to comfortably attempt such questions.

▶ INDUSTRY CONTEXT

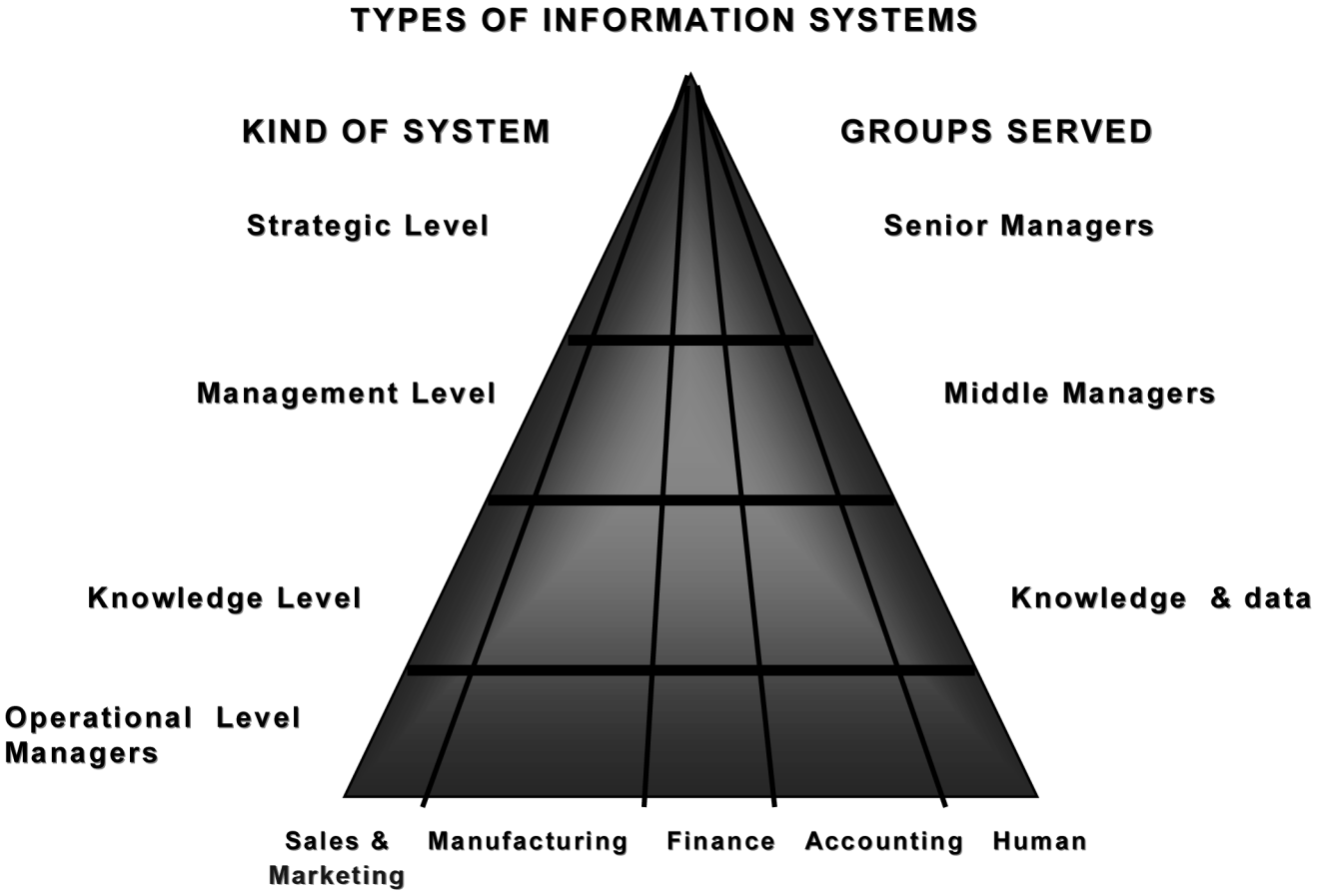
In a general sense, the term Information System (IS) refers to a system of people, data records and activities that process the data and information in an organisation, and it includes the organisation's manual and automated processes. In a narrow sense, the term information system (or computer-based information system) refers to the specific application software that is used to store data records in a computer system and automates some of the information-processing activities of the organisation. Computer-based information systems are in the field of information technology. The discipline of business process modelling describes the business processes supported by information systems.

Fast Forward: The individuals and organisations best equipped to respond to the challenge of rapidly changing technologies are those with the vision to ensure that their skills and knowledge are kept current and set in a broad educational context.

2. Management structure and use of information

Information systems support different types of decisions at different levels of the organisational hierarchy. While operational managers mostly make structured decisions, senior managers deal with unstructured decisions while middle managers are often faced with semi-structured decisions.

For each functional area in the organisation, four levels of organisational hierarchy can be identified: the operational level, knowledge level, management level and strategic level. Different types of information systems serve each of these levels.



3. Components of an information system

Components of an information system include:

- People – These use the system to fulfil their informational needs. They include end users and operations personnel such as computer operators, systems analysts, programmers, information systems management and data administrators.

- Computer Hardware – Refers to physical computer equipment and devices, which provide for five major functions.
  - Input or data entry
  - Output
  - Secondary storage for data and programmes
  - Central processor (computation, control)
  - Communication

- Computer Software – Refers to the instructions that direct the operation of the computer

hardware. It is classified into system and application software.

- Telecommunication System/Communication network
- Databases – Contains all data utilised by application software. An individual set of stored data is referred to as a file. Physical storage media evidences the physical existence of stored data, that is: tapes, disk packs, cartridges and diskettes.
- Procedures – Formal operating procedures are components because they exist in physical forms as manuals or instruction booklets. Three major types of procedures are required.
  - User instructions – for application users to record data, to use a terminal for data entry or retrieval, or use the result.
  - Instructions for preparation of input by data preparation personnel.
  - Operating instructions for computer operations personnel.

4. Functions of an information system

The functions of an information system can be generally classified into those functions involved in:

- Transaction processing
- Management reporting
- Decision support

4.1 Transaction processing

Major processing functions include:

i. Process transactions – Activities such as making a purchase or a sale or manufacturing a product. It may be internal to the organisation or involve an external entity. Performance of a transaction requires records to:
   - Direct a transaction to take place
   - Report, confirm or explain its performance
   - Convey it to those needing a record for background information or reference.

ii. Maintain master files – Many processing activities require operation and maintenance of a master file, which stores relatively permanent or historical data about organisational entities. E.g. processing an employee paycheck needs data items such as rate of pay, deductions etc. Transactions when processed update data items in the master file to reflect the most current information.

iii. Produce reports –are significant products of an information system. Scheduled reports are produced on a regular basis. An information system should also be able to produce special reports quickly based on *ad hoc* or random requests.

iv. Process inquiries – Other outputs of the information system are responses to inquiries using the databases. These may be regular or *ad hoc* inquiries. Essentially inquiry processing should make any record or item in the database easily accessible to authorised personnel.

v. Process interactive support applications – The information system contains applications

to support systems for planning, analysis and decision making. The mode of operation is interactive, with the user responding to questions, requesting for data and receiving results immediately in order to alter inputs until a solution or satisfactory result is achieved.

1. Management reporting

This is the function involved in producing outputs for users. These outputs are mainly as reports to management for planning, control and monitoring purposes. Major outputs of an information system include:

i. Transaction documents or screens
ii. Preplanned reports
iii. Preplanned inquiry responses
iv. "Ad hoc" reports and "ad hoc" inquiry responses
v. User-machine dialog results

2. Decision support

Types of decisions

>> a) Structured/programmable decisions

These decisions tend to be repetitive and well defined e.g. inventory replenishment decisions. A standardised pre-planned or pre-specified approach is used to make the decision and a specific methodology is applied routinely. Also the type of information needed to make the decision is known precisely. They are programmable in the sense that unambiguous rules or procedures can be specified in advance. These may be a set of steps, flowchart, decision table or formula on how to make the decision. The decision procedure specifies information to be obtained before the decision rules are applied. They can be handled by low-level personnel and may be completely automated.

It is easy to provide information systems support for these types of decisions. Many structured decisions can be made by the system itself e.g. rejecting a customer order if the customer's credit with the company is less than the total payment for the order. Yet managers must be able to override these systems' decisions because managers have information that the system doesn't have e.g. the customer order is not rejected because alternative payment arrangements have been made with the customer.

In other cases the system may make only part of the decision required for a particular activity e.g. it may determine the quantities of each inventory item to be reordered, but the manager may select the most appropriate vendor for the item on the basis of delivery lead time, quality and price.

Examples of such decisions include: inventory reorder formulas and rules for granting credit. Information systems requirements include:

- Clear and unambiguous procedures for data input
- Validation procedures to ensure correct and complete input
- Processing input using decision logic
- Presentation of output so as to facilitate action

STUDY TEXT

>> b) Semi-structured/semi-programmable decisions

The information requirements and the methodology to be applied are often known, but some aspects of the decision still rely on the manager; e.g. selecting the location to build a new warehouse. Here the information requirements for the decision such as land cost, shipping costs are known, but aspects such as local labour attitudes or natural hazards still have to be judged and evaluated by the manager.

>> c) Unstructured/non-programmable decisions

These decisions tend to be unique e.g. policy formulation for the allocation of resources. The information needed for decision-making is unpredictable and no fixed methodology exists. Multiple alternatives are involved and the decision variables as well as their relationships are too many and/or too complex to fully specify. Therefore, the manager's experience and intuition play a large part in making the decision.

In addition, there are no pre-established decision procedures either because:

- The decision is too infrequent to justify organisational preparation cost of procedure, or
- The decision process is not understood well enough, or
- The decision process is too dynamic to allow a stable pre-established decision procedure.

Information system requirements for support of such decisions are:

- Access to data and various analyses and decision procedures.
- Data retrieval must allow for *ad hoc* retrieval requests
- Interactive decision support systems with generalised inquiry and analysis capabilities.

Example: Selecting a Chief Executive Officer of a company.

STUDY TEXT

5. Types of information systems: characteristics and differences

Major types of systems include:

1. Transaction Processing Systems (TPS)
2. Management Information Systems (MIS)
3. Decision Support Systems (DSS)
4. Executive Support Systems (ESS)
5. Expert Systems

5.1 Transaction Processing System (TPS)

A transaction is any business related exchange, such as a sale to a client or a payment to a vendor. Transaction processing systems process and record transactions as well as update records. They automate the handling of data about business activities and transactions. They record daily routine transactions such as sales orders from customers, or bank deposits and withdrawals. Although they are the oldest type of business information system around and handle routine tasks, they are critical to business organisation. For example, what would happen if a bank's system that records deposits and withdrawals and maintain accounts balances disappears?

TPS are vital for the organisation, as they gather all the input necessary for other types of systems. Think of how one could generate a monthly sales report for middle management or critical marketing information to senior managers without TPS. TPS provide the basic input to the company's database. A failure in TPS often means disaster for the organisation. Imagine what happens when an airline reservation system fails: all operations stop and no transaction can be carried out until the system is up and running again. Long queues form in front of ATMs and tellers when a bank's TPS crashes.

Transaction processing systems were created to maintain records and do simple calculations faster, more accurately and more cheaply than people could do the tasks.

Characteristics of TPS:

- TPS are large and complex in terms of the number of system interfaces with the various users and databases and usually developed by MIS experts.
- TPS's control collection of specific data in specific formats and in accordance with rules, policies, and goals of organisation- standard format
- They accumulate information from internal operations o the business.
- They are general in nature—applied across organisations.
- They are continuously evolving.

The goals of TPS is to improve transaction handling by:

- Speeding it up
- Using fewer people
- Improving efficiency and accuracy
- Integrating with other organisational information systems
- Providing information that was not available previously

Examples—Airline reservation systems, ATMs, order processing systems, registration systems, payroll systems and point of sale systems.

5.2 Management Reporting System (MRS)

Management Reporting Systems (MRS) formerly called Management Information Systems (MIS) provide routine information to decision makers to make structured, recurring and routine decisions, such as restocking decisions or bonus awards. They focus on operational efficiency and provide summaries of data. An MRS takes the relatively raw data available through a TPS and converts it into meaningful aggregated form that managers need to conduct their responsibilities. They generate information for monitoring performance (e.g. productivity information) and maintaining coordination (e.g. between purchasing and accounts payable).

The main input to an MRS is data collected and stored by transaction processing systems. An MRS further processes transaction data to produce information useful for specific purposes. Generally, all MIS output have been pre-programmed by information systems personnel. Outputs include:

a) Scheduled Reports – These were originally the only reports provided by early management information systems. Scheduled reports are produced periodically, such as hourly, daily, weekly or monthly. An example might be a weekly sales report that a store manager gets each Monday showing total weekly sales for each department compared to sales this week last year or planned sales.
b) Demand Reports – These provide specific information upon request. For instance, if the store manager wanted to know how weekly sales were going on Friday, and not wait until the scheduled report on Monday, she could request the same report using figures for the part of the week already elapsed.
c) Exception Reports – These are produced to describe unusual circumstances. For example, the store manager might receive a report for the week if any department's sales were more than 10% below planned sales.

>>> Characteristics of MRS

- MIS professionals usually design MRS rather than end users - using life cycle oriented development methodologies.
- They are large and complex in terms of the number of system interfaces with the various users and databases.
- MRS are built for situations in which information requirements are reasonably well known and are expected to remain relatively stable. This limits the informational flexibility of MRS but ensures that a stable informational environment exists.
- They do not directly support the decision-making process in a search for alternative solutions to problems. Information gained through MRS is used in the decision-making process.
- They are oriented towards reporting on the past and the present, rather than projecting the future. Can be manipulated to do predictive reporting.
- MRS have limited analytical capabilities. They are not built around elaborate models, but rather rely on summarisation and extraction from the databases according to the given criteria.

5.3 Decision Support System (DSS)

Decision support systems provide problem-specific support for non-routine, dynamic and often complex decisions or problems. DSS users interact directly with the information systems, helping to model the problem interactively. DSS basically provide support for non-routine decisions or problems and an interactive environment in which decision makers can quickly manipulate data and models of business operations. A DSS might be used, for example, to help a management team decide where to locate a new distribution facility. This is a non-routine, dynamic problem. Each time a new facility must be built, the competitive, environmental, or internal contexts are most likely different. New competitors or government regulations may need to be considered, or the facility may be needed due to a new product line or business venture.

When the structure of a problem or decision changes, or the information required to address it is different each time the decision is made, then the needed information cannot be supplied by an MIS, but must be interactively modelled using a DSS. DSS provide support for analytical work in semi-structured or unstructured situations. They enable mangers to answer 'What if' questions by providing powerful modelling tools (with simulation and optimisation capabilities) and to evaluate alternatives e.g. evaluating alternative marketing plans.

DSS have less structure and predictable use. They are user-friendly and highly interactive. Although they use data from the TPS and MIS, they also allow the inclusion of new data, often from external sources such as current share prices or prices of competitors.

DSS components include:

a) Database (usually extracted from MIS or TPS)
b) Model Base
c) User Dialogue/Dialogue Module

5.4 Executive Information System (EIS) / Executive Support Systems (ESS)

EIS provide a generalized computing and communication environment to senior managers to support strategic decisions. They draw data from the MIS and allow communication with external sources of information. But unlike DSS, they are not designed to use analytical models for specific problem solving. EIS are designed to facilitate senior managers' access to information quickly and effectively.

ESS has menu-driven user-friendly interfaces, interactive graphics to help visualisation of the situation and communication capabilities that link the senior executives to the external databases he requires.

Top executives need ESS because they are busy and want information quickly and in an easy to read form. They want to have direct access to information and want their computer set-up to directly communicate with others. They want structured forms for viewing and want summaries rather than details.

5.5 Expert System (ES)

- It is an advanced DSS that provides expert advice by asking users a sequence of questions dependent on prior answers that lead to a conclusion or recommendation. It is made of a knowledge base (database of decision rules and outcomes), inference engine (search algorithm), and a user interface.
- ES use artificial intelligence technology.

- It attempts to codify and manipulate knowledge rather than information
- ES may expand the capabilities of a DSS in support of the initial phase of the decision making process. It can assist the second (design) phase of the decision making process by suggesting alternative scenarios for "what if" evaluation.
- It assists a human in the selection of an appropriate model for the decision problem. This is an avenue for an automatic model management; the user of such a system would need less knowledge about models.
- ES can simplify model-building in particular simulation models lends itself to this approach.
- ES can provide an explanation of the result obtained with a DSS. This would be a new and important DSS capability.
- ES can act as tutors. In addition ES capabilities may be employed during DSS development; their general potential in software engineering has been recognised.

5.6 Other Information Systems

These are special purpose information systems. They are more recent types of information systems that cannot be characterised as one of the types discussed above.

5.6.1 Office Automation Systems (OAS)

Office automation systems support general office work for handling and managing documents and facilitating communication. Text and image processing systems evolved as from word processors to desktop publishing, enabling the creation of professional documents with graphics and special layout features. Spreadsheets, presentation packages like PowerPoint, personal database systems and note-taking systems (appointment book, notepad, card file) are part of OAS.

In addition OAS include communication systems for transmitting messages and documents (e-mail) and teleconferencing capabilities.

5.6.2 Artificial Intelligence Systems

Artificial intelligence is a broad field of research that focuses on developing computer systems that simulate human behaviour, that is, systems with human characteristics. These characteristics include, vision, reasoning, learning and natural language processing.

Examples: Expert systems, Neural Networks, Robotics.

5.6.3 Knowledge-Based Systems/ Knowledge Work Systems (KWS)

Knowledge Work Systems support highly skilled knowledge workers in the creation and integration

of new knowledge in the company. Computer Aided Design (CAD) systems used by product designers not only allow them to easily make modifications without having to redraw the entire object (just like word processors for documents), but also enable them to test the product without having to build physical prototypes.

Architects use CAD software to create, modify, evaluate and test their designs; such systems can generate photo-realistic pictures, simulating the lighting in rooms at different times of the day, perform calculations, for instance on the amount of paint required. Surgeons use sophisticated CAD systems to design operations. Financial institutions use knowledge work systems to support trading and portfolio management with powerful high-end PCs. These allow managers to get instantaneously analysed results on huge amounts of financial data and provide access to external databases.

Workflow systems are rule-based programmes - (IF 'this happens' THEN 'take this action') - that coordinate and monitor the performance of a set of interrelated tasks in a business process.

5.6.4 Geographic Information Systems (GIS)

Geographic information systems include digital mapping technology used to store and manipulate data relative to locations on the earth. An example is a marketing GIS database. A GIS is different from a Global Positioning System (GPS). The latter is a satellite-based system that allows accurate location determination.

5.6.5 Virtual Reality Systems

Virtual reality systems include 3-dimensional simulation software, where often the user is immersed in a simulated environment using special hardware (such as gloves, data suits or head mounted displays). Sample applications include flight simulators, interior design or surgical training using a virtual patient.

5.6.6 E-Commerce/E-Business Systems

E-Commerce involves business transactions executed electronically between parties. Parties can be companies, consumers, public sector organisations or governments.

5.6.7 Enterprise Resource Planning (ERP) systems

ERP systems are a set of integrated programmes that handle most or all organisations' key business processes at all its locations in a unified manner. Different ERP packages have different scopes. They often coordinate planning, inventory control, production and ordering. Most include finance and manufacturing functions, but many are now including customer relationship management, distribution, human resource as well as supply chain management. ERP systems are integrated around a common database. Some well known ERP vendors are ORACLE, SAP and PeopleSoft.

For instance a manufacturing company may prepare a demand forecast for an item for the next month. The ERP system would then check existing items inventory to see if there is enough on hand to meet the demand. If not, the ERP system schedules production of the shortfall, ordering additional raw material and shipping materials if necessary.

5.6.8 Electronic Funds Transfer (EFT)

EFT is the exchange of money via telecommunications without currency actually changing hands. EFT refers to any financial transaction that transfers a sum of money from one account to another electronically. Usually, transactions originate at a computer at one institution (location) and are transmitted to a computer at another institution (location) with the monetary amount recorded in the respective organisation's accounts. Because of the potential high volume of money being exchanged, these systems may be in an extremely high-risk category. Therefore, access security and authorisation of processing are important controls.

Security in an EFT environment is extremely important. Security includes methods used by the customer to gain access to the system, the communications network and the host or application-processing site. Individual customer access to the EFT system is generally controlled by a plastic card and a personal identification number (PIN). Both items are required to initiate a transaction.

5.6.9 Automated Teller Machine (ATM)

An ATM is a specialised form of point of sale terminal designed for the unattended use by a customer of a financial institution. These customarily allow a range of banking and debit operations, especially financial deposits and cash withdrawals. ATMs are usually located in uncontrolled areas and utilise unprotected telecommunications lines for data transmissions. Therefore, the system must provide high levels of logical and physical security for both the customer and the machinery.

Recommended internal control guidelines for ATMs include the following:

- Review measures to establish proper customer identification and maintenance of their confidentiality
- Review file maintenance and retention system to trace transactions
- Review and maintain exception reports to provide an audit trail
- Review daily reconciliation of ATM machine transactions.

6. The organisation of ICT department

ICT Department functions

a) Development, ongoing operation and maintenance of information systems
b) Advisor to ICT users throughout the organisation
c) Catalyst for improving operations through system enhancements/ new systems development

d) Co-ordinating systems integration in the organisation.
e) Establishing standards, policy, and procedures relating to ICT.
f) Evaluating and selecting hardware and software.
g) Co-ordinating end-user education.

Officers in ICT department

- IT Manager/Director
- Systems analysts
- Programmers - system and applications
- Database administrator
- Network administrator
- Librarian
- Support staff - hardware, software technicians
- Data entry clerks

The number of people working in the ICT department and what they do will depend on:

- *The size of the computing facility.* Larger computers are operated on a shift work basis.
- *The nature of the work.* Batch processing systems tend to require more staff.
- *Whether a network is involved.* This requires additional staff.
- *How much software and maintenance is done inhouse* instead of seeking external resources.

The information technology staff may be categorised into various sections whose managers are answerable to the information technology manager. The responsibilities of the information technology manager include:

- Giving advice to managers on all issues concerning the information technology department.
- Determining the long-term IT policy and plans of the organisation.
- Liaisons with external parties like auditors and suppliers.
- Setting budgets and deadlines.
- Selecting and promoting IT staff.

Structure of ICT department

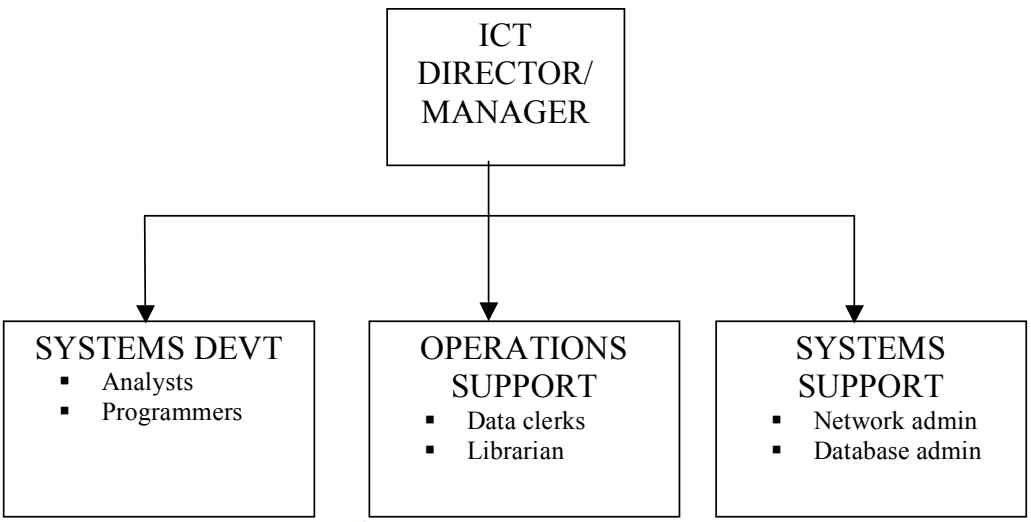
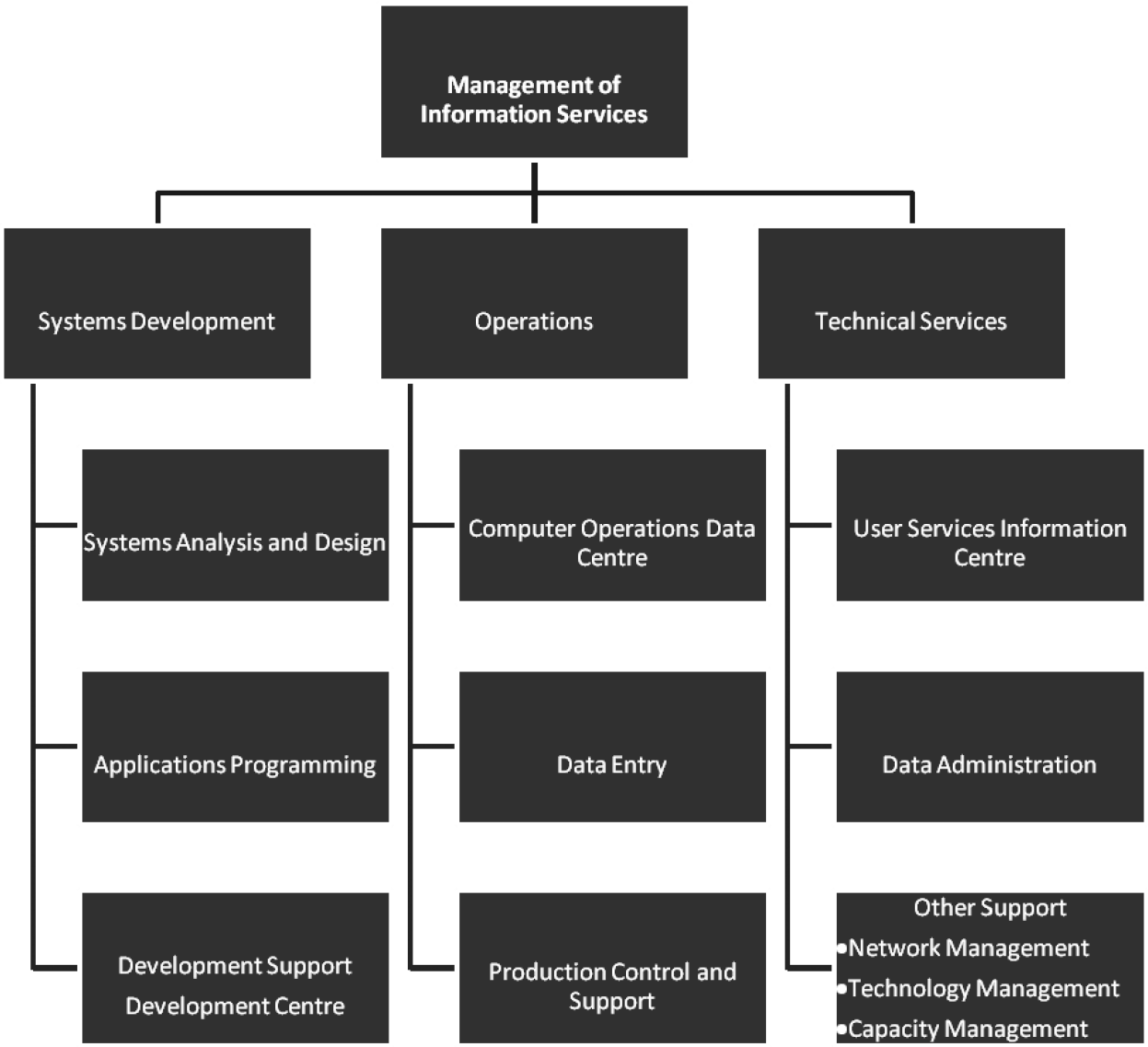


Figure: Structure of ICT Department in a medium institution

Functional structure for information services department



The sections that make up the ICT department and their functions are discussed below:

1) Development section

>>> System Analysis Functions include:

- System investigations.
- System design.
- System testing.
- System implementation.

- System maintenance.

>>> Programming Functions include:

- Writing programmes.
- Testing programmes.
- Maintenance of programmes.
- System programmers write and maintain system software. Application programmers write programmes or customise software to carry out specific tasks.

2) Operations section

Duties include:

- Planning procedures, schedules and staff timetables.
- Contingency planning.
- Supervision and coordination of data collection, preparation, control and computer room operations.
- Liaison with the IT manager and system development manager.

The operations section also carries out:

a) Data preparation

Data preparation staff are responsible for converting data from source documents to computer sensible form.

Duties are:

- Correctly entering data from source documents and forms.
- Keeping a record of data handled.
- Reporting problems with data or equipment.

b) Data control

Data control staff are generally clerks. Duties include:

- Receiving incoming work on time.
- Checking and logging incoming work before passing it to the data preparation staff.
- Dealing with errors and queries on processing.
- Checking and distributing output.

>> Computer room manager

Duties include:

- Control of work progress as per targets.
- Monitoring machine usage.

- Arranging for maintenance and repairs.

>>> Computer operators

Control and operate hardware in the computer room.

Duties include:

- Starting up equipment.
- Running programmes.
- Loading peripherals with appropriate media.
- Cleaning and simple maintenance.

>>> Files librarian

Keeps all files organised and up to date. Typical duties are:

- Keeping records of files and their use.
- Issuing files for authorised use.
- Storing files securely.

3) System Support Section

This section is charged with responsibilities over database and network management

>>> Database management

The database administrator: He is responsible for the planning, organisation and control of the database. His functions include

- Coordinating database design.
- Controlling access to the database for security and privacy.
- Establishing back-up and recovery procedures.
- Controlling changes to the database.
- Selecting and maintaining database software.
- Meeting with users to resolve problems and determine changing requirements.

>>> Network management

The network administrator/controller/manager. Functions include:

- Assignment of user rights.
- Creating and deleting of users.
- Training of users.
- Conflict resolution.
- Advising managers on planning and acquisition of communication equipment.

7. Evaluating effectiveness and efficiency of ICT departments

Fast Forward: It is important to measure how a system, organisation or a department performs, mainly its efficiency and effectiveness.

Efficiency is a ratio of what is produced to what is consumed. It ranges from 0–100%. Systems can be compared by how efficient they are.

SUMMARY

Components of an information system include:

- People
- Computer Hardware
- Computer Software
- Telecommunication System/Communication network
- Databases
- Procedures

The functions of an information system can be generally classified into those functions involved in:

- Transaction processing
- Management reporting
- Decision support

Major types of systems include:

1. Transaction Processing Systems (TPS)
2. Management Information Systems (MIS)
3. Decision Support Systems (DSS)
4. Executive Support Systems (ESS)
5. Expert Systems

The number of people working in the ICT department and what they do will depend on:

- *The size of the computing facility.* Larger computers are operated on a shift work basis.
- *The nature of the work.* Batch processing systems tend to require more staff.
- *Whether a network is involved.* This requires additional staff.

- *How much software and maintenance is done inhouse* instead of seeking external resources.

The responsibilities of the information technology manager include:

- Giving advice to managers on all issues concerning the information technology department.
- Determining the long-term IT policy and plans of the organisation.
- Liaisons with external parties like auditors and suppliers.
- Setting budgets and deadlines.
- Selecting and promoting IT staff.

PAST PAPER ANALYSIS

6/00, 12/00, 6/01, 12/01, 6/02, 12/02, 6/03, 6/04, 12/04, 6/05, 12/05, 6/06, 12/06, 6/07

CHAPTER QUIZ

1. ATM stands for.....

2. ..... support general office work for handling and managing documents and facilitating communication.

3. Which one is the odd one out?
   a. Semi-programmable Systems (SPS)
   b. Transaction Processing Systems (TPS)
   c. Management Information Systems (MIS)
   d. Decision Support Systems (DSS)

4. Which of the following is not a function of an information system
   a. Transaction processing
   b. Management reporting
   c. Budget formulating
   d. Decision support

5. ..... involves business transactions executed electronically between parties.

ANSWERS TO CHAPTER QUIZ

1. Automated Teller Machine
2. Office automation systems
3. a. Semi-programmable Systems (SPS) – it is not one of information systems
4. c. Budget formulating
5. E-Commerce

EXAMS QUESTIONS

1. Within all organisations of substance there should be an identified post with responsibility for information management. Briefly discuss the role of an individual filling this post, indicating the issues which he or she may be expected to address.
2. Your organisation is investigating the value of setting up an information centre. Briefly report on the concept of the information centre.
3. A management services department represents a link between decision-makers and the information system by providing support tools, or by providing the techniques, methodologies, and expertise to drive those tools. Briefly describe how a management services department may fit into a typical commercial organisation.
4. Discuss the components of an information system.
   The number of people working in the ICT department and what they do will depend on various factors. Outline some of these factors.

CHAPTER FIVE

INFORMATION SYSTEMS STRATEGY

CHAPTER FIVE

INFORMATION SYSTEMS STRATEGY

▶ OBJECTIVES

When you have completed this chapter, you should be able to:

1. Identify the applications of information systems in businesses.
2. Identify the various applications of information systems in different fields: accounting, sales and marketing, manufacturing and production, banking, etc.

▶ INTRODUCTION

Information system (IS) refers to a collection of components that collects, processes, stores, and analyses and disseminates information for a specific purpose. It contains the four elements of input, processing, output and control. Information technology (IT) refers to the technological aspect of information systems. IT is often used interchangeably with the term IS but it is an inclusive term, which describes a collection of several IS within an organisation. IT basically represents the modern merger of computer technology with telecommunications technology.

▶ DEFINITION OF KEY TERMS

Online transaction processing systems – A transaction processing mode in which transactions entered online are immediately processed by the CPU.

Fault-tolerant systems – systems with extra (redundant) hardware, software, and power as backups against failure.

▶ EXAM CONTEXT

The chapter relates to application of Information Technology in the industry. As such, it gives an overview of the various uses of technology in different departments of an organisation(s). Questions from this chapter will test various applications of technology in different industries or department(s) within an organisation. The student will be required to have a wide knowledge on various applications of the technology not restricting to the applications outlined in this chapter.

STUDY TEXT

▶ INDUSTRY CONTEXT

In accounting the separate entity concept treats a business as distinct and completely separate from its owners. The business stands apart from other organisations as separate economic unit. It is necessary to record the business transactions separately to distinguish it from the owner's personal transactions. This concept is now extended to accounting for various divisions of a firm in order to ascertain results for each division.

1. Business Environment

The **business environment** is changing and as a result organisations are changing. These changes are facilitated and accelerated by advances in IT. IS is part of the organizational framework to manage that change. Thus IS/IT is an important enabler for cost reduction, increased competitiveness and increased sales. Organizations respond to both environmental change and future technological change. Major business pressures include:

a) Technology – New innovations, obsolescence of current technology, information overload and emergence of electronic commerce.
b) Market – digital economy and strong global competition, changing workforce, powerful consumers, new markets, increased competition etc. Digital economy refers to an economy that is based on digital technologies, including digital communication networks, computers and software.
c) Society – need for social responsibility, government regulations and government deregulation, shrinking government budgets/subsidies, good corporate governance, accurate accounting reports and ethical issues.

There has been a critical shift in the application of IT in most organisations. For example:

- From personal computing to workgroup computing.
- From systems 'islands' to integrated systems.
- From stand alone systems to distributed and networked systems.
- From internal to inter enterprise computing.
- From desktop oriented systems to web based systems.

2. Organisations major responses to business pressures

- Strategic systems for competitive advantage
- Continuous improvement efforts
- Business process re-engineering (BPR)
- Business alliances
- Electronic commerce

3. General technological trends

General trends within computing systems include:

- Object oriented environment and document management
- Networked computing
- Mobile commerce
- Integrated home computing
- The Internet
- Intranets and extranets
- Optical networks

4. Application of information systems in business

Basic business systems serve the most elementary day-to-day activities of an organisation; they support the operational level of the business and also supply data for higher-level management decisions. They provide support of the functional areas of business (marketing, production/ operations, accounting, finance, human resource management) through computer-based information systems. Common properties for these systems include:

- Often critical to survival of the organisation
- Mostly for predefined, structured tasks
- Can have strategic consequences (e.g. airline reservation system)
- Most have high volumes of input and output
- Summarised information from basic systems used by higher levels of management
- Need to be fault-tolerant (ability to cope with failure of a system component without entire business system going down/failing).

Some of the challenges that business systems pose are:

- Organisational challenges
  - The need to streamline systems (manual and computer) as much as possible
  - The need to update systems without disrupting the firm
- People challenges
  - Ensuring consistency and completeness in procedures

- Ensuring time is actually saved
- Technology challenges
  - Using client/server technology than mainframes
  - Linking different types of systems
  - Ensuring the right data is supplied to management

5. Application of information systems in accounting

These are systems that maintain records concerning the flow of funds in the firm and produce financial statements, such as balance sheets and income statements. They are among the earliest systems to be computerised.

5.1 OPERATIONAL-LEVEL ACCOUNTING IS

Operational accounting information systems produce the routine, repetitive information outputs that every organisation finds necessary, including pay cheques, cheques to vendors, customer invoices, purchase orders, stock reports, and other regular forms and reports.

The heart of an organisation's operational-level accounting information system is the financial accounting system. A computerized financial accounting system is composed of a series of software modules or subsystems used separately or in an integrated fashion.

The system modules typically include

- General ledger.
- Fixed assets.
- Sales order processing.
- Accounts receivable.
- Accounts payable.
- Inventory control.
- Purchase order processing.
- Payroll.

When these computerised financial accounting subsystems are integrated, each subsystem receives data as input from other subsystems and provides information as output to other subsystems.

The General Ledger Subsystem

The general ledger subsystem ties all other financial accounting system subsystems together. It provides managers with:

- Periodic accounting reports and statements, such as income statement and balance sheets.
- Support for budgeting.
- Creation of general ledger accounts and definition of the organisation's fiscal period
- Production of a list of accounts maintained by the financial accounting system.

The Fixed Assets Subsystem

The fixed assets subsystem maintains records of equipment, property and other long-term assets an organisation owns. The records include:

- Original cost of the assets
- Depreciation rate on each asset or group of assets
- Accumulated depreciation to date
- Book value of the asset.

The general ledger subsystem uses this information to maintain up-to-date balances in the various long-term asset accounts of the organisation. The subsystem also may maintain and process data on the gain or loss on the sale of fixed assets and prepare special income tax forms for fixed assets required by the federal government.

The Sales Order Processing Subsystem

The sales order processing subsystem, or order entry subsystem:

- Routinely records sales orders.
- Provides the documents that other subsystems use to fill those orders, that maintain inventory levels, and that bill the customer (sales invoices).
- Provides sales tax data to the general ledger subsystem for posting to taxing-agency accounts.
- Provides stock data to the inventory subsystem for updating inventory balances
- Provides sales invoice data to the accounts receivable subsystem for posting to customer accounts.

The Accounts Receivable Subsystem

The accounts receivable subsystem allows one to enter, update, and delete customer information, such as:

- Charge sales
- Credit terms
- Cash payments received
- Credit for returned or damaged merchandise
- Account balances

Typical inputs to the accounts receivable subsystem include

- Sales invoices
- Credit memoranda
- Cash received from customers

Typical outputs are:

- Monthly customer statements of account.
- Schedule of accounts receivable listing each account and its balance.

The Accounts Payable Subsystem

The accounts payable subsystem processes much of the same routine, repetitive information as the accounts receivable subsystem, except that the information is about the organisation's creditors rather than customers.

The accounts payable subsystem provides data directly to the general ledger subsystem and receives data from the purchase order subsystem.

Typical inputs to the accounts payable subsystem include

- Purchase orders
- Adjustments (returns, credit memos)

Typical outputs are:

- Cheques to creditors
- Schedule of accounts payable

The Inventory Control Subsystem

The inventory control subsystem provides input to the general ledger subsystem and receives input from the purchase order and the sales order subsystems. The basic purpose of the subsystem is to

- Keep track of inventory levels
- Keep track of inventory costs for the organisation

The subsystem maintains information about each stock item, such as:

- Stock numbers
- Stock descriptions
- Receipts and issues of stock
- Stock balances

The Purchase Order Processing Subsystem

The purchase order processing subsystem processes purchase orders and tracks regarding:

- Which purchase orders have been filled.
- Which stock items ordered are on backorder.
- Which stock items have been damaged.
- Which stock items do not meet the specifications of the original order.
- When orders are expected to be received.

The purchase order subsystem provides information to the accounts payable and inventory subsystems.

The Payroll Subsystem

The payroll subsystem processes wage and salary information, such as :

- Payments to employees
- Deductions from employee pay cheques
- Payments to state
- Other taxing agencies for taxes owed

Operational-level financial accounting information systems are transaction-processing systems.

They record and report the voluminous, routine, and repetitive transactions that mirror the day-to-day operations of an organisation. By computerizing these operational-level systems, organisation often eliminate the drudgery of manually recording the endless detail needed in these systems. This usually reduces the costs of processing this work.

5.2 TACTICAL ACCOUNTING AND FINANCIAL IS

Tactical accounting and financial information systems support management decision making by providing managers with:

- Regular summary reports.
- Regular exception reports.
- Ad hoc reports.
- Other information that helps them control their areas of responsibility and allocate their resources to pursue organisation goals.

The focus of tactical information systems is resource allocation. It is possible to design many computer-supported, tactical-level information systems for the financial decisions that managers must make. These include:

- Budgeting systems
- Cash management systems
- Capital budgeting systems
- Investment management systems

Budgeting Systems

The budgeting system permits managers to:

- Track actual revenues
- Track actual expenses
- Compare these amounts to expected revenues and expenses
- Compare current budget amounts to those of prior fiscal periods
- Compare current budget amounts to other divisions
- Compare current budget amounts to other departments
- Compare current budget amounts to industry wide-data.

Comparisons of budget data against such standards allow managers to assess how they use their resources to achieve their goals.

The general ledger system of computerised financial accounting systems often permits budget amounts to be entered by account number. Periodically (weekly, monthly, quarterly, or annually) these budgeted amounts (allocations) and the actual amounts spent or received (actual) for each account are compared and reports prepared.

Cash Management Systems

Cash Management Systems help managers to:

- Ensure that the organisation has sufficient cash to meet its needs
- Put excess funds from any period to use through investments
- Provide borrowing power to meet the organization's cash needs in those periods of insufficient cash flow

The information supplied by a cash flow report helps the manager to make decisions about investing, purchasing, and borrowing money. By simulating many different possible business conditions, the manager is able to make more informed decisions about the use of or need for cash for the short term. In short, the manager can study various reallocations of the resources of a department, division or other unit.

Capital Budgeting Systems

Capital Budgeting Systems manage information about

- The planned acquisition
- The disposal of major plant assets during the current year.
- The manager may compare the various capital spending plans using three commonly used evaluation tools: net present value, internal rate of return, and payback period.

Investment Management Systems

Investment Management Systems assist the managers in overseeing the organisation's investments in

- Stocks
- Bonds
- Other securities

Whatever their source of investment funds, most organisations invest money in securities of one kind or another. Careful management of these investments is necessary to ensure the achievement of organisational goals.

5.3 STRATEGIC ACCOUNTING AND FINANCIAL IS

Strategic-level Information Systems are goal oriented and are designed to support organisation goal and direction setting.

Two major outcomes of financial strategic planning are:

- The setting of financial goals (investments and return on investments)
- Directions for the organisation (new investment opportunities or the mix of capital sources used to fund the organisation)

Strategic Accounting and Financial IS contain

- Financial Condition Analysis Systems
- Long-Range Forecasting Systems

Financial Condition Analysis Systems

Financial Condition Analysis Systems provide the managers with many reports to which ratios and analysis tools may be applied. They supply reports that automatically calculate and present the results of these tools and ratios. This system provides management with a variety of measures of the soundness of the organisation and makes it possible to explore ways of improving the organisation's financial condition.

Long-Range Forecasting Systems

Long-Range Forecasting Systems provide forecasts on a variety of factors that will affect organisation performance in future. Some forecasts may involve the use of internally generated data (past sales data); others may use only external data or both internal and external data. These systems forecast the financial health of the organisation through long-range budget estimates including:

- A variety of possible wage negotiation settlements
- Actions by competitors
- Interest rate fluctuations
- Fuel cost changes
- Different inflation rates

5.4 ACCOUNTING AND FINANCIAL MANAGEMENT SOFTWARE

To provide managers with the capability to handle financial information systems, a number of software products, both general and specialized, have emerged. General software products are not designed specifically for the financial manager and may be used by most people. Specialised software products have been designed especially for the financial manager.

General software helpful to the financial manager include

- Spreadsheet software
- Forecasting and statistical software
- Query language and report writer software

Spreadsheet Software

Spreadsheet software packages provide a versatile tool for financial managers. Spreadsheet software allows the manager to design partially completed tables or forms called templates, which contain the headings and names of the items in the spreadsheet. The templates also contain the formulas used to calculate column or row totals, column or row averages and other statistical quantities on the values entered into the template.

Forecasting and Statistical Software

Many financial analysis tasks involve forecasting future events and require that you use statistical tools. Selecting statistical or forecasting software to aid you in tactical-level decisions and long-range planning requires that you carefully analyse what your applications require.

Query Language and Report Writing Software

If your database management system contains a query language, a report writer, or both, then these tools can be used to poke through the data in the database to find useful information to your *ad hoc* questions about financial management.

5. 5 COMPUTERIZED ACCOUNTING SYSTEMS

Commercially packaged accounting system software contains the operating-level software used to produce:

- Invoices
- Cheques
- Monthly financial statements
- Other regular, routine output necessary to run an organisation

In addition, many computerised accounting systems provide a variety of features including financial analysis tools for the tactical decision maker and strategic planner, such as the various financial statement ratio analyses.

5.6 COMPUTERISED AUDITING SOFTWARE

Fast Forward: With an increasing focus on governance, risk and compliance, internal audit departments face mounting pressure and heavier workloads in providing expanded oversight and assurance.

A number of computerised auditing programmes are available to assist auditors when they evaluate or monitor a computerised accounting system. Generalised audit software :

- Provides access to the computer files
- Lets EDP auditors create audit files
- Extract data
- Analyse data statistically
- Sorts, summarises, and samples data
- Generates reports

A variety of commercially prepared software provides the manager with specific financial analysis and planning tools. These financial analysis software products are often quite narrow in scope. For example, some specialised software products assist the financial manager in developing and analysing the capital budgeting needs of the organisation. Others assist the investment manager in monitoring and analysing the organisation's investment portfolio. The financial manager can use specialised software products to help manage the cash flow of the organisation.

6. Application of information systems in sales and marketing

These are systems that support the sales and marketing function by facilitating the movement of goods and services from producers to customers.

6.1 OPERATIONAL MARKETING INFORMATION SYSTEMS

Marketing information systems at the operating level, primarily produce routine repetitive, descriptive, expected and objective data that describe past marketing activities. The information they produce is usually detailed, highly structured, accurate, derived from internal sources and produced regularly.

Contact Information Systems

Customer contact information systems provide information to the sales force on customers, their product or service preferences, sales history data and a historical record of sales calls and visits.

Prospect Information Systems

Prospect Information Systems help the sales team to achieve locate potential customers. This is often a time-consuming and frustrating part of the salesperson's work. The sources of information for leads on prospective customers are frequently diverse and may include other customers, other vendors who sell supporting or auxillary products, newspaper notices, telephone directories, and direct customer inquiries. Searching hard-copy directories and other paper lists of customers may be very time-consuming and yield few future customers. When these files are stored on magnetic media, they are easier for the salesperson to search or summarise.

Telemarketing Systems

Use of the telephone to sell products and services, or telemarketing systems, has become a common and important means by which organisations improve the productivity of their sales forces. The telephone allows salespeople to initiate contacts, offer products and services, or follow up on sales without travel cost or travel time. It also lets salespeople to reach many more customers in a given time period than they could have through other means.

Direct-Mail Advertising Systems

Many organisations generate sales by mailing sales brochures and catalogs directly to customers using direct-mail advertising systems. To distribute sales documents rapidly to large numbers of potential customers, most marketing departments maintain customer mailing lists for mass mailing. The lists may be drawn from customer files, accounts receivable records, prospect files or commercial databases of households, businesses and organisations.

Inquiry Information Systems

Inquiry Information Systems record, process and store the inquires when customers inquire about the products and services the organisation offers. It is important to compile information about the actual or potential customers who made the inquiry, what products or services the query pertained to, when the inquiry was made, and where the potential customer is located and to record these data on a medium that will allow analysis easily at some future time.

Distribution Information Systems

Distribution Information Systems monitor the goods being distributed regardless of the systems chosen. An organisation may choose to use existing commercial and public delivery systems for its products and services, such as the postal service, private parcel services or freight companies. It may also choose to provide its own product delivery systems for its customers.

It is important to track products or services throughout the distribution system to identify and correct delivery errors and reduce delivery time. The speed with which an organisation can deliver its products is an important customer service.

If the organisation maintains its own distribution system, information about its effectiveness must be collected and reported to management. Information should also be maintained about the

acquisition, repair, use and allocation of equipment.

Supporting Operational-Level Financial Accounting Systems

The following financial operational information systems provide much-needed data to the marketing function.

- Sales Order Processing Systems
- Point-of-sale (POS) systems
- Inventory Information Systems
- Credit Information Systems

6.2 TACTICAL MARKETING INFORMATION SYSTEMS

A great deal of the data that tactical marketing information systems utilise is collected by operational financial information systems. Tactical marketing information systems often combine operational-level financial data with other data to support tactical decision-making managers.

Sales Management Information Systems

A major objective of sales managers is to reach the sales goals set by top management. To accomplish this objective, sales managers must make many tactical decisions. To make these decisions effectively, sales managers should have at their disposal a great deal of data about the sales histories of each salesperson, territory product, and market segment. Sales Management Information Systems provide the managers with this data. Managers can use these data to develop reports analysing sales activities that help them make decisions about salespeople, territories, products and customers and to control current campaigns.

Advertising and Promotion Information Systems

Advertising and promotional tactics also need to be developed by marketing managers to implement strategic sales goals set by top management. Managers must decide which advertising media and promotional devices to use to reach the selected market segments, when these media and devices should be used, and what overall mix of promotional activities should be deployed to achieve sales goals. Advertising and promotion information systems assist managers in these tasks.

Product pricing Information Systems

These provide information to managers that help them set prices for their products and services. The marketing manager usually selects a price that will at least recover production costs, but the price chosen is constrained by the prices of competitors for similar products or services and for alternative products or services. To make pricing decisions, the marketing manager should know the expected demand for the product or similar products, the desired profit margin for the organisation, the costs of producing the product or providing the service and the prices of competing products.

Distribution Channel Decision Support Systems

A distribution channel decision support system should provide information on the costs of using

the various distribution channels, the time lags caused by the various channels, the reliability of the various channels in delivering the products and services, and the market segment saturation provided by the channels. It should also track the demand and inventory at all levels of the distribution channels so that the manager may anticipate excess inventories or shortfalls.

6.3 STRATEGIC MARKETING INFORMATION SYSTEMS

The strategic activities include segmenting the market into target groups of potential customers based on common characteristics or needs or wants, selecting those market segments the organisation wishes to reach, planning products and services to meet those customers needs, and forecasting sales for the market segments and products.

Sales Forecasting Information Systems

Strategic sales forecasting information systems usually include several varieties of forecasts:

- Forecast of sales for the industry as a whole.
- Forecast of sales for the entire organisation.
- Forecasts of sales for each product or service.
- Forecasts of sales for a new product or service.

Regardless of type, sales forecasts are usually based on more than historical data; they are not merely projections of past trends. Sales forecasts are also based on assumptions about the activities of the competition, governmental action, shifting customer demand, demographic trends and a variety of other pertinent factors, including even the weather.

Product Planning and Development Information Systems

The major objective of product planning and development information systems is to make information about consumer preferences obtained from the marketing research system and the customer inquiry system available for the development of new products. The primary output of planning and development activities is a set of product specifications.

6.4 SPECIFIC MARKETING SOFTWARE

In the last few years, many specialized software packages have been developed for a variety of marketing activities. According to Horton (1986), specialised marketing software can be classified into five categories. That which will:

1. Help salespeople sell the organisation's products and services
2. Help sales managers manage sales personnel.
3. Help manage the telemarketing programme.
4. Help manage customer support.
5. Provide integrated services for many sales and marketing activities.

Sales Personnel Support Software

Sales Personnel Support Software provides document, file, scheduling and other support for salespeople. Document support features may include:

- A package of form letters (these are forms that sales people may use to document their activities, customers' details, customers' performance and so forth) that salespeople can use or adapt for use.
- The ability to keep customer lists.
- The ability to merge letters with customer lists for large mailings.

File support features may include the ability to record and store information about potential and current customers.

Salesperson support software often includes a calendar module to help salespeople manage their meetings and customer appointments and a tickler file module to ensure that they follow through on their promises to customers at the appointed time.

Sales Management Software

Sales Management Software allows the manager to:

- Identify weak territories or weak products in a territory
- Compare salesperson performance by product and customer type
- Compare salesperson performance against salesperson goals
- Analyse salesperson calls within territories or by customer type
- Identify trends in customer purchase
- Identify potential shortages or excess stock in inventory
- Perform other planning, controlling, and organising tasks with ease and speed

Telemarketing Software

Telemarketing Software provides computer support for identifying customers and calling them from disk-based telephone directories or from customer files maintained on a database. The packages may allow you to:

- Make notes about the telephone calls you make
- Generate follow-up letters to the customer
- View a customer file while a call to that customer is in progress

Other software is designed to find, dial, and connect salespeople automatically to people or companies listed in disk-based telephone directories. This software may then provide a digitised message about a product to those who answer the phone, or permit the salesperson to answer the call.

Customer Support Software

This provides information to salespeople about the previous experiences of customers with the organisation such as detailed information on purchases, payments, and specific products purchased by each customer, including competitor products. Customer support software allows salespeople to view customer data prior to sales calls, to identify customers who should be called, to analyse customer-purchasing trends, to identify customers who have purchased products that require follow-up calls and to perform many other sales activities pertaining to customer maintenance.

Integrated Marketing Software

This combines programmes that also may be sold as stand alone packages for salesperson

support, sales management, or customer support. In addition, highly integrated software supports many marketing professionals throughout the organisation by drawing on data not only from salespeople but also from the organisation's financial database.

7. Application of information systems in manufacturing and production

These are systems that supply data to operate, monitor and control the production process.

7.1 OPERATIONAL PRODUCTION IS

- Purchasing Information Systems
- Receiving Information Systems
- Quality Control Information Systems
- Shipping Information Systems
- Cost Accounting Information Systems
- Inventory Management and Control Information Systems

Purchasing Information Systems

To produce goods and services, you must have the right quantity of raw materials and production supplies on hand. Furthermore, you will want to procure these materials and supplies at the lowest cost and have them delivered at the right time. To assist in this function, the Purchasing Information System has to maintain data on all phases of the acquisition of raw materials and purchased parts used in production.

Receiving Information Systems

When shipments of purchased goods and supplies are received, they must usually be inspected and verified and the information about their status passed on to the accounts payable, inventory, and production departments. Delivery dates should also be noted so that data on delivery times can be collected. This type of information is supplied by Receiving Information Systems.

Quality Control Information Systems

Quality Control Information Systems provide information about the status of production goods as they move from the raw materials state, through goods-in-process, to the finished goods inventory. Quality control systems also ensure that raw materials or parts purchased for use in the production processes meet the standards set for those materials.

Shipping Information Systems

Many records and documents assist and monitor the inventory and shipping processes such as shipping reports and packing slips. Packing slips usually include a partial copy of the sales invoice and list the quantity, stock number, and description of the merchandise packed in a shipping carton. The information from the shipping system affects the inventory and accounts receivable systems.

Cost Accounting Information Systems

Many operational information subsystems of the financial accounting system collect and report information about the resources used in the production processes so that accurate production costs can be obtained for products and services. Cost accounting systems monitor the three major resources used in production: personnel, materials, and equipment and facilities.

Inventory Management and Control Information Systems

The management and control of raw materials, goods-in-process, and finished goods inventories is an important part of the production system. Careful management and control of these inventories usually provide considerable savings to the organization. Inventory management and control systems use information from operational information systems, such as the shipping and receiving systems, purchasing systems, and order entry systems.

7.2 TACTICAL MANUFACTURING AND PRODUCTION IS

Manufacturing and production costs are a major cost component of any organisation. It should not be surprising, therefore, to find that many information systems are available to help managers:

- Monitor and control manufacturing and production processes
- Allocate resources to achieve manufacturing and production goals set through the strategic planning process

Materials Requirements Planning Systems

Inventory management can be taken a step further so that the system automatically produces purchase orders for stock that needs to be reordered. The processes of identifying stock that planned production calls for, determining the lead time to get the stock from suppliers, calculating safety stock levels, calculating the most cost-effective order quantities, and then producing purchase orders for those stock items in the right amounts at the right times to ensure that the stock will be on hand when it is needed is known as materials requirements planning (MRP).

Just-in-Time Systems

The Just-in-Time (JIT) system is not a tactical information system, but a tactical approach to production. The JIT approach was created by the Toyota Motor Company of Japan and has generated many advantages to organisations, especially those that do repetitive manufacturing. The purpose of the approach is to eliminate waste in the use of equipment, parts, space, workers' time, and materials, including the resources devoted to inventories. The basic philosophy of JIT is that operations should occur just when they are required to maintain the production schedule. To ensure a smooth flow of operations in that environment, sources of problems must be eradicated.

Capacity Planning Information Systems

Capacity Planning Information Systems allow the managers to

- Allocate personnel and production facilities
- Select sites for constructing plant facilities
- Acquire plant facilities

- Plan those facilities to meet long-term production goals are usually categorised as strategic planning manufacturing decisions.

Production Scheduling Information Systems

The purpose of the production schedule is to allocate the use of specific production facilities for the production of finished goods to meet the master production schedule. To manage the scheduling process, a number of scheduling tools have been developed. Two of these tools are Gantt and PERT (Program Evaluation and Review Technique) charts.

Product Design and Development Information Systems

Many tactical decisions must be made to design and develop a product, especially a new product. The design engineering team usually depends on product specification information derived from customer surveys, target population analysis, or other marketing research information systems. Teams may use other computerised systems for designing new products as well.

Strategic Planning Manufacturing Information Systems

Production Information Systems are primarily operational and tactical in nature. They provide information to monitor and control the production of goods and services and to allocate resources to complete production processes. Manufacturing information systems are typically strategic in nature.

Technology Planning and Assessment

Having access to information on new production technologies allows top management to make better and more informed decisions about which production technologies to use for a product or service. Technology Assessment Information Systems, which identify new technologies and assess them for their strategic advantage, can help top management in many areas, not merely manufacturing.

Plant design

Designing and laying out a manufacturing plant requires large amounts of diverse information about the proposed plant including:

- Engineering data on the proposed site
- Proposed production technologies
- The number and duties of plant personnel
- The expected schedule for the use of the facility
- The area transportation system
- Choices of water and power systems and their costs
- The cost and availability of construction materials
- The plans for shop-floor information systems
- The need for physical security

7.3 SPECIFIC SOFTWARE

Software that addresses the managerial problems in manufacturing and production environments

has grown rapidly. Many software packages are available for specific production tasks such as bill-of-materials software, inventory management software, capacity planning software, production scheduling software, shop-floor scheduling and control software, job costing software, even simulating running a factory. However, the industry is clearly moving toward integrated and comprehensive computer hardware and software systems that provide greater control over all or groups of production and manufacturing activities.

Quality Control Software

Quality Control Software typically includes statistical software tailored to the needs of quality control tasks. For example, quality control software may produce control charts and Pareto diagrams.

Automated Materials Handling Software

Automated Materials handling (AMH) software tracks, controls, and otherwise supports the movement of raw materials, work-in-process, and finished goods from the receiving docks to the shipping docks. AMH software combines with various materials handling equipment, including conveyors, pick-and-place robots, and automated guided vehicles, to get this job done.

Computer-Aided Design and Manufacturing Software

A great deal of software has been developed to aid product engineers in the design of new products or the improvement of old products. One type of software that helps product engineers is CAD/CAM (computer-aided design/computer-aided manufacturing) software. CAD software normally falls into two categories. One category is designed to help mechanical engineers and architects construct and modify complex drawings, blueprints, diagrams, or illustrations quickly and easily. Another category of CAD software includes programmes that help electrical engineers produce schematics quickly and easily, alter the schematics, and then produce a final draft of the electrical circuits.

Image Management Software

Engineering and architectural drawings are difficult to store and retrieve in hardcopy form. Parts of one design may be useful in another, if only you can find the design that contained the useful element. Image management software is designed to manage the storage and retrieval of engineering and architectural drawings using optical disk storage media.

Materials Selection Software

Many programmes are available that aid the engineer in choosing materials for the product under design. These programs are called materials selection programmes, or MSP.

Materials Requirements Planning Software

The basic purpose of MRP software is to ensure that the proper amount of the right materials and production capacity are available for the production processes at the right time.

Manufacturing Resource Planning Software

More recently, software that provides for manufacturing resource planning, or MRP-II, has become

available. MRP-II software extends the production information system to finance, marketing, human resource management, and other organisational functions.

Computer-Integrated Manufacturing Software

Many production and manufacturing professionals envision a day when factory and product planning, control, design, and operation will be totally integrated and almost totally computerized. Some software and hardware firms that provide MSP, MRP, MRP-II, CAD, CAM, CAE, CAT, CAPP, CAI, robotics, and related information systems are joining forces through mergers, acquisitions, and joint projects to integrate current manufacturing hardware and software products into systems that provide computer-integrated manufacturing(CIM).

8. Application of information systems in banking

Some of the information systems implemented by banks include:

8.1 OPERATIONAL INFORMATION SYSTEMS

- ATM systems
- Cash vault automation
- Cheque processing and verification systems
- EDI systems
- EFT systems
- Document processing systems
- Voice response systems
- Cash management systems
- General ledger systems
- Image processing systems
- Payroll processing systems
- Online banking systems

8.2 TACTICAL AND MANAGERIAL CONTROL SYSTEMS

- Account analysis systems
- Asset liability management systems
- Bankruptcy analysis systems
- Credit analysis systems – credit processing, customer account analysis, customer information database
- Risk management systems – securities processing, security management
- Trust management systems

8.3 STRATEGIC PLANNING SYSTEMS

Financial planning systems

Investment planning and management systems

8.4 ONLINE BANKING

Fast Forward: The coming of the Internet era and the personal computers trend gave an opportunity and a challenge for the banking industry.

Online banking uses today's computer technology to give customers the option of bypassing the time-consuming, paper-based aspects of traditional banking in order to manage finances more quickly and efficiently.

The advent of the Internet and the popularity of personal computers presented both an opportunity and a challenge for the banking industry. For years, financial institutions have used powerful computer networks to automate millions of daily transactions. Today, often the only paper record is the customer's receipt at the point of sale. Now that customers are connected to the Internet via personal computers, banks envision similar economic advantages by adapting those same internal electronic processes to home use.

Banks view online banking as a powerful 'value-added' tool to attract and retain new customers while helping to eliminate costly paper handling and teller interactions in an increasingly competitive banking environment. Today, most national banks, many regional banks and even smaller banks and credit unions offer some form of online banking (at least in developed countries), variously known as PC banking, home banking, electronic banking or Internet banking. Those that do are sometimes referred to as "brick-to-click" banks, both to distinguish them from brick-and-mortar banks that have yet to offer online banking, as well as from online or "virtual" banks that have no physical branches or tellers whatsoever.

The challenge for the banking industry has been to design this new service channel in such a way that its customers will readily learn to use and trust it. Most of the large banks now offer fully secure, fully functional online banking for free or for a small fee. Some smaller banks offer limited access or functionality; for instance, you may be able to view your account balance and history but not initiate transactions online. As more banks succeed online and more customers use their sites, fully functional online banking likely will become as commonplace as automated teller machines.

Virtual banks

Virtual banks are banks without bricks; from the customer's perspective, they exist entirely on the Internet, where they offer pretty much the same range of services and adhere to the same federal regulations as your corner bank.

Virtual banks pass the money they save on overhead like buildings and tellers along to the customer in the form of higher yields, lower fees and more generous account thresholds. The major disadvantage of virtual banks revolves around ATMs. Because they have no ATM machines, virtual banks typically charge the same surcharge that the brick-and-mortar bank would if a customer used another bank's automated teller. Likewise, many virtual banks won't accept deposits via ATM; a customer has to either deposit the cheque by mail or transfer money from another account.

Advantages of online banking

- **Convenience**: Unlike your corner bank, online banking sites never close; they're available 24 hours a day, seven days a week, and they're only a mouse click away.
- **Ubiquity**: If you're out of state or even out of the country when a money problem arises, you can log on instantly to your online bank and take care of business, 24/7.
- **Transaction speed**: Online bank sites generally execute and confirm transactions at or quicker than ATM processing speeds.
- **Efficiency**: You can access and manage all of your bank accounts, even securities, from one secure site.
- **Effectiveness**: Many online banking sites now offer sophisticated tools, including account aggregation, stock quotes, rate alerts and portfolio managing programs to help you manage all of your assets more effectively. Most are also compatible with money managing programs such as Quicken and Microsoft Money.

Disadvantages of online banking

- Start-up may take time: In order to register for your bank's online programme, you will probably have to provide ID and sign a form at a bank branch. If you and your spouse wish to view and manage your assets together online, one of you may have to sign a durable power of attorney before the bank will display all of your holdings together.
- Learning curve: Banking sites can be difficult to navigate at first. Plan to invest some time and/or read the tutorials in order to become comfortable in your virtual lobby.
- Bank site changes: Even the largest banks periodically upgrade their online programs, adding new features in unfamiliar places. In some cases, you may have to re-enter account information.
- The trust thing: For many people, the biggest hurdle to online banking is learning to trust it. Did my transaction go through? Did I push the transfer button once or twice? Best bet: always print the transaction receipt and keep it with your bank records until it shows up on your personal site and/or your bank statement.

STUDY TEXT

9. Application of information systems in human resource

These are systems that deal with recruitment, placement, performance evaluation, compensation and career development of the firm's employees.

9.1 OPERATIONAL HUMAN RESOURCE IS

Operational human resource information systems provide the manager with data to support routine and repetitive human resource decisions. Several operational-level information systems collect and report human resource data. These systems include information about the organisation's positions and employees and about governmental regulations.

Employee Information Systems

The human resource department must maintain information on each of the organisation's employees for a variety of decision making and reporting purposes. One part of this employee

information system is a set of human resource profile records. An employee profile usually contains personal and organisation-related information, such as name, address, sex, minority status, marital status, citizenship, years of service or seniority data, education and training, previous experience, employment history within the organisation, salary rate, salary or wage grade, and retirement and health plan choices. The employee inventory may also contain data about employee preferences for geographical locations and work shifts. Another part of an employee information system is an employee skills inventory. The skills inventory contains information about every employee, such as work experience, work preferences, test scores, interests, and special skills or proficiencies.

Position Control Systems

A job is usually defined as a group of identical positions. A position, on the other hand, consists of tasks performed by one worker. The purpose of a position control system is to identify each position in the organization, the job title within which the position is classified, and the employee currently assigned to the position. Reference to the position control system allows a human resource manager to identify the details about unfilled positions.

Applicant Selection and Placement Information Systems

After jobs and the employee requirements for those jobs have been identified and after a suitable pool of job candidates has been recruited, the candidates must be screened, evaluated, selected, and placed in the positions that are open. The primary purpose of the applicants selection and placement information system is to assist human resource staff in these tasks.

Performance Management Information Systems

These include performance appraisal data and productivity information data. Data is frequently used as evidence in employee grievance matters. Careful documentation of employee performance and of how the performance was measured and reported is critical to acceptance of appraisal information in grievance hearings. Performance management information can lead to a number of decisions beyond merely supporting the operational decision to retain, promote, transfer or terminate a single employee.

Government Reporting and Compliance Information Systems

Government Reporting and Compliance Information Systems provide information needed both to maintain compliance with government regulations and to improve productivity and reduce costs associated with employees.

9.2 TACTICAL HUMAN RESOURCE INFORMATION SYSTEMS

Tactical information systems provide managers with support for decisions that emphasiSe the allocation of resources. Within the human resource management area, these decisions include recruitment decisions; job analysis and design decisions, training and development decisions, and employee compensation plan decisions.

Job Analysis and Design Information Systems

The information inputs to the job analysis and design information system include data from interviews with supervisors and workers and affirmative action guidelines. Inputs also include information from sources external to the firm, such as labour unions, competitors and government from sources external to the firm, such as labour unions, competitors, and government agencies. The outputs of the job analysis information system are job descriptions and job specifications. These outputs provide managers with the basis for many tactical human resource decisions.

Recruiting Information Systems

To direct the recruiting function, the organisation needs to develop a recruiting plan. The plan specifies the positions to be filled and the skills required of the employees for these positions. To develop the plan and to monitor its success, a recruiting information system is necessary to collect and process the many different types of information needed to construct the plan, including a list of unfilled positions; the duties and requirements of these positions; lists of planned employee retirements, transfers, or terminations; information about the skills and preferences of current employees; and summaries of employee appraisals. Other inputs to the recruiting plan include data about turnover rates and about the success of past placements.

Compensation and Benefits Information Systems

The Compensation and Benefits Information Systems may support a variety of tactical human resource decisions, especially when compensation and benefits information is related to information from internal and external sources. Compensation and benefit plans can play an important part in improving an organisation's productivity. Tying employee productivity to pay or encouraging increased productivity with incentive pay plans can often improve an organisation's productivity substantially.

Employee Training and Development Systems

The training offered by the employee training and development systems must meet the needs of jobs available in the organisation as identified through the position control system and the job analysis and design system. The training should also be directed at those persons interested and capable of benefiting from it, as identified by the skills inventory and human resource files.

9.3 STRATEGIC HUMAN RESOURCE IS

Information Systems Supporting Workforce Planning

Organisations involved in long-term strategic planning, such as those planning to expand into new market areas, construct factories or offices in new locations or add new products, will need information about the quantity and quality of the available workforce to achieve their goals. Information systems that support workforce planning serve this purpose.

Information Systems Supporting Labour Negotiations

Negotiating with craft, maintenance, office, and factory unions requires information gathered from many of the human resource information systems. The human resource team completing the

negotiating needs to be able to obtain numerous *ad hoc* reports that analyse the organisation's and union's positions within the framework of both the industry and the current economic situation. It is also important that the negotiating team be able to receive *ad hoc* reports on a very timely basis because additional questions and tactics will occur to the team while they are conducting labour negotiations.

Specialised Human Resource Information Systems Software

A great deal of software has been specifically designed for the human resource function. This software is available for all types and sizes of computers, including microcomputers. Software specifically designed for the human resource management function can be divided into two basic categories: comprehensive human resource information systems software and limited-function packages that support one or a few human resource activities.

Comprehensive Human Resource Information Systems Software

In the last few years, the software industry has produced several products that organise the various human resource information systems into integrated software referred to as human resource information systems(HRIS), software.

In general, the computerisation of HRIS has resulted in an integrated database of human resource files. Position files, employee files, skills inventory files, job analysis and design files, affirmative action files, occupational health and safety files, and many other human resource files are constructed in a coordinated manner using database management systems software so that application programmes can produce reports from any or all of the files. Thus, the human resource management director can produce reports listing likely internal candidates for open positions by running an application programme that queries position files job requirements files, and skills inventory files.

Limited-Function Human Resource Information Software

Numerous commercial software packages are sold for use on mainframes, minicomputers, and microcomputers that are designed to handle one or a small number of human resource functions. Microcomputer versions of these single-function software packages are relatively inexpensive and easy to operate and allow the human resource manager to automate a function quickly and easily.

Training Software

Many training software packages are available for all types and sizes of computers to provide on-line training for employees. They include:

- Management training software
- Sales training software
- Microcomputer training software
- Word processing training software

These software packages can be used in computer-based training programmes designed by the human resource department for training specific employees in-group and independent study programmes. Computer-based training aids often simplify the trainer's job and allow the trainer to individualize instruction more easily than in traditional, group-based training classes.

SUMMARY

Major business pressures include:

a) Technology
b) Market
c) Society

Some of the challenges that business systems pose are:

- Organisational challenges
- People challenges
- Technology challenges

Just-in-Time Systems

The just-in-Time (JIT) system is not a tactical information system, but a tactical approach to production. The purpose of the approach is to eliminate waste in the use of equipment, parts, space, workers' time, and materials, including the resources devoted to inventories.

Past Paper Analysis:

6/00, 12/00, 6/01, 6/02, 12/02, 6/03, 12/03, 6/04, 12/04, 6/06, 12/06, 6/07, 12/07

CHAPTER QUIZ

1. ..... uses today's computer technology to give customers the option of bypassing the time-consuming.
2. The ..... system is not a tactical information system, but a tactical approach to production.
3. Information technology (IT) refers to the technological aspect of information systems.

a. True
b. False

4. ..... packages provide a versatile tool for financial managers.
5. ..... are banks without bricks, they exist entirely on the Internet.

ANSWERS TO CHAPTER QUIZ

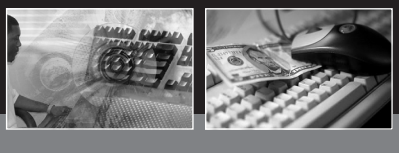
1. Online banking
2. Just-in-Time (JIT)
3. a. True
4. Spreadsheet software
5. Virtual bank

EXAM QUESTIONS

1. The objectives formulated by an organisation will be affected by a number of factors which will be particular to that organisation and its operations. Briefly describe FIVE dimensions that will impinge on an organisation when formulating its objectives.
2. An information system may be defined as a series of interrelated activities concerned with conversion of data to information. Briefly discuss an outline model of this conversion process.
3. The continuing development of technologies is increasingly revolutionising both data processing and management information system. Discuss the potential benefits and dangers from the increasing use of information technologies.
4. The entire decision making process can be viewed as the acquisition and processing information. List and briefly describe the stages in a decision making process.
5. It is commonly accepted model that organisational decision making has three levels. Briefly describe three levels of decision making, indicating the character of the decision made at each level, using examples where appropriate.

CHAPTER SIX

INFORMATION SYSTEMS SECURITY, LEGAL AND ETHICAL ISSUES



CHAPTER SIX

INFORMATION SYSTEMS SECURITY, LEGAL AND ETHICAL ISSUES

▶ OBJECTIVES

When you have completed this chapter, you should be able to:

1. Differentiate threats from hazards.
2. Identify the controls in a system at different levels.
3. Differentiate application controls from access controls.
4. Differentiate logical security from physical security
5. Describe the controls over the communication network.
6. Identify the environmental exposures and their controls
7. Appreciate threats represented by hacking and electronic eavesdropping.

▶ INTRODUCTION

There could be distinct controls for each separate resource, with separate identifiers for each user on each application. This will be determined in part by the relative sensitivity of the data and the resources, but this progressive approach can be difficult to manage and administer, with users having to remember different passwords, and probably being out of compassion with the underlying philosophy.

▶ DEFINITION OF KEY TERMS

Authorisation - Involves determining the access rights to various system objects/resources.

Data diddling involves changing data before or as it is being entered into the computer.

Trojan horses involve hiding malicious, fraudulent code in an authorised computer programme.

Viruses are malicious programme code inserted into other executable code that can self-replicate and spread from computer to computer.

Encryption is the process of converting a plaintext message into a secure coded form of text called cipher text.

Firewall - is a set of hardware and software equipment placed between an organisation's internal network and an external network to prevent outsiders from invading private networks.

▶ EXAM CONTEXT

Questions from this chapter are easy to point out. However, emphasis is normally put on the terms from this chapter. Therefore, the student will be required to have a clear understanding of the chapter's concepts as much as possible to comfortably attempt questions put across.

▶ INDUSTRY CONTEXT

Electronic voting systems for electorates have been in use since the 1960s when punch card systems debuted. Electronic voting technology can speed up the counting of ballots and can provide improved accessibility for disabled voters. However, there has been contention, especially in the United States, that electronic voting, especially DRE voting, could facilitate electoral fraud.

Fast Forward: Companies are yearning for a solution to guard their network from security risks such as external or untrusted users, and unmanaged endpoints on their internal LAN.

1. Definition of computer security – threats, hazards and controls

Information is a strategic resource and a significant portion of organisational budget is spent on managing information. A security system is a set of mechanisms and techniques that protect a computer system, specifically the assets. They are protected against loss or harm including unauthorised access, unauthorised disclosure and interference of information.

Assets can be categorised into:

- Resources – all instances of hardware, software, communication channels, operating environment, documentation and people
- Data – files, databases, messages in transit, etc.

A security attack is the act or attempt to exploit vulnerability in a system. Security controls are the mechanisms used to control an attack. Attacks can be classified into active and passive attacks.

- Passive attacks – attacker observes information without interfering with information or flow of information. He/she does not interfere with operation. Message content and message traffic is what is observed.

- Active attacks – involves more than message or information observation. There is interference of traffic or message flow and may involve modification, deletion or destruction. This may be done through the attacker masquerading or impersonating as another user. There is denial or repudiation where someone does something and denies later. This is a threat against authentication and to some extent integrity.

1.1 Security goals

To retain a competitive advantage and to meet basic business requirements, organisations must endeavour to achieve the following security goals:

- Confidentiality – protect information value and preserve the confidentiality of sensitive data. Information should not be disclosed without authorization. Information the release of which is permitted to a certain section of the public should be identified and protected against unauthorised disclosure.
- Integrity – ensure the accuracy and reliability of the information stored on the computer systems. Information has integrity if it reflects some real world situation or is consistent with real world situation. Information should not be altered without authorisation. Hardware designed to perform some functions has lost integrity if it does not perform those functions correctly. Software has lost integrity if it does not perform according to its specifications. Communication channels should relay messages in a secure manner to ensure that integrity. People should ensure the system functions according to the specifications.
- Availability – ensure the continued availability of the information system and all its assets to legitimate users at an acceptable level of service or quality of service. Any event that degrades performance or quality of a system affects availability
- Ensure conformity to laws, regulations and standards.

1.2 Hazards (exposures) to information security

An exposure is a form of possible loss or harm. Examples of exposures include:

- Unauthorised access resulting in a loss of computing time
- Unauthorised disclosure – information revealed without authorisation
- Destruction, especially with respect to hardware and software
- Theft
- Interference with system operation.

1.3 Threats to information security

These are circumstances that have potential to cause loss or harm i.e. circumstances that have

a potential to bring about exposures.

- Human error
- Disgruntled employees
- Dishonest employees
- Greedy employees who sell information for financial gain
- Outsider access – hackers, crackers, criminals, terrorists, consultants, ex-consultants, ex-employees, competitors, government agencies, spies (industrial, military etc), disgruntled customers
- Acts of God/natural disasters – earthquakes, floods, hurricanes
- Foreign intelligence
- Accidents, fires, explosion
- Equipment failure
- Utility outage
- Water leaks, toxic spills
- Viruses – these are programmed threats

1.4 Vulnerability

A vulnerability is a weakness within the system that can potentially lead to loss or harm. The threat of natural disasters has instances that can make the system vulnerable. If a system has programmes that have threats (erroneous programmes) then the system is vulnerable.

1.5 Security controls

These include:

1. Administrative controls – they include
   a. Policies – a policy can be seen as a mechanism for controlling security
   b. Administrative procedures – may be put in place by an organization to ensure that users only do that which they have been authorised to do
   c. Legal provisions – serve as security controls and discourage some form of physical threats
   d. Ethics
2. Logical security controls – measures incorporated within the system to provide protection from adversaries who have already gained physical access
3. Physical controls – any mechanism that has a physical form e.g. lockups
4. Environmental controls

1.6 Administering security

- Risk analysis
- Security planning – a security plan identifies and organises the security activities of an organisation.
- Security policy

Risk analysis

The process involves:

- Identification of the assets
- Determination of the vulnerabilities
- Estimate the likelihood of exploitation
- Computation of expected annual loss
- Survey of applicable controls and their costs
- Projection of annual savings

Security policy

Security failures can be costly to business. Losses may be suffered as a result of the failure itself or costs can be incurred when recovering from the incident, followed by more costs to secure systems and prevent further failure. A well-defined set of security policies and procedures can prevent losses and save money.

The information systems security policy is the responsibility of top management of an organisation who delegate its implementation to the appropriate level of management with permanent control. The policy contributes to the protection of information assets. Its objective is to protect the information capital against all types of risks, accidental or intentional. An existing and enforced security policy should ensure systems conformity with laws and regulations, integrity of data, confidentiality and availability.

Key components of such a policy include the following:

- Management support and commitment – management should approve and support formal security awareness and training.
- Access philosophy – access to computerised information should be based on a documented 'need-to-know, need-to-do' basis.
- Compliance with relevant legislation and regulations
- Access authorisation – the data owner or manager responsible for the accurate use and reporting of the information should provide written authorisation for users to gain access to computerized information.
- Reviews of access authorisation – like any other control, access controls should be evaluated regularly to ensure they are still effective.
- Security awareness – all employees, including management, need to be made aware on a regular basis of the importance of security. A number of different mechanisms are available for raising security awareness including:
  - Distribution of a written security policy.
  - Training on a regular basis of new employees, users and support staff.
  - Non-disclosure statements signed by employees.
  - Use of different media in promulgating security e.g. company newsletter, web page, videos, etc.
  - Visible enforcement of security rules.
  - Simulate security incidents for improving security procedures.
  - Reward employees who report suspicious events.
    Periodic audits.

2. Security in the application level: Application controls

Application controls are controls over input, processing and output functions. Application controls include methods for ensuring that:

- Only complete, accurate and valid data is entered and updated in a computer system.
- Processing accomplishes the correct task.
- Processing results meet expectations.
- Data is maintained.

These controls may consist of edit tests, totals, reconciliations and identification and reporting of incorrect, missing or exception data. Automated controls should be coupled with manual procedures to ensure proper investigation of exceptions.

2.1 Input/origination controls

Input control procedures must ensure that every transaction to be processed is received, processed and recorded accurately and completely. These controls should ensure that only valid and authorised information is input and that these transactions are processed only once. In an integrated systems environment, output generated by one system is the input for another system, therefore, the edit checks, validations and access controls of the system generating the output must be reviewed as input/origination controls.

Input authorisation

Input authorization verifies that all transactions have been authorised and approved by management. Authorisation of input helps ensure that only authorized data is entered into the computer system for processing by applications. Authorisation can be performed online at the time when the data is entered into the system. A computer-generated report listing the items requiring manual authorization also may be generated. It is important that controls exist throughout processing to ensure that authorised data remains unchanged. This can be accomplished through various accuracy and completeness checks incorporated into an application's design.

Types of authorisation include:

- Signatures on batch forms provide evidence of proper authorization.
- Online access controls ensure that only authorised individuals may access data or perform sensitive functions
- Unique passwords are necessary to ensure that access authorisation cannot be compromised through use of another individual's authorised data access. Individual passwords also provide accountability for data changes.
- Terminal identification can be used to limit input to specific terminals as well as to individuals. Terminals can be equipped with hardware that transmits a unique identification such as a serial number that is authenticated by the system.

- Source documents are the forms used to record data. A source document may be a piece of paper, a turnaround document or an image displayed for online data input. A well-designed source document achieves several purposes. It increases the speed and accuracy with which data can be recorded, controls work flow, facilitates the preparation of the data in machine readable form for pattern recognition devices, increases the speed and accuracy with which data can be read and facilitates subsequent reference checking.

Batch controls and balancing

Batch controls group input transactions in order to provide control totals. The batch control can be based on total monetary amount, total items and total documents.

Batch header forms are a data preparation control. All input forms should be clearly identified with the application name and transaction codes. Where possible, pre-printed and pre-numbered forms with transaction identification codes and other constant data items are recommended. This would help ensure that all pertinent data has been recorded on the input forms and can reduce data recording/entry errors.

Types of batch controls include:

- Total monetary amount – verification that the total monetary amount value of items processed equals the total monetary value of the batch documents. For example, the total monetary value of the sales invoices in the batch agrees with the total monetary values of the sales invoices processed.
- Total items – verification that the total number of items included on each document in the batch agrees to the total number of items processed. For example, the total number of units ordered in the batch of invoices agrees with the total number of units processed.
- Total documents – verification that the total number of documents in the batch equals the total number of documents processed. For example, the total number of invoices in a batch agrees with the total number of invoices processed.
- Hash totals – verification that a predetermined numeric field existing for all documents in a batch agrees with the total of documents processed.

Types of batch balancing include:

- Batch registers – these registers enable manual recording of batch totals
- Control accounts – control account use is performed through the use of an initial edit file to determine batch totals. The data are then processed to the master file and reconciliation is performed between the totals processed during the initial edit file and the master file.
- Computer agreement – computer agreement with batch totals is performed through the use of batch header slips that record the batch total.

Input error reporting and handling

Input processing requires that controls be identified to verify that data are accepted into the system correctly, and that input errors are recognised and corrected.

Data conversion error corrections are needed during the data conversion process. Errors can occur due to duplication of transactions and inaccurate data entry. These errors can, in turn, negatively impact on the completeness and accuracy of the data. Corrections to data should be processed through the normal data conversion process and should be verified, authorised and re-entered to the system as a part of normal processing.

Input error handling can be processed by:

- Rejecting only transactions with errors – only transactions containing errors would be rejected; the rest of the batch would be processed.
- Rejecting the whole batch of transactions – any batch containing errors would be rejected for correction prior to processing.
- Accepting batch in suspense – any batches containing errors would not be rejected; however, the batch would be posted to suspense pending correction.
- Accepting batch and flagging error transactions – any batch containing errors would be processed; however, those transactions containing error would be flagged for identification enabling subsequent errors correction.

Input control techniques include:

- Transaction log – contains a detailed list of all updates. The log can be either manually maintained or provided through automatic computer logging.
- Reconciliation of data – controls are needed to ensure that all data received are recorded and properly processed.
- Documentation of user, data entry and data control procedures
- Error correction procedures
  - Logging of errors
  - Timely corrections
  - Upstream resubmission
  - Approval of corrections
  - Suspense file
  - Error file
  - Validity of corrections
- Anticipation – the user anticipates the receipt of data
- Transmittal log – this log documents transmission or receipt of data
- Cancellation of source documents – procedures to cancel source documents, for example, by punching with holes or mark, to avoid duplicate entry

Online integrity in online or database systems

Online systems also require control over input. Batches may be established by time of day, specific terminal or individual inputting the data. A supervisor should then review the online batch and release it to the system for processing. This method is preferred over review of the output by the same person preparing the input.

2.2 Processing, validation and editing

Data validation and editing

Procedures should be established to ensure that input data is validated and edited as close to the point of origination as possible. Preprogrammed input formats ensure that data is input to the

correct field in the correct format. If input procedures allow supervisor overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log.

Data validation identifies data errors, incomplete or missing data and inconsistencies among related data items. Front-end data editing and validation can be performed if intelligent terminals are used.

Edit controls are preventative controls that are used in a programme before data is processed. If the edit control is not in place or does not work correctly; the preventative control measures do not work effectively. This may cause processing of inaccurate data.

Data validation edits include:

- Sequence check – the control number follows sequentially and any control number out of sequence or duplicated are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoices begin with 12001 and end with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.
- Limit check – data should not exceed a predetermined amount. For example payroll checks should not exceed 4,000.00. If a check exceeds 4,000.00, the data would be rejected for further verification/authorization.
- Range check – data should be within a predetermined range of values. For example, product type codes range from 100 to 250. Any code outside this range should be rejected as an invalid product type.
- Validity check – programmed checking of the data validity in accordance with predetermined criteria. For example, a payroll record contains a field for marital status; the acceptable status codes are M or S. If any other code is entered the record should be rejected.
- Reasonableness check – input data is matched to predetermined reasonable limits or occurrence rates. For example, in most instances, a bakery usually receives orders for no more than 20 crates. If an order for more than 20 crates is received, the computer programme should be designed to print the record with a warning indicating that the order appears unreasonable.
- Table look-ups – input data complies with predetermined criteria maintained in a computerized table of possible values. For example, the input clerk enters a city code of 1 to 10. This number corresponds with a computerised table that matches the code to a city name.
- Existence check – data is entered correctly and agrees with valid predetermined criteria. For example, a valid transaction code must be entered in the transaction code field.
- Key verification – keying-in process is repeated by a separate individual using a machine that compares original keystrokes to the repeated keyed input. For example, the worker number is keyed in twice and compared to verify the keying process.
- Check digit – a numeric value that has been calculated mathematically is added to data to ensure that the original data have not been altered or an incorrect but valid value submitted. This control is effective in detecting transposition and transcription errors. For example, a check digit is added to an account number so it can be checked for accuracy when it is used.
- Completeness check – a field should always contain data and not zeros or blanks.

A check of each byte of that field should be performed to determine that some form of data, not blanks or zeros, are present. For example, a worker number on a new employee record is left blank. This is identified as a key field and the record would be rejected, with a request that the field is completed before the record is accepted for processing.

- Duplicate check – new transactions are matched to those previously input to ensure that they have not already been entered. For example, a vendor invoice number agrees with previously recorded invoices to ensure that the current order is not a duplicate and therefore, the vendor will not be paid twice.
- Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationships may be required to be true and consider the input valid. For example, the date of engagement of an employee may be required to be more than 16 years past his or her date of birth.

Processing control procedures

Processing controls ensure the completeness and accuracy of accumulated data. They ensure that data on a file/database remains complete and accurate until changed as a result of authorized processing or modification routines. The following are processing control techniques that can be used to address the issues of completeness and accuracy of accumulated data.

- Manual recalculations – a sample of transactions may be recalculated manually to ensure that processing is accomplishing the anticipated task.
- Editing – an edit check is a programme instruction or subroutine that tests for accurate, complete and valid input and updates in an application.
- Run-to-run totals – These totals provide the ability to verify data values through the stages of application processing. Run-to-run total verification ensures that data read into the computer was accepted and then applied to the updating process.
- Programmed controls – software can be used to detect and initiate corrective action for errors in data and processing. For example, if the incorrect file or file version is provided for processing, the application programme could display messages instructing that the proper file and version be used.
- Reasonableness verification of calculated amounts – application programmes can verify the reasonableness of calculated amounts. The reasonableness can be tested to ensure appropriateness to predetermined criteria. Any transaction that is determined to be unreasonable may be rejected pending further review.
- Limit checks on calculated amounts – an edit check can provide assurance through the use of predetermined limits that calculated amounts have not been keyed in correctly. Any transaction exceeding the limit may be rejected for further investigation.
- Reconciliation of file totals – reconciliation of file totals should be performed on a routine basis. Reconciliation may be performed through use of a manually maintained account, a file control record or an independent control file.
- Exception reports – an exception report is generated by a programme that identifies transactions or data that appear to be incorrect. These items may be outside a predetermined range or may not conform to specified criteria.

Data file control procedures

File controls should ensure that only authorised processing occurs to stored data. Types of controls over data files are:

- Before and after image reporting – computer data on a file prior to and after a transaction is processed can be recorded and reported. The before and after image makes it possible to trace the impact transactions have on computer records.
- Maintenance error reporting and handling – control procedures should be in place to ensure that all error reports are properly reconciled and corrections are submitted on a timely basis. To ensure segregation of duties, error corrections should be properly reviewed and authorised by personnel who did not initiate the transaction.
- Source documentation retention – source documentation should be retained for an adequate time period to enable retrieval, reconstruction or verification of data. Policies regarding the retention of source documentation should be enforced. Originating departments should maintain copies of source documentation and ensure that only authorised personnel have access. When appropriate, source documentation should be destroyed in a secure, controlled environment.
- Internal and external labelling – internal and external labelling of removable storage media is imperative to ensure that the proper data is loaded for processing. External labels provide the basic level of assurance that the correct data medium is loaded for processing. Internal labels, including file header records, provide assurance that the proper data files are used and allow for automated checking.
- Version usage – it is critical that the proper version of a file, such as date and time of data, be used as well as the correct file in order for the processing to be correct. For example, transactions should be applied to the most current database while restart procedures should use earlier versions.
- Data file security – data file security controls prevent unauthorised users that may have access to the application to alter data files. These controls do not provide assurances relating to the validity of data, but ensure that unauthorised users who may have access to the application cannot improperly alter stored data.
- One-for-one checking – individual documents agree with a detailed listing of documents processed by the computer. It is necessary to ensure that all documents have been received for processing.
- Pre-recorded input – certain information fields are pre-printed on blank input forms to reduce initial input errors.
- Transaction logs – all transaction input activity is recorded by the computer. A detailed listing including date of input, time of input, user ID and terminal location can then be generated to provide an audit trail. It also permits operations personnel to determine which transactions have been posted. This will help to decrease the research time needed to investigate exceptions and decrease recovery time if a system failure occurs.
- File updating and maintenance authorisation – proper authorisation for file updating and maintenance is necessary to ensure that stored data are adequately safeguarded, correct and up-to-date. Application programmes may contain access restrictions in addition to overall system access restrictions. The additional security may provide levels of authorization in addition to providing an audit trail of file maintenance.
- Parity checking – data transfers in a computer system are expected to be made in a relatively error-free environment. However, when programmes or vital data are transmitted, additional controls are needed. Transmission errors are controlled primarily by error detecting or correcting codes. The former is used more often because error-correcting codes are costly to implement and are unable to correct all errors.

2.3 Output controls

Output controls provide assurance that the data delivered to users will be presented, formatted and delivered in a consistent and secure manner. Output controls include the following:

- Logging and storage of negotiable, sensitive and critical forms in a secure place – negotiable, sensitive or critical forms should be properly logged and secured to provide adequate safeguards against theft or damage. The form log should be routinely reconciled to inventory on hand and any discrepancies should be properly researched.
- Computer generation of negotiable instruments, forms and signatures – the computer generation of negotiable instruments, forms and signatures should be properly controlled. A detailed listing of generated forms should be compared to the physical forms received. All exceptions, rejections and mutilations should be accounted for properly.
- Report distribution – output reports should be distributed according to authorised distribution parameters, which may be automated, or manual. Operations personnel should verify that output reports are complete and that they are delivered according to schedule. All reports should be logged prior to distribution.

In most environments, processing output is spooled to a buffer or print spool upon completion of job processing where it waits for an available printer. Controls over access to the print spools are important to prevent reports from being accidentally deleted from print spools or directed to a different printer. In addition, changes to the output print priority can delay printing of critical jobs.

Access to distributed reports can compromise confidentiality. Therefore, physical distribution of reports should be adequately controlled. Reports containing sensitive data should be printed under secured, controlled conditions. Secured output drop-off points should be established.

Output disposal also should be adequately secured to ensure that no unauthorised access may occur. Also to be considered are reports that are distributed electronically through the computer system. Logical access to these reports also should be carefully controlled and subject to authorisation:

- Balancing and reconciling – data processing application programme output should be routinely balanced to the control totals. Audit trails should be provided to facilitate the tracking of transaction processing and the reconciliation of data.
- Output error handling – procedures for reporting and controlling errors contained in the application programme output should be established. The error report should be timely and delivered to the originating department for review and error correction.
- Output report retention – a record retention schedule should be firmly adhered to. Any governing legal regulations should be included in the retention policy.
- Verification of receipt of reports – to provide assurance that sensitive reports are properly distributed, the recipient should sign a log as an evidence receipt of output.

2.4 Data integrity testing

Data integrity testing is a series of substantive tests that examines accuracy, completeness, consistency and authorisation of data holdings. It employs testing similar to that used for input

control. Data integrity tests will indicate failures in input or processing controls. Controls for ensuring the integrity of accumulated data on a file can be exercised by checking data on the file regularly. When this checking is done against authorised source documentation, it is usual to check only a portion of the file at a time. Since the whole file is regularly checked in cycles, the control technique is often referred to as cyclical checking. Data integrity issues can be identified as data that conform to the following definitions:

(i) Domain integrity – this testing is really aimed at verifying that the data conform to definitions, that is, that the data items are all in the correct domains. The major objective of this exercise is to verify that edit and validation routines are working satisfactorily. These tests are field level based and ensure that the data item has a legitimate value in the correct range or set.

(ii) Relational integrity – these tests are performed at the record based level and usually involve calculating and verifying various calculated fields such as control totals. Examples of their use would be in checking aspects such as payroll calculations or interest payments. Computerised data frequently have control totals built into various fields and by the nature of these fields, they are computed and would be subject to the same type of tests. These tests will also detect direct modification of sensitive data i.e. if someone has bypassed application programmes, as these types of data are often protected with control totals.

(iii) Referential integrity – database software will sometimes offer various procedures for checking or ensuring referential integrity (mainly offered with hierarchical and network-based databases). Referential integrity checks involve ensuring that all references to a primary key from another file (called foreign key) actually exist in their original file. In non-pointer databases e.g. relational databases, referential integrity checks involve making sure that all foreign keys exist in their original table.

3. Security in operating system: Access control security function

This is a function implemented at the operating system level and usually also availed at the application level by the operating system. It controls access to the system and system resources so that only authorised accesses are allowed, e.g.

- Protect the system from access by intruders
- Protect system resources from unauthorised access by otherwise legitimate system user
- Protect each user from inadvertent or malicious interference from another

It is a form of logical access control, which involves protection of resources from users who have physical access to the computer system.

The access control reference monitor model has a reference monitor, which intercepts all access attempts. It is always invoked when the target object is referenced and decides whether to deny or grant requests as per the rules incorporated within the monitor.

The components of an access control system can be categorised into identification, authentication and authorisation components. Typical operating system based access control mechanisms are:

- User identification and authentication
- Access control to the systems general objects e.g. files and devices
- Memory protection – prevent one programme from interfering with another i.e. any form of unauthorised access to another programme's memory space.

3.1 Identification

Involves establishing identity of the subject (who are you?). Identification can use:

- Identity, full name
- Workstation ID, IP address
- Magnetic card (requires a reader)
- Smart card (inbuilt intelligence and computation capability)

Biometrics is the identification based on unique physical or behavioural patterns of people and may be:

- Physiological systems – something you are e.g. fingerprints
- Behavioural systems – how you work

They are quite effective when thresholds are sensible (substantial difference between two different people) and physical conditions of person are normal (equal to the time when reference was first made). They require expensive equipment and are rare. Also buyers are deterred by impersonation or belief that devices will be difficult to use. In addition, users dislike being measured.

3.2 Authentication

Involves verification of identity of subject (Are you who you say you are? Prove it!). Personal authentication may involve:

- Something you know: password, PIN, code phrase
- Something you have: keys, tokens, cards, smart cards
- Something you are: fingerprints, retina patterns, voice patterns
- The way you work: handwriting (signature), keystroke patterns
- Something you know: question about your background, favourite colour, pet name, etc.

3.3 Authorisation

Involves determining the access rights to various system objects/resources. The security requirement to be addressed is the protection against unauthorised access to system resources. There is need to define an authorisation policy as well as implementation mechanisms. An authorisation policy defines activities permitted or prohibited within the system. Authorisation

mechanisms implement the authorisation policy and includes directory of access rights, access control lists (ACL) and access tickets or capabilities.

4. Logical security

Logical access into the computer can be gained through several avenues. Each avenue is subject to appropriate levels of access security. Methods of access include the following:

1. Operator console – these are privileged computer terminals, which controls most computer operations and functions. To provide security, these terminals should be located in a suitably controlled location so that physical access can only be gained by authorised personnel. Most operator consoles do not have strong logical access controls and provide a high level of computer system access; therefore, the terminal must be located in a physically secured area.
2. Online terminals – online access to computer systems through terminals typically require entry of at least a logon-identifier (logon-ID) and a password to gain access to the host computer system and may also require further entry of authentication data for access to application specific systems. Separate security and access control software may be employed on larger systems to improve the security provided by the operating system or application system.
3. Batch job processing – this mode of access is indirect since access is achieved via processing of transactions. It generally involves accumulating input transactions and processing them as a batch after a given interval of time or after a certain number of transactions have been accumulated. Security is achieved by restricting who can accumulate transactions (data entry clerks) and who can initiate batch processing (computer operators or the automatic job scheduling system).
4. Dial-up ports – use of dial-up ports involves hooking a remote terminal or PC to a telephone line and gaining access to the computer by dialling a telephone number that is directly or indirectly connected to the computer. Often a modem must interface between the remote terminal and the telephone line to encode and decode transmissions. Security is achieved by providing a means of identifying the remote user to determine authorisation to access. This may be a dial-back line, use of logon-ID and access control software or may require a computer operator to verify the identity of the caller and then provide the connection to the computer.
5. Telecommunications network – telecommunications networks link a number of computer terminals or PCs to the host computer through a network of telecommunications lines. The lines can be private (i.e. dedicated to one user) or public such as a nation's telephone system. Security should be provided in the same manner as that applied to online terminals.

4.1 Logical access issues and exposures

Inadequate logical access controls increase an organisation's potential for losses resulting from exposures. These exposures can result in minor inconveniences or total shutdown of computer functions. Logical access controls reduce exposure to unauthorised alteration and manipulation

of data and programmes. Exposures that exist from accidental or intentional exploitation of logical access control weaknesses include technical exposures and computer crime.

Technical exposures

This is the unauthorised (intentional or unauthorised) implementation or modification of data and software.

1. **Data diddling** involves changing data before or as it is being entered into the computer. This is one of the most common abuses because it requires limited technical knowledge and occurs before computer security can protect data.
2. **Trojan horses** involve hiding malicious, fraudulent code in an authorized computer programme. This hidden code will be executed whenever the authorised programme is executed. A classic example is the Trojan horse in the payroll-calculating programme that shaves a barely noticeable amount off each paycheck and credits it to the perpetrator's payroll account.
3. **Rounding down** involves drawing off small amounts of money from a computerised transaction or account and rerouting this amount to the perpetrator's account. The term 'rounding down' refers to rounding small fractions of a denomination down and transferring these small fractions into the unauthorised account. Since the amounts are so small, they are rarely noticed.
4. **Salami techniques** involve the slicing of small amounts of money from a computerised transaction or account and are similar to the rounding down technique. The difference between them is that in rounding down the programme rounds off by the cent. For example, if a transaction amount was 234.39 the rounding down technique may round the transaction to 234.35. The salami technique truncates the last few digits from the transaction amount so 234.39 become 234.30 or 234.00 depending on the calculation built into the programme.
5. **Viruses** are malicious programme code inserted into other executable code that can self-replicate and spread from computer to computer, via sharing of computer diskettes, transfer of logic over telecommunication lines or direct contact with an infected machine or code. A virus can harmlessly display cute messages on computer terminals, dangerously erase or alter computer files or simply fill computer memory with junk to a point where the computer can no longer function. An added danger is that a virus may lie dormant for some time until triggered by a certain event or occurrence, such as a date (1 January – Happy New Year!) or being copied a pre-specified number of times. During this time the virus has silently been spreading.
6. **Worms** are destructive programmes that may destroy data or utilise tremendous computer and communication resources but do not replicate like viruses. Such programmes do not change other programs, but can run independently and travel from machine to a machine across network connections. Worms may also have portions of themselves running on many different machines.
7. **Logic bombs** are similar to computer viruses, but they do not self-replicate. The creation of logic bombs requires some specialised knowledge, as it involves programming the destruction or modification of data at a specific time in the future. However, unlike viruses or worms, logic bombs are very difficult to detect before they blow up; thus, of all the computer crime schemes, they have the greatest potential for damage. Detonation can be timed to cause maximum damage and to take place long after the departure of the perpetrator. The logic bomb may also be used as a tool of extortion, with a ransom being demanded in exchange for disclosure of the location of the bomb.

8. **Trap doors** are exits out of an authorised programme that allow insertion of specific logic, such as programme interrupts, to permit a review of data during processing. These holes also permit insertion of unauthorised logic.
9. **Asynchronous attacks** occur in multiprocessing environments where data move asynchronously (one character at a time with a start and stop signal) across telecommunication lines. As a result, numerous data transmissions must wait for the line to be free (and flowing in the proper direction) before being transmitted. Data that is waiting is susceptible to unauthorized accesses called asynchronous attacks. These attacks, which are usually very small pinlike insertions into cable, may be committed via hardware and are extremely hard to detect.
10. **Data leakage** involves siphoning or leaking information out of the computer. This can involve dumping files to paper or can be as simple as stealing computer reports and tapes.
11. **Wire-tapping** involves eavesdropping on information being transmitted over telecommunications lines.
12. **Piggybacking** is the act of following an authorised person through a secured door or electronically attaching to an authorised telecommunication link to intercept and possibly alter transmissions.
13. **Shut down of the computer** can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up lines) to the computer. Only individuals knowing a high-level systems logon-ID can usually initiate the shut down process. This security measure is effective only if proper security access controls are in place for the high-level logon-ID and the telecommunications connections into the computer. Some systems have proven to be vulnerable to shutting themselves down under certain conditions of overload.
14. **Denial of service** is an attack that disrupts or completely denies service to legitimate users, networks, systems or other resources. The intent of any such attack is usually malicious in nature and often takes little skill because the requisite tools are readily available.

STUDY TEXT

Viruses

Fast Forward: A **computer virus** is a computer program that can copy itself and infect a computer without the permission or knowledge of the user.

Viruses are a significant and a very real logical access issue. The term virus is a generic term applied to a variety of malicious computer programmes. Traditional viruses attach themselves to other executable code, infect the user's computer, replicate themselves on the user's hard disk and then damage data, hard disk or files. Viruses usually attack four parts of the computer:

- Executable programme files
- File-directory system that tracks the location of all the computer's files
- Boot and system areas that are needed to start the computer
- Data files

Control over viruses

Computer viruses are a threat to computers of any type. Their effects can range from the annoying but harmless prank to damaged files and crashed networks. In today's environment, networks are the ideal way to propagate viruses through a system. The greatest risk is from electronic mail

(e-mail) attachments from friends and/or anonymous people through the Internet. There are two major ways to prevent and detect viruses that infect computers and network systems.

- Having sound policies and procedures in place
- Technical means, including anti-virus software

Policies and procedures

Some of the policy and procedure controls that should be in place are:

- Build any system from original, clean master copies. Boot only from original diskettes whose write protection has always been in place.
- Allow no disk to be used until it has been scanned on a stand-alone machine that is used for no other purpose and is not connected to the network.
- Update virus software scanning definitions frequently.
- Write-protect all diskettes with .EXE or .COM extensions.
- Have vendors run demonstrations on their machines, not yours.
- Enforce a rule of not using shareware without first scanning the shareware thoroughly for a virus.
- Commercial software is occasionally supplied with a Trojan horse (viruses or worms). Scan before any new software is installed.
- Insist that field technicians scan their disks on a test machine before they use any of their disks on the system.
- Ensure that the network administrator uses workstation and server anti-virus software.
- Ensure that all servers are equipped with an activated current release of the virus detection software.
- Create a special master boot record that makes the hard disk inaccessible when booting from a diskette or CD-ROM. This ensures that the hard disk cannot be contaminated by the diskette or optical media.
- Consider encrypting files and then decrypt them before execution.
- Ensure that bridge, route and gateway updates are authentic. This is a very easy way to place and hide a Trojan horse.
- Backups are a vital element of anti-virus strategy. Be sure to have a sound and effective backup plan in place. This plan should account for scanning selected backup files for virus infection once a virus has been detected.
- Educate users so they will heed these policies and procedures.
- Review anti-virus policies and procedures at least once a year.
- Prepare a virus eradication procedure and identify a contact person.

Technical means

Technical methods of preventing viruses can be implemented through hardware and software means.

The following are hardware tactics that can reduce the risk of infection:

- Use workstations without floppy disks
- Use boot virus protection (i.e. built-in firmware based virus protection)
- Use remote booting
- Use a hardware based password
- Use write protected tabs on floppy disks

Software is by far the most common anti-virus tool. Anti-virus software should primarily be used

as a preventative control. Unless updated periodically, anti-virus software will not be an effective tool against viruses.

The best way to protect the computer against viruses is to use anti-viral software. There are several kinds. Two types of scanners are available:

- One checks to see if your computer has any files that have been infected with known viruses
- The other checks for atypical instructions (such as instructions to modify operating system files) and prevents completion of the instruction until the user has verified that it is legitimate.

Once a virus has been detected, an eradication programme can be used to wipe the virus from the hard disk. Sometimes eradication programmes can kill the virus without having to delete the infected programme or data file, while other times those infected files must be deleted. Still other programmes, sometimes called inoculators, will not allow a programme to be run if it contains a virus.

There are three different types of anti-virus software:

a) **Scanners** look for sequence of bits called signatures that are typical of virus programmes. Scanners examine memory, disk boot sectors, executables and command files for bit patterns that match a known virus. Scanners, therefore, need to be updated periodically to remain effective.

b) **Active monitors** interpret DOS and ROM basic input-output (BIOS) calls, looking for virus like actions. Active monitors can be annoying because they cannot distinguish between a user request and a programme or virus request. As a result, users are asked to confirm actions like formatting a disk or deleting a file or set of files.

c) **Integrity checkers** compute a binary number on a known virus-free programme that is then stored in a database file. The number is called a cyclical redundancy check (CRC). When that programme is called to execute, the checker computes the CRC on the programme about to be executed and compares it to the number in the database. A match means no infection; a mismatch means that a change in the programme has occurred. A change in the programme could mean a virus within it. Integrity checkers take advantage of the fact that executable programmes and boot sectors do not change very often, if at all.

Computer crime exposures

Fast Forward: Computer crime encompasses a broad range of potentially illegal activities.

Computer systems can be used to steal money, goods, software or corporate information. Crimes also can be committed when the computer application process or data are manipulated to accept false or unauthorised transactions. There also is the simple, non-technical method of computer crime by stealing computer equipment.

Computer crime can be performed with absolutely nothing physically being taken or stolen. Simply viewing computerised data can provide an offender with enough intelligence to steal ideas or confidential information (intellectual property).

Committing crimes that exploit the computer and the information it contains can be damaging to

the reputation, morale and very existence of an organisation. Loss of customers, embarrassment to management and legal actions against the organisation can be a result.

Threats to business include the following:

- **Financial loss –** these losses can be direct, through loss of electronic funds or indirect, through the costs of correcting the exposure.

- **Legal repercussions –** there are numerous privacy and human rights laws an organisation should consider when developing security policies and procedures. These laws can protect the organisation but can also protect the perpetrator from prosecution. In addition, not having proper security measures could expose the organisation to lawsuits from investors and insurers if a significant loss occurs from a security violation. Most companies also must comply with industry-specific regulatory agencies.

- **Loss of credibility or competitive edge –** many organisations, especially service firms such as banks, savings and loans and investment firms, need credibility and public trust to maintain a competitive edge. A security violation can severely damage this credibility, resulting in loss of business and prestige.

- **Blackmail/Industrial espionage –** by gaining access to confidential information or the means to adversely impact computer operations, a perpetrator can extort payments or services from an organisation by threatening to exploit the security breach.

- **Disclosure of confidential, sensitive or embarrassing information –** such events can damage an organisation's credibility and its means of conducting business. Legal or regulatory actions against the company may also be the result of disclosure.

- **Sabotage –** some perpetrators are not looking for financial gain. They merely want to cause damage due to dislike of the organisation or for self-gratification.

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.

a) Hackers – hackers are typically attempting to test the limits of access restrictions to prove their ability to overcome the obstacles. They usually do not access a computer with the intent of destruction; however, this is quite often the result.
b) Employees – both authorised and unauthorised employees
c) Information system personnel – these individuals have the easiest access to computerised information since they are the custodians of this information. In addition to logical access controls, good segregation of duties and supervision help reduce logical access violations by these individuals.
d) End users
e) Former employees
f) Interested or educated outsiders
   - Competitors
   - Foreigners
   - Organised criminals
   - Crackers (hackers paid by a third party)
   - Phreackers (hackers attempting access into the telephone/communication

system)
- Part-time and temporary personnel – remember that office cleaners often have a great deal of physical access and may well be competent in computing
- Vendors and consultants
- Accidental ignorant – someone who unknowingly perpetrates a violation

4.2 Access control software

Access control software is designed to prevent unauthorised access to data, use of system functions and programmes, unauthorised updates/changes to data and to detect or prevent an unauthorized attempt to access computer resources. Access control software interfaces with the operating system and acts as a central control for all security decisions. The access control software functions under the operating system software and provides the capability of restricting access to data processing resources either online or in batch processing.

Access control software generally performs the following tasks:

- Verification of the user
- Authorisation of access to defined resources
- Restriction of users to specific terminals
- Reports on unauthorised attempts to access computer resources, data or programmes

Access control software generally processes access requests in the following way:

- Identification of users – users must identify themselves to the access control software such as name and account number
- Authentication – users must prove that they are who they claim to be. Authentication is a two way process where the software must first verify the validity of the user and then proceed to verify prior knowledge information. For example, users may provide information on:
  - Name, account number and password
  - Objects such as badge, plastic cards and key
  - Personal characteristics such as fingerprint, voice and signature

4.3 Logical security features, tools and procedures

1) Logon-IDs and passwords

This two-phase user identification/authentication process based on something you know can be used to restrict access to computerised information, transactions, programmes and system software. The computer can maintain an internal list of valid logon-IDs and a corresponding set of access rules for each logon-ID. These access rules identify the computer resources the user of the logon-ID can access and constitute the user's authorisation.

The logon-ID provides individual's identification and each user gets a unique logon-ID that can be identified by the system. The format of logon-Ids is typically standardized. The password provide individual' authentication. Identification/authentication is a two-step process by which the computer system first verifies that the user has a valid logon-ID (user identification) and then requires the user to substantiate his/her validity via a password.

>> Features of passwords

- A password should be easy to remember but difficult for a perpetrator to guess.
- Initial password assignment should be done discreetly by the security administrator. When the user logs on for the first time, the system should force a password change to improve confidentiality. Initial password assignments should be randomly generated and assigned where possible on an individual and not a group basis. Accounts never used with or without an initial password should be removed from the system.
- If the wrong password is entered a predefined number of times, typically three, the logon-ID should be automatically and permanently deactivated (or at least for a significant period of time).
- If a logon-ID has been deactivated because of a forgotten password, the user should notify the security administrator. The administrator should then reactivate the logon-ID only after verifying the user's identification.
- Passwords should be internally one-way encrypted. Encryption is a means of encoding data stored in a computer. This reduces the risk of a perpetrator gaining access to other users' passwords (if the perpetrator cannot read and understand it, he cannot use it).
- Passwords should not be displayed in any form either on a computer screen when entered, on computer reports, in index or card files or written on pieces of paper taped inside a person's desk. These are the first places a potential perpetrator will look.
- Passwords should be changed periodically. The best method is for the computer system to force the change by notifying the user prior to the password expiration date.
- Password must be unique to an individual. If a password is known to more than one person, the responsibility of the user for all activity within their account cannot be enforced.

>> Password syntax (format) rules

- Ideally, passwords should be five to eight characters in length. Anything shorter is too easy to guess, anything longer is too hard to remember.
- Passwords should allow for a combination of alpha, numeric, upper and lower case and special characters.
- Passwords should not be particularly identifiable with the user (such as first name, last name, spouse name, pet's name, etc). Some organisations prohibit the use of vowels, making word association/guessing of passwords more difficult.
- The system should not permit previous password(s) to be used after being changed.
- Logon-IDs not used after a number of days should be deactivated to prevent possible misuse.
- The system should automatically disconnect a logon session if no activity has occurred for a period of time (one hour). This reduces the risk of misuse of an active logon session left unattended because the user went to lunch, left for home, went to a meeting or otherwise forgot to logoff. This is often referred to as 'time out'.

2) Logging computer access

With most security packages today, computer access and attempted access violations can be automatically logged by the computer and reported. The frequency of the security administrator's review of computer access reports should be commensurate with the sensitivity of the computerised information being protected.

The review should identify patterns or trends that indicate abuse of access privileges, such as

concentration on a sensitive application. It should also identify violations such as attempting computer file access that is not authorised and/or use of incorrect passwords. The violations should be reported and appropriate action taken.

3) Token devices, one-time passwords

A two-factor authentication technique such as microprocessor-controlled smart cards generates one-time passwords that are good for only one logon session. Users enter this password along with a password they have memorised to gain access to the system. This technique involves something you have (a device subject to theft) and something you know (a personal identification number). Such devices gain their one time password status because of a unique session characteristic (e.g. ID or time) appended to the password.

4) Biometric security access control

This control restricts computer access based on a physical feature of the user, such as a fingerprint or eye retina pattern. A reader is utilised to interpret the individual's biometric features before permitting computer access. This is a very effective access control because it is difficult to circumvent, and traditionally has been used very little as an access control technique. However due to advances in hardware efficiencies and storage, this approach is becoming a more viable option as an access control mechanism. Biometric access controls are also the best means of authenticating a user's identity based on something they are.

5) Terminal usage restraints

- Terminal security – this security feature restricts the number of terminals that can access certain transactions based on the physical/logical address of the terminal.
- Terminal locks – this security feature prevents turning on a computer terminal until a key lock is unlocked by a turnkey or card key.

6) Dial-back procedures

When a dial-up line is used, access should be restricted by a dial-back mechanism. Dial-back interrupts the telecommunications dial-up connection to the computer by dialling back the caller to validate user authority.

7) Restrict and monitor access to computer features that bypass security

Generally, only system software programmers should have access to these features:

- Bypass Label Processing (BLP) – BLP bypasses computer reading of the file label. Since most access control rules are based on file names (labels), this can bypass access security.
- System exits – this system software feature permits the user to perform complex system maintenance, which may be tailored to a specific environment or company. They often exist outside of the computer security system and thus are not restricted or reported in their use.
- Special system logon-IDs – these logon-IDs are often provided with the computer by the vendor. The names can be easily determined because they are the same for all similar computer systems. Passwords should be changed immediately upon installation to secure them.

8) Logging of online activity

Many computer systems can automatically log computer activity initiated through a logon-ID or computer terminal. This is known as a transaction log. The information can be used to provide a management/audit trail.

9) Data classification

Computer files, like documents have varying degrees of sensitivity. By assigning classes or levels of sensitivity to computer files, management can establish guidelines for the level of access control that should be assigned. Classifications should be simple, such as high, medium and low. End user managers and the security administrator can use these classifications to assist with determining who should be able to access what.

A typical classification described by US National Institute of Standards and Technology has four data classifications:

- Sensitive – applies to information that requires special precautions to ensure the integrity of the information, by protecting it from unauthorised modification or deletion. It is information that requires a higher than normal assurance of accuracy and completeness e.g. passwords, encryption parameters.
- Confidential – applies to the most sensitive business information that is intended strictly for use within an organisation. Its unauthorised disclosure could seriously and adversely impact the organisation's image in the eyes of the public e.g. application programme source code, project documentation, etc.
- Private – applies to personal information that is intended for use within the organisation. Its unauthorised disclosure could seriously and adversely impact the organization and/or its customers e.g. customer account data, e-mail messages, etc.
- Public – applies to data that can be accessed by the public but can be updated/deleted by authorised people only e.g. company web pages, monetary transaction limit data etc.

10) Safeguards for confidential data on a PC

In today's environment, it is not unusual to keep sensitive data on PCs and diskettes where it is more difficult to implement logical and physical access controls.

Sensitive data should not be stored in a microcomputer. The simplest and most effective way to secure data and software in a microcomputer is to remove the storage medium (such as the disk or tape) from the machine when it is not in use and lock it in a safe. Microcomputers with fixed disk systems may require additional security procedures for theft protection. Vendors offer lockable enclosures, clamping devices and cable fastening devices that help prevent equipment theft. The computer can also be connected to a security system that sounds an alarm if equipment is moved.

Passwords can also be allocated to individual files to prevent them being opened by an unauthorised person, one not in possession of the password. All sensitive data should be recorded on removable hard drives, which are more easily secured than fixed or floppy disks. Software can also be used to control access to microcomputer data. The basic software approach restricts access to programme and data files with a password system. Preventative controls such as encryption become more important for protecting sensitive data in the event that a PC or laptop is lost, stolen or sold.

11) Naming conventions for access controls

On larger mainframe and midrange systems, access control naming conventions are structures used to govern user access to the system and user authority to access or use computer resources such as files, programmes and terminals. These general naming conventions and associated files are required in a computer environment to establish and maintain personal accountability and segregation of duties in the access of data. The need for sophisticated naming conventions over access controls depends on the importance and level of security that is needed to ensure that unauthorised access has not been granted.

5. Physical security

5.1 Physical access exposures

Exposures that exist from accidental or intentional violation of these access paths include:

- Unauthorised entry
- Damage, vandalism or theft to equipment or documents
- Copying or viewing of sensitive or copyrighted information
- Alteration of sensitive equipment and information
- Public disclosure of sensitive information
- Abuse of data processing resources
- Blackmail
- Embezzlement

Possible perpetrators

- Employees with authorised or unauthorised access who are:
  - Disgruntled (upset by or concerned about some action by the organisation or its management)
  - On strike
  - Threatened by disciplinary action or dismissal
  - Addicted to a substance or gambling
  - Experiencing financial or emotional problems
  - Notified of their termination
- Former employees
- Interested or informed outsiders such as competitors, thieves, organised crime and hackers
- Accidental ignorant – someone who unknowingly perpetrates a violation (could be an employee or outsider)

The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.

From an information system perspective, facilities to be protected include the following:

- Programming area
- Computer room

- Operator consoles and terminals
- Tape library, tapes, disks and all magnetic media
- Storage room and supplies
- Offsite backup file storage facility
- Input/output control room
- Communication closet
- Telecommunication equipment (including radios, satellites, wiring. Modems and external network connections)
- Microcomputers and personal computers (PCs)
- Power sources
- Disposal sites
- Minicomputer establishments
- Dedicated telephones/Telephone lines
- Control units and front end processors
- Portable equipment (hand-held scanners and coding devices, bar code readers, laptop computers and notebooks, printers, pocket LAN adapters and others)
- Onsite and remote printers
- Local area networks

5.2 Physical access controls

Physical access controls are designed to protect the organisation from unauthorised access. They reduce exposure to theft or destruction of data and hardware. These controls should limit access to only those individuals authorised by management. This authorisation may be explicit, as in a door lock for which management has authorised you to have a key; or implicit, as in a job description that implies a need to access sensitive reports and documents. Examples of some of the more common access controls are:

- **Bolting door locks –** these locks require the traditional metal key to gain entry. The key should be stamped 'Do not duplicate'.

- **Combination door locks (cipher locks) –** this system uses a numeric keypad or dial to gain entry. The combination should be changed at regular intervals or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces the risk of the combination being known by unauthorised people.

- **Electronic door locks –** this system uses a magnetic or embedded chip-based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by the sensor device that then activates the door locking mechanism. Electronic door locks have the following advantages over bolting and combination locks:

    - Through the special internal code, cards can be assigned to an identifiable individual.
    - Through the special internal code and sensor devices, access can be restricted based on the individual's unique access needs. Restriction can be assigned to particular doors or to particular hours of the day.
    - They are difficult to duplicate
    - Card entry can be easily deactivated in the event an employee is terminated

or a card is lost or stolen. Silent or audible alarms can be automatically activated if unauthorised entry is attempted. Issuing, accounting for and retrieving the card keys is an administrative process that should be carefully controlled. The card key is an important item to retrieve when an employee leaves the firm.

- **Biometric door locks –** an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

- **Manual logging –** all visitors should be required to sign a visitor's log indicating their name, company represented, reason for visiting and person to see. Logging typically is at the front reception desk and entrance to the computer room. Before gaining access, visitors, should also be required to provide verification of identification, such as a driver's license, business card or vendor identification tag.

- **Electronic logging –** this is a feature of electronic and biometric security systems. All access can be logged, with unsuccessful attempts being highlighted.

- **Identification badges (photo IDs) –** badges should be worn and displayed by all personnel. Visitor badges should be a different colour from employee badges for easy identification. Sophisticated photo IDs can also be utilised as electronic card keys. Issuing, accounting for and retrieving the badges in an administrative process must be carefully controlled.
- **Video cameras –** cameras should be located at strategic points and monitored by security guards. Sophisticated video cameras can be activated by motion. The video surveillance recording should be retained for possible future playbacks.

- **Security guards –** guards are very useful if supplemented by video cameras and locked doors. Guards supplied by an external agency should be bonded to protect the organisation from loss.

- **Controlled visitor access –** all visitors should be escorted by a responsible employee. Visitors include friends, maintenance personnel, computer vendors, consultants (unless long-term, in which case special guest access may be provided) and external auditors.

- **Bonded personnel –** all service contract personnel, such as cleaning people and off-site storage services, should be bonded. This does not improve physical security but limits the financial exposure of the organisation.

- **Deadman doors –** this system uses a pair of (two) doors, typically found in entries to facilities such as computer rooms and document stations. For the second door to operate, the first entry door must close and lock, with only one person permitted in the holding area. This reduces risk of piggybacking, when an unauthorised person follows an authorised person through a secured entry.

- **Not advertising the location of sensitive facilities –** facilities such as computer rooms should not be visible or identifiable from the outside, that is, no windows or directional signs. The building or department directory should discreetly identify only the general location of the information processing facility.

- **Computer terminal locks –** these lock devices to the desk, prevent the computer from being turned on or disengage keyboard recognition, preventing use.

- **Controlled single entry point –** a controlled entry point monitored by a receptionist should be used by all incoming personnel. Multiple entry points increase the risk of unauthorised entry. Unnecessary or unused entry points should be eliminated or deadlocked.

- **Alarm system –** an alarm system should be linked to inactive entry points, motion detectors and the reverse flow of enter or exit only doors. Security personnel should be able to hear the alarm when activated.

- **Secured report/document distribution cart –** secured carts, such as mail carts, should be covered and locked and should not be left unattended.

6. Personnel issues

Employee responsibilities for security policy are:

- Reading the security policy and adhering to it
- Keeping logon-IDs and passwords secret
- Reporting suspected violations of security
- Maintaining good physical security by keeping doors locked, safeguarding access keys, not disclosing access door lock combinations and questioning unfamiliar people
- Conforming to local laws and regulations
- Adhering to privacy regulations with regard to confidential information e.g. health, legal etc.

Non-employees with access to company systems should be held accountable for security policies and responsibilities. This includes contract employees, vendors, programmers, analysts, maintenance personnel and clients.

Segregation of responsibilities

A traditional security control is to ensure that there are no instances where one individual is solely responsible for setting, implementing and policing controls and, at the same time, responsible for the use of the systems. The use of a number of people, all responsible for some part of information system controls or operations, allows each to act as a check upon another. Since no employee is performing all the steps in a single transaction, the others involved in the transaction can monitor for accidents and crime.

The logical grouping of information systems activities might be:

- Systems development
- Management of input media
- Operating the system
- Management of documentation and file archives
- Distribution of output

Where possible, to segregate responsibilities fully, no one person should cross these task boundaries. Associated with this type of security control is the use of rotation of duties and unannounced audits.

Other human resources policies and practices include:

- Hiring practices – to ensure that the most effective and efficient staff is chosen and that the company is in compliance with legal requirements. Practices include:
  - Background checks
  - Confidentiality agreements
  - Employee bonding to protect against losses due to theft
  - Conflict of interest agreements
  - Non-compete agreements
- Employee handbook – distributed to all employees upon being hired, should explain items such as
  - Security policies and procedures
  - Company expectations
  - Employee benefits
  - Disciplinary actions
  - Performance evaluations etc.
- Promotion policies – should be fair and understood by employees. Based on objective criteria considering performance, education, experience and level of responsibility.
- Training – should be provided on a fair and regular basis
- Scheduling and time reporting – proper scheduling provides for a more efficient operation and use of computing resources
- Employee performance evaluations – employee assessment must be a standard and regular feature for all IS staff
- Required vacations – ensures that once a year, at a minimum, someone other than the regular employee will perform a job function. This reduces the opportunity to commit improper or illegal acts.
- Job rotation – provides an additional control (to reduce the risk of fraudulent or malicious acts), since the same individual does not perform the same tasks all the time.
- Termination policies – policies should be structured to provide adequate protection for the organisation's computer assets and data. Should address:
  - Voluntary termination
  - Immediate termination
  - Return of all access keys, ID cards and badges to prevent easy physical access
  - Deletion of assigned logon-ID and passwords to prohibit system access
  - Notification to other staff and facilities security to increase awareness of the terminated employee's status.
  - Arrangement of the final pay routines to remove the employee from active payroll files
  - Performance of a termination interview to gather insight on the employee's perception of management
  - Return of all company property
  - Escort from the premises.

7. Network security

Communication networks (Wide Area or Local Area Networks) generally include devices connected to the network, and programmes and files supporting the network operations. Control is accomplished through a network control terminal and specialised communications software.

The following are controls over the communication network:

- Network control functions should be performed by technically qualified operators.
- Network control functions should be separated and duties rotated on a regular basis where possible.
- Network control software must restrict operator access from performing certain functions such as ability to amend or delete operator activity logs.
- Network control software should maintain an audit trail of all operator activities.
- Audit trails should be reviewed periodically by operations management to detect any unauthorised network operation activities.
- Network operation standards and protocols should be documented and made available to the operators and should be reviewed periodically to ensure compliance.
- Network access by system engineers should be closely monitored and reviewed to direct unauthorised access to the network.
- Analysis should be performed to ensure workload balance, fast response time and system efficiency.
- A terminal identification file should be maintained by the communication software to check the authentication of a terminal when it tries to send or receive messages.
- Data encryption should be used where appropriate to protect messages from disclosure during transmission.

Some common network management and control software include Novell NetWare, Windows NT, UNIX, NetView and NetPass.

7.1 Local Area Network (LAN) security

Local area networks (LANs) facilitate the storage and retrieval of programs and data used by a group of people. LAN software and practices also need to provide for the security of these programs and data. Risks associated with use of LANs include:

- Loss of data and programme integrity through unauthorised changes
- Lack of current data protection through inability to maintain version control
- Exposure to external activity through limited user verification and potential public network access from dial-up connections
- Virus infection
- Improper disclosure of data because of general access rather than need-to-know access provisions
- Violating software licenses by using unlicensed or excessive number of software copies
- Illegal access by impersonating or masquerading as a legitimate LAN user
- Internal user's sniffing (obtaining seemingly unimportant information from the network

that can be used to launch an attack, such as network address information)
- Internal user's spoofing (reconfiguring a network address to pretend to be a different address)
- Destruction of the logging and auditing data

The LAN security provisions available depend on the software product, product version and implementation. Commonly available network security administrative capabilities include:

- Declaring ownership of programmes, files and storage
- Limiting access to read only
- Implementing record and file locking to prevent simultaneous update to the same record
- Enforcing user ID/password sign-on procedures, including the rules relating to password length, format and change frequency

7.2 Dial-up access controls

It is possible to break LAN security through the dial-in route. Without dial-up access controls, a caller can dial in and try passwords until they gain access. Once in, they can hide pieces of software anywhere, pass through Wide Area Network (WAN) links to other systems and generally cause as much or as little havoc as they like.

- To minimise the risk of unauthorized dial-in access, remote users should never store their passwords in plain text login scripts on notebooks and laptops. Furthermore, portable PCs should be protected by physical keys and/or basic input output system (BIOS) based passwords to limit access to data if stolen.

- In order to prevent access by the guessing of passwords, a dial-back modem should be used. When a call is answered by the modem, the caller must enter a code. The modem then hangs up the connection and looks up a corresponding phone number that has been authorised for dial-in access and calls the number back if it is authenticated.

7.3 Client/server security

A client/server system typically contains numerous access points. Client/server systems utilise distributed techniques, creating increased risk of access to data and processing. To effectively secure the client/server environment, all access points should be identified. In mainframe-based applications, centralised processing techniques require the user to go through one pre-defined route to access all resources. In a client/server environment, several access points exist, as application data may exist on the client or the server. Each of these routes must, therefore, be examined individually and in relation to each other to determine that no exposures are left unchecked.

In order to increase the security in a client/server environment, the following control techniques should be in place:

- Securing access to the data or application on the client/server may be performed by disabling the floppy disk drive, much like a keyless workstation that has access to a mainframe. Diskless workstations prevent access control software from being by-

passed and rendering the workstation vulnerable to unauthorised access. By securing the automatic boot or start up batch files, unauthorised users may be prevented from overriding login scripts and access.

- Network monitoring devices may be used to inspect activity from known or unknown users.
- Data encryption techniques can help protect sensitive or proprietary data from unauthorized access.
- Authentication systems may provide environment-wide, logical facilities that can differentiate among users. Another method, system smart cards, uses intelligent hand-held devices and encryption techniques to decipher random codes provided by client/server systems. A smart card displays a temporary password that is provided by an algorithm (step-by-step calculation instructions) on the system and must be re-entered by the user during the login session for access into the client/server system.
- The use of application level access control programmes and the organisation of users into functional groups is a management control that restricts access by limiting users to only those functions needed to perform their duties.

Client/server risks and issues

Since the early 1990s, client/server technology has become one of the predominant ways many organisations have processed production data and developed and delivered mission critical products and services.

The areas of risk and concern in a client/server environment are:

- Access controls may be inherently weak in a client/server environment if network administration does not properly set up password change controls or access rules.
- Change control and change management procedures, whether automated or manual may be inherently weak. The primary reason for this weakness is due to the relatively high level of sophistication of client/server change control tools together with inexperienced staff who are reluctant to introduce such tools for fear of introducing limitations on their capability.
- The loss of network availability may have a serious impact on the business or service
- Obsolescence of the network components, including hardware, software and communications.
- Unauthorised and indiscriminate use of synchronous and asynchronous modems to connect the network to other networks.
- Connection of the network to public switched telephone networks.
- Inaccurate, unauthorised and unapproved changes to systems or data.
- Unauthorised access to confidential data, the unauthorized modification of data, business interruption and incomplete and inaccurate data.
- Application code and data may not be located on a single machine enclosed in a secure computer room as with mainframe computing.

7.4 Internet threats

The very nature of the Internet makes it vulnerable to attack. It was originally designed to allow for the freest possible exchange of information, data and files. However, today the freedom carries a price. Hackers and virus-writers try to attack the Internet and computers connected to the Internet and those who want to invade other's privacy attempt to crack into databases of

sensitive information or snoop on information as it travels across Internet routes.

It is, therefore, important in this situation to understand the risks and security factors that are needed to ensure proper controls are in place when a company connects to the Internet. There are several areas of control risks that must be evaluated to determine the adequacy of Internet security controls:

- Corporate Internet policies and procedures
- Firewall standards
- Firewall security
- Data security controls

Internet threats include:

>>> a) Disclosure

It is relatively simple for someone to eavesdrop on a 'conversation' taking place over the Internet. Messages and data traversing the Internet can be seen by other machines including e-mail files, passwords and in some cases key-strokes as they are being entered in real time.

>>> b) Masquerade

A common attack is a user pretending to be someone else to gain additional privileges or access to otherwise forbidden data or systems. This can involve a machine being reprogrammed to masquerade as another machine (such as changing its Internet Protocol – IP address). This is referred to as spoofing.

>>> c) Unauthorised access

Many Internet software packages contain vulnerabilities that render systems subject to attack. Additionally, many of these systems are large and difficult to configure, resulting in a large percentage of unauthorized access incidents.

>>> d) Loss of integrity

Just as it is relatively simple to eavesdrop a conversation, so it is also relatively easy to intercept the conversation and change some of the contents or to repeat a message. This could have disastrous effects if, for example, the message was an instruction to a bank to pay money.

>>> e) Denial of service

Denial of service attacks occur when a computer connected to the Internet is inundated (flooded) with data and/or requests that must be serviced. The machine becomes so tied up with dealing with these messages that it becomes useless for any other purpose.

>>> f) Threat of service and resources

Where the Internet is being used as a channel for delivery of a service, unauthorised access to the service is effectively theft. For example, hacking into a subscription-based news service is effectively theft.

It is difficult to assess the impact of the threats described above, but in general terms the following types of impact could occur:

- Loss of income
- Increased cost of recovery (correcting information and re-establishing services)
- Increased cost of retrospectively securing systems
- Loss of information (critical data, proprietary information, contracts)
- Loss of trade secrets
- Damage to reputation
- Legal and regulatory non-compliance
- Failure to meet contractual commitments

7.5 Encryption

Encryption is the process of converting a plaintext message into a secure coded form of text called cipher text that cannot be understood without converting back via decryption (the reverse process) to plaintext again. This is done via a mathematical function and a special encryption/ decryption password called the key.

Encryption is generally used to:

- Protect data in transit over networks from unauthorised interception and manipulation
- Protect information stored on computers from unauthorised viewing and manipulation
- Deter and detect accidental or intentional alterations of data
- Verify authenticity of a transaction or document

The limitations of encryption are that it can't prevent loss of data and encryption programs can be compromised. Therefore encryption should be regarded as an essential but incomplete form of access control that should be incorporated into an organization's overall computer security program.

Key elements of encryption systems are:

(i) Encryption algorithm – a mathematically based function or calculation which encrypts/ decrypts data

(ii) Encryption keys – a piece of information that is used within an encryption algorithm (calculation) to make the encryption or decryption process unique/ similar to passwords, a user needs to use the correct key to access or decipher a message. The wrong key will decipher the message into an unreadable form.

(iii) Key length – a predetermined length for the key. The longer the key, the more difficult it is to compromise in a brute-force attack where all possible key combinations are tried. Effective encryption systems depend upon the secrecy and the difficulty of compromising a key, the existence of back doors by which an encrypted file can be decrypted without knowing the key, the ability to decrypt an entire cipher text message if you know the way that a portion of it decrypts (called a known text attack), and the properties of the plaintext known by a perpetrator.

There are two common encryption or cryptographic systems:

a) Symmetric or private key system

Symmetric cryptosystem use a secret key to encrypt the plaintext to the cipher text. The same key is also used to decrypt the cipher text to the corresponding plaintext. In this

case the key is symmetric because the encryption key is the same as the decryption key. The most common private key cryptography system is data encryption standard (DES).

b) Asymmetric or public key system

Asymmetric encryption systems use two keys, which work together as a pair. One key is used to encrypt data, the other is used to decrypt data. Either key can be used to encrypt or decrypt, but once one key has been used to encrypt data, only its partner can be used to decrypt the data (even the key that was used to encrypt the data cannot be used to decrypt it). Generally, with asymmetric encryption, one key is known only to one person – the secret or private key – the other key is known by many people – the public key. A common form of asymmetric encryption is RSA (named after its inventors Rivest, Shamir and Adelman).

7.6 Firewall security

A firewall is a set of hardware and software equipment placed between an organisation's internal network and an external network to prevent outsiders from invading private networks.

Companies should build firewalls to protect their networks from attacks. In order to be effective, firewalls should allow individuals on the corporate network to access the Internet and at the same time stop hackers or others on the Internet from gaining access to the corporate network to cause damage.

Firewalls are hardware and software combinations that are built using routers, servers and a variety of software. They should sit in the most vulnerable point between a corporate network and the Internet and they can be as simple or complex as system administrators want to build them.

There are many different types of firewalls, but many enable organisations to:

- Block access to particular sites on the Internet
- Prevent certain users from accessing certain servers or services
- Monitor communications between an internal and external networks
- Eavesdrop and record all communications between an internal network and the outside world to investigate network penetrations or detect internal subversions.
- Encrypt packets that are sent between different physical locations within an organisation by creating a virtual private network over the Internet.

Problems faced by organisations that have implemented firewalls are:

- A false sense of security exists where management feels that no further security checks and controls are needed on the internal network.
- Firewalls are circumvented through the use of modems connecting users to Internet Service Providers.
- Mis-configured firewalls, allowing unknown and dangerous services to pass through freely.
- Misunderstanding of what constitutes a firewall e.g. companies claiming to have a firewall merely having a screening router.
- Monitoring activities do not occur on a regular basis i.e. log settings not appropriately applied and reviewed.

7.7 Intrusion detection systems (IDS)

Intrusion or intruder detection is the identification of and response to ill-minded activities. An IDS is a tool aiding in the detection of such attacks. An IDS detects patterns and issues an alert. There are two types of IDSs, network-based and host-based.

Network-based IDSs identify attacks within the network that they are monitoring and issue a warning to the operator. If a network-based IDS is placed between the Internet and the firewall, it will detect all the attack attempts, whether they do or do not enter the firewall. If the IDS is placed between a firewall and the corporate network it will detect those attacks that could not enter the firewall (intruders). The IDS is not a substitute for a firewall, but complements the function of a firewall.

Host-based IDSs are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack. They can detect the modification of executable programmes, the deletion of files and issue a warning when an attempt is made to use a privileged command.

8. Environmental exposures and controls

Environmental exposures are primarily due to naturally occurring events. However, with proper controls, exposure to these elements can be reduced. Common exposures are:

- Fire
- Natural disasters – earthquake, volcano, hurricane, tornado
- Power failure
- Power spike
- Air conditioning failure
- Electrical shock
- Equipment failure
- Water damage/flooding – even with facilities located on upper floors of high-rise buildings, water damage is a risk, typically occurring from broken water pipes
- Bomb threat/attack

Other environmental issues and exposures include the following:

- Is the power supply to the computer equipment properly controlled to ensure that it remains within the manufacturer's specifications?
- Are the air conditioning, humidity and ventilation control systems for the computer equipment adequate to maintain temperatures within manufacturers' specifications?
- Is the computer equipment protected from the effects of static electricity, using an anti-static rug or anti-static spray?
- Is the computer equipment kept free of dust, smoke and other particulate matter, such as food?
- Is consumption of food, beverage and tobacco products prohibited, by policy, around

computer equipment?

- Are backup media protected from damage due to temperature extremes, the effects of magnetic fields and water damage?

Controls for environmental exposures

a) Water detectors – in the computer room, water detectors should be placed under the raised floor and near drain holes, even if the computer room is on a high floor (remember water leaks). When activated, the detectors should produce an audible alarm that can be heard by security and control personnel.

b) Hand-held fire extinguishers – fire extinguishers should be in strategic locations throughout the information system facility. They should be tagged for inspection and inspected at least annually.

c) Manual fire alarms – hand-pull fire alarms should be strategically placed throughout the facility. The resulting audible alarm should be linked to a monitored guard station.

d) Smoke detectors – they supplement not replace fire suppression systems. Smoke detectors should be above and below the ceiling tiles throughout the facility and below the raised computer room floor. They should produce an audible alarm when activated and be linked to a monitored station (preferably by the fire department).

e) Fire suppression system – these systems are designed to activate immediately after detection of high heat typically generated by fire. It should produce an audible alarm when activated. Ideally, the system should automatically trigger other mechanisms to localise the fire. This includes closing fire doors, notifying the fire department, closing off ventilation ducts and shutting down nonessential electrical equipment. Therefore, fire suppression varies but is usually one of the following:

- Water based systems (sprinkler systems) – effective but unpopular because they damage equipment
- Dry-pipe sprinkling – sprinkler systems that do not have water in the pipes until an electronic fire alarm activates the water pumps to send water to the dry pipe system.
- Halon systems – release pressurised halon gases that remove oxygen from the air, thus starving the fire. Halon is popular because it is an inert gas and does not damage equipment.
- Carbon dioxide systems – release pressurised carbon dioxide gas into the area protected to replace the oxygen required for combustion. Unlike halon, however, carbon dioxide is unable to sustain human life and can, therefore, not be set to automatic release.

f) Strategically locating the computer room – to reduce the risk of flooding, the computer room should not be located in the basement. If located in a multi-storey building, studies show that the best location for the computer room to reduce the risk of fire, smoke and water damage is between 3rd, and 6th floor.

g) Regular inspection by fire department – to ensure that all fire detection systems comply with building codes, the fire department should inspect the system and facilities annually.

h) Fireproof walls, floors and ceilings surrounding the computer room – walls surrounding the information processing facility should contain or block fire from spreading. The surrounding walls would have at least a two-hour fire resistance rating.

i) Electrical surge protectors – these electrical devices reduce the risk of damage to equipment due to power spikes. Voltage regulators measure the incoming electrical current and either increase or decrease the charge to ensure a consistent current. Such protectors are typically built into the uninterruptible power supply (UPS) system.

j) Uninterruptible power supply system (UPS)/generator – a UPS system consists of a battery or petrol powered generator that interfaces between the electrical power entering the facility and the electrical power entering the computer. The system typically cleanses the power to ensure wattage into the computer is consistent. Should a power failure occur, the UPS continues providing electrical power from the generator to the computer for a certain length of time. A UPS system can be built into a computer or can be an external piece of equipment.

k) Emergency power-off switch – there may be a need to shut off power to the computer and peripheral devices, such as during a computer room fire or emergency evacuation. Two emergency power-off switches should serve this purpose, one in the computer room, the other near, but outside, the computer room. They should be clearly labelled, easily accessible for this purpose and yet still secured from unauthorised people. The switches should be shielded to prevent accidental activation.

l) Power leads from two substations – electrical power lines that feed into the facility are exposed to many environmental hazards - water, fire, lightning, cutting to due careless digging etc. To reduce the risk of a power failure due to these events that, for the most part, are beyond the control of the organisation, redundant power lines should feed into the facility. In this way, interruption of one power line does not adversely affect electrical supply.

m) 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 fire-resistant panels and conduit. This conduit generally lies under the fire-resistant raised computer room floor.

n) Prohibitions against eating, drinking and smoking within the information processing facility – food, drink and tobacco use can cause fires, build-up of contaminants or damage to sensitive equipment especially in case of liquids. They should be prohibited from the information processing facility. This prohibition should be overt, for example, a sign on the entry door.

o) Fire resistant office materials – wastebaskets, curtains, desks, cabinets and other general office materials in the information processing facility should be fire resistant. Cleaning fluids for desktops, console screens and other office furniture/fixtures should not be flammable.

p) Documented and tested emergency evacuation plans – evacuation plans should emphasise human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation, if time permits.

9. Computer ethics

Although ethical decision-making is a thoughtful process, based on one's own personal fundamental principles, we need codes of ethics and professional conduct for the following reasons:

- Document acceptable professional conduct to:
  - Establish status of the profession
  - Educate professionals of their responsibilities to the public
  - Inform the public of expectations of professionals

- Judge inappropriate professional behaviour and punish violators
- Aid the professional in ethical decision-making.

The following issues distinguish computing professionals' ethics from other professionals' ethics:

- Computing (automation) affects such a large segment of the society (personal, professional, business, government, medical, industry, research, education, entertainment, law, agriculture, science, art, etc); it changes the very fabric of society.
- Information technology is a very public business
- Computing is a young discipline
- It changes relationships between: people, businesses, industries, governments, etc
  - Communication is faster
  - Data can be fragile: it may be insecure, invalid, outdated, leaked, lost, unrecoverable, misdirected, copied, stolen, misrepresented, etc.
  - The well-being of people, businesses, governments, and social agencies may be jeopardised through faulty computing systems and/or unethical behaviour by computing professionals
  - Computing systems can change the way people work: it can not only make people more productive but can also isolate them from one another
  - Conceivably could create a lower and upper class society
  - People can lose their identity in cyberspace
  - Computing systems can change humankind's quality of life
  - Computing systems can take control of parts of our lives: for good or bad.

Some of the issues addressed in computer ethics include:

General moral imperatives

- Contribute to society and human well-being: minimise negative consequences of computing systems including threats to health and safety, ensure that products will be used in socially responsible ways and be alert and make others aware of potential damage to the environment.
- Avoid harm to others: this principle prohibits use of computing technology in ways that result in harm to the users, general public, employees and employers. Harmful actions include intentional destruction or modification of files and programmes leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of computer viruses.
- Be honest and trustworthy: the honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems. He has a duty to be honest about his qualifications and about any circumstance that may lead to a conflict of interest.
- Be fair and take action not to discriminate: the values of equality, tolerance and respect for others and the principles of equal justice govern this imperative.
- Honour property rights including copyrights and patents: violation of copyrights, patents, trade secrets and the terms of license agreement is prohibited by the law in most circumstances. Even when software is not so protected, such violations are contrary to professional behaviour. Copies of software should be made only with proper authorisation. Unauthorised duplication of materials must not be condoned.
- Give proper credit for intellectual property: computing professionals are obligated to

protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.

- Respect the privacy of others: computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilisation. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from authorised access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.
- Honour confidentiality: the principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honour confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this code.

More specific professional responsibilities

- Strive to achieve the highest quality, effectiveness and dignity in both the process and product of professional work.
- Acquire and maintain professional competence
- Know and respect existing laws pertaining to professional work
- Accept and provide appropriate professional review
- Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
- Honour contracts, agreements and assigned responsibilities
- Improve public understanding of computing and its consequences
- Access computing and communication resources only when authorised to do so

Organisational leadership imperatives

- Articulate social responsibilities of members of an organisational unit and encourage full acceptance of those responsibilities
- Manage personnel and resources to design and build information systems that enhance the quality of working life.
- Acknowledge and support proper and authorised uses of an organisation's computing and communication resources.
- Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.
- Articulate and support policies that protect the dignity of users and others affected by a computing system.
- Create opportunities for members of the organisation to learn the principles and limitations of computer systems.

Software engineering code of ethics and professional practice

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software

engineers shall adhere to the following eight principles.

a) **Public** – software engineers shall act consistently with public interest.
b) **Client and employer** - software engineers shall act in a manner that is in the best interest of their client and employer consistent with public interest.
c) **Product** – software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
d) **Judgment** – software engineers shall maintain integrity and independence in their professional judgment.
e) **Management** – software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
f) **Profession** – software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
g) **Colleagues** – software engineers shall be fair to and supportive of their colleagues.
h) **Self** – software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

10. Terminology

>>> Digital signature

A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

How it works

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

a) You copy-and-paste the contract (it's a short one!) into an e-mail note.
b) Using special software, you obtain a message hash (mathematical summary) of the contract.
c) You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
d) The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

a) To make sure it's intact and from you, your lawyer makes a hash of the received message.
b) Your lawyer then uses your public key to decrypt the message hash or summary.
c) If the hashes match, the received message is valid.

>>> Digital Certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by organisations known as certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.

SUMMARY

To retain a competitive advantage and to meet basic business requirements organizations must endeavour to achieve the following security goals:

- Confidentiality – protect value of information and preserve the confidentiality of sensitive data.
- Integrity – ensure the accuracy and reliability of the information stored on the computer systems.
- Availability – ensure the continued access to the information system and all its assets to legitimate users
- Ensure conformity to laws, regulations and standards.

Hazards (exposures) to information security **-** is a form of possible loss or harm. Examples of exposures include:

- Unauthorised access resulting in a loss of computing time
- Unauthorised disclosure – information revealed without authorisation

Threats to information security - These are circumstances that have potential to cause loss or harm

- Human error
- Disgruntled employees
- Dishonest employees

Application controls includes methods for ensuring that:

- Only complete, accurate and valid data is entered and updated in a computer system
- Processing accomplishes the correct task
- Processing results meet expectations
- Data is maintained

There are two common encryptions or cryptographic systems:

a) **Symmetric or private key system**
Symmetric cryptosystem use a secret key to encrypt the plaintext to the cipher text. The same key is also used to decrypt the cipher text to the corresponding plaintext.

b) **Asymmetric or public key system**
Asymmetric encryption systems use two keys, which work together as a pair. One key is used to encrypt data, the other is used to decrypt data. Either key can be used to encrypt or decrypt, but once one key has been used to encrypt data, only its partner can be used to decrypt the data.

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by organisations known as certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key.

Past Paper Analysis:

12/00, 6/01, 12/01, 6/02, 6/03, 12/03, 6/04, 12/04, 6/05, 6/06, 12/06, 6/07, 12/07

CHAPTER QUIZ

1. ..... is the identification of and response to ill-minded activities.

2. Environmental exposures are primarily due to human initiated occurring events
   a. True
   b. False

3. Private Key systems use two keys, which work together as a pair.
   a. True
   b. False

4. UPS stands for.....

5. .....facilitate the storage and retrieval of programmes and data used by a group of people.

STUDY TEXT

SOLUTIONS TO CHAPTER QUIZ

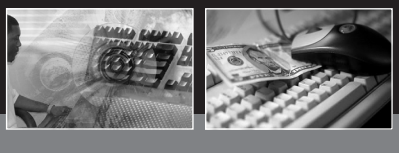
1. Intrusion or intruder detection
2. b. False – they are naturally occurring events
3. b. False – that is public key system
4. Uninterruptible power supply
5. Local area networks (LANs)

QUESTIONS

1. It may be said that organisations wishing to benefit from the advantages that an information system may give must be prepared to incur the costs – both financial and organisational – of maintaining system security. Produce a report as if for the management of a commercial company explaining the factors which increase the company's vulnerability to threats, and the issue of risk.
2. Disaster planning is best carried out as a team activity, with members from all areas of the organisation under the active sponsorship of senior management.
   (a). List and briefly describe the make-up of a security planning team for a typical commercial organisation.
   (b). Explain the detailed work of the security team.
3. An organisation which chooses to computerise its information resources must take seriously the possibility of fraud.
   (a). Briefly list the factors which may motivate a person to commit fraud
   (b). Describe the steps which may be taken by the perpetrator to conceal the existence of a fraud.
4. The security cost analysis process compares the cost of the proposed security measures with the possible cost disruption to the organisation. Describe the factors that may influence the cost analysis process in a typical commercial organisation.
   The adoption of a contingency plan for an information system will involve an organisation in a range of security decisions. Explain the decisions that would have to be made by management when installing major security procedures in an organisation.

CHAPTER SEVEN

DATA COMMUNICATION & COMPUTER NETWORKS



CHAPTER SEVEN

DATA COMMUNICATION & COMPUTER NETWORKS

▶ OBJECTIVES

When you have completed this chapter, you should be able to:

1. Describe communication channels.
2. Identify types of computer networks.
3. Outline the various applications of computer networks within an organisation.
4. Describe and differentiate the data transmission techniques.

▶ INTRODUCTION

Data is useful once it has been transferred from the source to the recipient. The transfer of such data involves various techniques and technology of essence to facilitate fast, efficient and effective data transfer so that delays and eavesdropping by unintended recipients is avoided.

▶ DEFINITION OF KEY TERMS

Modem is a hardware device that converts computer signals (digital signals) to telephone signals (analog signals) and vice versa.

Bandwidth is the bits-per-second (bps) transmission capability of a communication channel.

Protocols are sets of communication rules for exchange of information.

Computer network is a communications system connecting two or more computers that work to exchange information and share resources.

▶ EXAM CONTEXT

Examiners constantly focus on configurations. Hence, the student should have proper understanding of configurations as outlined in this chapter. Additionally, there are a number of abbreviations in this chapter; the student will be required to familiarise with them and their applications as they can easily confuse the student.

▶ INDUSTRY CONTEXT

Users and network administrators often have different views of their networks. Often, users share printers and some servers form a workgroup, which usually means they are in the same

geographic location and are on the same LAN. A community of interest has less of a connotation of being in a local area, and should be thought of as a set of arbitrarily located users who share a set of servers, and possibly also communicate via peer-to-peer technologies.

Fast Forward: The network allows computers to communicate with each other and share resources and information.

1. Principles of data communication

Data communication systems are the electronic systems that transmit data over communication lines from one location to another. End users need to know the essential parts of communication technology, including connections, channels, transmission, network architectures and network types. Communication allows microcomputer users to transmit and receive data and gain access to electronic resources.

- Source – creates the data, could be a computer or a telephone
- Transmitter – encodes the information e.g. modem, network card
- Transmission system – transfers the information e.g. wire or complex network
- Receiver – decodes the information for the destination e.g. modem, network card
- Destination – accepts and uses the incoming information, could be a computer or telephone

1.1 Communication channels

The transmission media used in communication are called communication channels. Two ways of connecting microcomputers for communication with each other and with other equipment is through cable and air. There are five kinds of communication channels used for cable or air connections:

- Telephone lines
- Coaxial cable
- Fibre-optic cable
- Microwave
- Satellite

Telephone lines (Twisted Pair)

Telephone line cables made up of copper wires called twisted pair. A single twisted pair culminates

in a wall jack where you plug your phone. Telephone lines have been the standard communication channel for both voice and data. More technically advanced and reliable transmission media are now replacing it.

Coaxial cable

This is a high-frequency transmission cable that replaces the multiple wires of telephone lines with a single solid copper core. It has over 80 times the transmission capacity of twisted pair. It is often used to link parts of a computer system in one building.

Fibre-optic cable

Fibre-optic cable transmits data as pulses of light through tubes of glass. It has over 26,000 times the transmission capacity of twisted pair. A fibre-optic tube can be half the diameter of human hair. Fibre-optic cables are immune to electronic interference and more secure and reliable. Fibre-optic cable is rapidly replacing twisted-pair telephone lines.

Microwave

Microwaves transmit data as high-frequency radio waves that travel in straight lines through air. Microwaves cannot bend with the curvature of the earth. They can only be transmitted over short distances. Microwaves are good medium for sending data between buildings in a city or on a large college campus. Microwave transmission over longer distances is relayed by means of 'dishes' or antennas installed on towers, high buildings or mountaintops.

Satellite

Satellites are used to amplify and relay microwave signals from one transmitter on the ground to another. They orbit about 22,000 miles above the earth. They rotate at a precise point and speed and can be used to send large volumes of data. Bad weather can sometimes interrupt the flow of data from a satellite transmission. INTELSAT (INternational TELecommunication SATellite consortium), owned by 114 governments forming a worldwide communications system, offers many satellites that can be used as microwave relay stations.

2. Data transmission: analog versus digital

Information is available in an analogue or in a digital form. Computer-generated data can easily be stored in a digital format, but analogue signals, such as speech and video, must first be sampled at regular intervals and then converted into a digital form. This process is known as digitisation and has the following advantages:

- Digital data is less affected by noise
- Extra information can be added to digital signals so that errors can either be detected or corrected.
- Digital data tends not to degrade over time.
- Processing of digital information is relatively easy, either in real-time or non real-time.
- A single type of media can be used to store many different types of information (such as video, speech, audio and computer data can be stored on tape, hard-disk or CD-

ROM).

- A digital system has a more dependable response, whereas an analogue system's accuracy depends on parameters such as component tolerance, temperature, power supply variations, and so on. Analogue systems thus produce a variable response and no two analogue systems are identical.
- Digital systems are more adaptable and can be reprogrammed with software. Analogue systems normally require a change of hardware for any functional changes (although programmable analogue devices are now available).

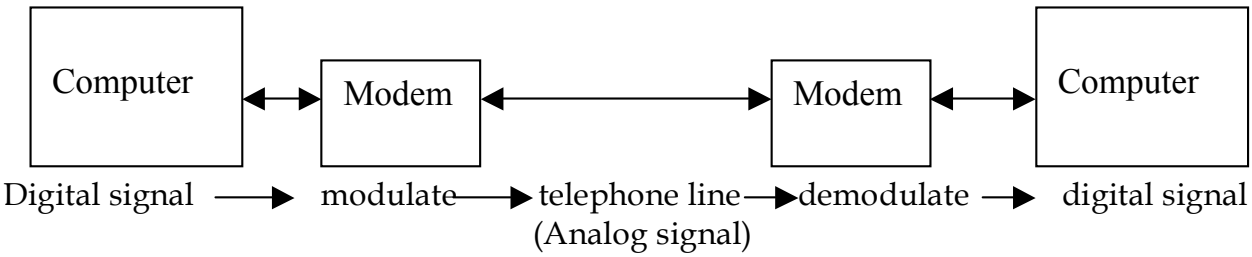
The main disadvantage with digital conversion is:

- Digital samples must be quantised to given levels: this adds an error called quantisation error. The larger the number of bits used to represent each sample, the smaller the quantisation error.

2.1 Modem

A modem is a hardware device that converts computer signals (digital signals) to telephone signals (analog signals) and vice versa.

The process of converting digital signals to analog is called modulation while the process of converting analog signals to digital is called demodulation.



Modem transmission speed

The speed with which modems transmit data varies. Communications speed is typically measured in bits per second (bps). The most popular speeds for conventional modems are 36.6 kbps (36,600 bps) and 56kbps (56,000 bps). The higher the speed, the faster you can send and receive data.

Types of modems

a) External modem

An external modem stands apart from the computer. It is connected by a cable to the computer's serial port. Another cable is used to connect the modem to the telephone wall jack.

b) Internal modem

An internal modem is a plug-in circuit board inside the system unit. A telephone cable connects this type of modem to the telephone wall jack.

c) Wireless modem

A wireless modem is similar to an external modem. It connects to the computer's serial port, but does not connect to telephone lines. It uses new technology that receives data through the air.

2.2 Data transmission

Technical matters that affect data transmission include:

- Bandwidth
- Type of transmission
- Direction of data flow
- Mode of transmitting data
- Protocols

Bandwidth

Bandwidth is the bits-per-second (bps) transmission capability of a communication channel. **There are three types of bandwidth:**

- Voice band – bandwidth of standard telephone lines (9.6 to56 kbps)
- Medium band – bandwidth of special leased lines used (56 to 264,000 kbps)
- Broadband – bandwidth of microwave, satellite, coaxial cable and fiber optic (56 to 30,000,000 kbps).

>> Types of transmission – serial or parallel

Serial data transmission

In serial transmission, bits flow in a continuous stream. It is the way most data is sent over telephone lines. It is used by external modems typically connected to a microcomputer through a serial port. The technical names for such serial ports are RS-232C connector or asynchronous communications port.

Parallel data transmission

In parallel transmission, bits flow through separate lines simultaneously (at the same time). Parallel transmission is typically limited to communications over short distances (not telephone lines). It is the standard method of sending data from a computer's CPU to a printer.

>> Direction of data transmission

There are three directions or modes of data flow in a data communication system.

- Simplex communication – data travels in one-direction only e.g. point-of-sale terminals.
- Half-duplex communication – data flows in both directions, but not simultaneously. E.g. electronic bulletin board
- Full-duplex communication – data is transmitted back and forth at the same time e.g. mainframe communications.

>> Mode of data transmission

Data may be sent over communication channels in either asynchronous or synchronous mode.

- Asynchronous transmission – data is sent and received one byte at a time. Used with microcomputers and terminals with slow speeds.
- Synchronous transmission – data is sent and received several bytes (blocks) at a time. It requires a synchronised clock to enable transmission at timed intervals.

>> Protocols

These are sets of communication rules for exchange of information. Protocols define speeds and modes for connecting one computer with another. Network protocols can become very complex and therefore must adhere to certain standards. The first set of protocol standards was IBM Systems Network Architecture (SNA), which only works for IBM's own equipment.

The Open Systems Interconnection (OSI) is a set of communication protocols defined by International Standards Organisation. The OSI is used to identify functions provided by any network and separates each network's functions into seven 'layers' of communication rules.

>> Error detection and control

Data has to arrive intact in order to be used. Two techniques are used to detect and correct errors:

a) Forward error control – additional redundant information is transmitted with each character or frame so that the receiver cannot only detect when errors are present, but can also determine where the error has occurred and thus corrects it.
b) Feedback (backward) error control – only enough additional information is transmitted so that the receiver can identify that an error has occurred. An associated retransmission control scheme is then used to request that another copy of the information be sent.

Error detection methods include:

- Parity check – the transmitter adds an additional bit to each character prior to transmission. The parity bit used is a function of the bits making up the character. The recipient performs the same function on the received character and compares it to the parity bit. If it is different an error is assumed.

- Block sum check – an extension of the parity check in that an additional set of parity bits is computed for a block of characters (or frame). The set of parity bits is known as the block (sum) check character.

- Cyclic Redundancy Check (CRC) – the CRC or frame check sequence (FCS) is used for situations where bursts of errors may be present (parity and block sum checks are not effective at detecting bursts of errors). A single set of check digits is generated for each frame transmitted, based on the contents of the frame and appended to the tail of the frame.

>> Recovery

When errors are so bad and that you can't ignore them, have a new plan to get the data.

>> Security

What are you concerned about if you want to send an important message?

- Did the receiver get it?
  - Denial of service
- Is it the right receiver?
  - Receiver spoofing
- Is it the right message?
  - Message corruption
- Did it come from the right sender?
  - Sender spoofing

>> Network management

This involves configuration, provisioning, monitoring and problem-solving.

3. Computer networks

A computer network is a communications system connecting two or more computers that work to exchange information and share resources (hardware, software and data). A network may consist of microcomputers or it may integrate microcomputers or other devices with larger computers. Networks may be controlled by all nodes working together equally or by specialised nodes coordinating and supplying all resources. Networks may be simple or complex, self-contained or dispersed over a large geographical area.

Network architecture is a description of how a computer is set-up (configured) and what strategies are used in the design. The interconnection of PCs over a network is becoming more important, especially as more hardware is accessed remotely and PCs intercommunicate with one another.

3.1 Terms used to describe computer networks

- Node – any device connected to a network such as a computer, printer or data storage device.
- Client – a node that requests and uses resources available from other nodes. Typically a microcomputer.
- Server – a node that shares resources with other nodes. May be called a file server, printer server, communication server, web server or database server.
- Network Operating System (NOS) – the operating system of the network that controls and coordinates the activities between computers on a network, such as electronic communication and sharing of information and resources.
- Distributed processing – computing power is located and shared at different locations. Common in decentralised organisations (each office has its own computer system but is networked to the main computer).
- Host computer – a large centralised computer, usually a minicomputer or mainframe.

3.2 Types of computer networks

Different communication channels allow different types of networks to be formed. Telephone lines may connect communications equipment within the same building. Coaxial cable or fibre-optic cable can be installed on building walls to form communication networks. You can also create your own network in your home or apartment. Communication networks also differ in geographical size.

Three important networks according to geographical size are LANs, MANs and WANs.

Local Area Network (LAN)

A LAN is a computer network in which computers and peripheral devices are in close physical proximity. It is a collection of computers within a single office or building that connect to a common electronic connection – commonly known as a network backbone. This type of network typically uses microcomputers in a busy organisation linked with telephone, coaxial or fibre-optic cable. A LAN allows all users to share hardware, software and data on the network. Minicomputers, mainframes or optical disk storage devices can be added to the network. A network bridge device may be used to link a LAN to other networks with the same configuration. A network gateway device may be used to link a LAN to other networks, even if their configurations are different.

Metropolitan Area Network (MAN)

A MAN is a computer network that may be citywide. This type of network may be used as a link between office buildings in a city. The use of cellular phone systems expands the flexibility of a MAN network by linking car phones and portable phones to the network.

Wide Area Networks (WAN)

A WAN is a computer network that may be countrywide or worldwide. It normally connects networks over a large physical area, such as in different buildings, towns or even countries. A modem connects a LAN to a WAN when the WAN connection is an analogue line.

For a digital connection, a gateway connects one type of LAN to another LAN or WAN, and a bridge connects a LAN to similar types of LAN. This type of network typically uses microwave relays and satellites to reach users over long distances. The widest of all WANs is the Internet, which spans the entire globe.

WAN technologies

How you get from one computer to the other across the Internet.

(i) Circuit switching
- A dedicated path between machines is established.
- All resources are guaranteed.
- Has limitation of set-up delay but has fast transmission.

(ii) Packet switching
- Nodes in the network ‘routers’ decide where to send data next.

- No resources are guaranteed “best effort”.
- Little set-up, transmission delay at each router.
- Computer-computer communication.

(iii) Frame relay
- Like packet switching
- Low level error correction removed to yield higher data rates.

(iv) Cell relay – ATM (Asynchronous Transmission Mode)
- Frame relay with uniformly sized packets (cells).
- Dedicated circuit paths.

(v) ISDN (Integrated Services Digital Network)
- Transmits voice and data traffic.
  Specialised circuit switching.
- Uses frame relay (narrowband) and ATM (broadband).

3.3 Configurations

A computer network configuration is also called its topology. The topology is the method of arranging and connecting the nodes of a network. There are four principal network topologies:

a) Star
b) Bus
c) Ring
d) Hierarchical (hybrid)
e) Completely connected (mesh)

Star network

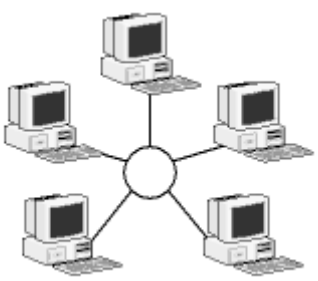
In a star network there are a number of small computers or peripheral devices linked to a central unit called a main hub. The central unit may be a host computer or a file server. All communications pass through the central unit and control is maintained by polling. This type of network can be used to provide a time-sharing system and is common for linking microcomputers to a mainframe.

Advantages:

- It is easy to add new and remove nodes
- A node failure does not bring down the entire network
- It is easier to diagnose network problems through a central hub

Disadvantages:

- If the central hub fails, the whole network ceases to function
- It costs more to cable a star configuration than other topologies (more cable is required than for a bus or ring configuration).



Node

Bus network

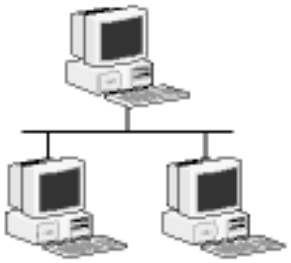
In a bus network each device handles its communications control. There is no host computer; however there may be a file server. All communications travel along a common connecting cable called a bus. It is a common arrangement for sharing data stored on different microcomputers. It is not as efficient as star network for sharing common resources, but is less expensive. The distinguishing feature is that all devices (nodes) are linked along one communication line - with endpoints - called the bus or backbone.

Advantages:

- Reliable in very small networks as well as easy to use and understand
- Requires the least amount of cable to connect the computers together and therefore is less expensive than other cabling arrangements.
- Is easy to extend. Two cables can be easily joined with a connector, making a longer cable for more computers to join the network
- A repeater can also be used to extend a bus configuration

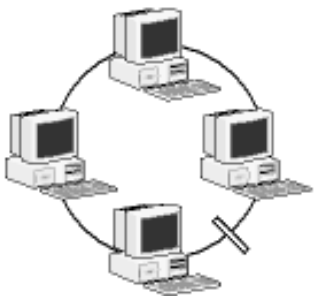
Disadvantages:

- Heavy network traffic can also slow down a bus considerably. Because any computer can transmit at any time, bus networks do not coordinate when information is sent. Computers interrupting each other can use a lot of bandwidth.
- Each connection between two cables weakens the electrical signal.
- The bus configuration can be difficult to troubleshoot. A cable break or malfunctioning computer can be difficult to find and can cause the whole network to stop functioning.



Ring network

In a ring network, each device is connected to two other devices, forming a ring. There is no central file server or computer. Messages are passed around the ring until they reach their destination. Often used to link mainframes, especially over wide geographical areas. It is useful in a decentralised organisation called a distributed data processing system.



Advantages:

- Ring networks offer high performance for a small number of workstations or for larger

networks where each station has a similar work load.
- Ring networks can span longer distances than other types of networks.
- Ring networks are easily extendable.

Disadvantages

- Relatively expensive and difficult to install.
- Failure of one component on the network can affect the whole network.
- It is difficult to troubleshoot a ring network.
- Adding or removing computers can disrupt the network.

Hierarchical (hybrid) network

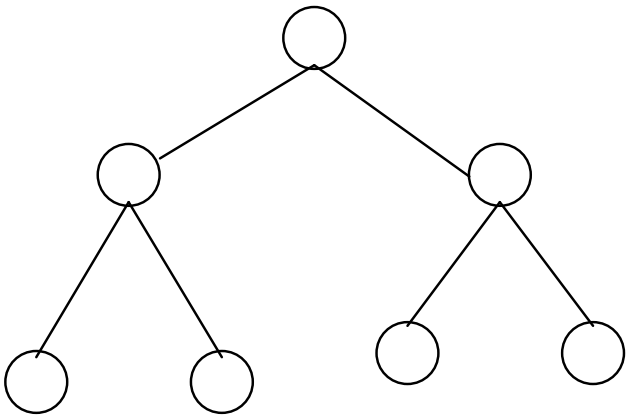
A hierarchical network consists of several computers linked to a central host computer. It is similar to a star. Other computers are also hosts to other, smaller computers or to peripheral devices in this type of network. It allows various computers to share databases, process power and different output devices. It is useful in centralised organisations.

Advantages:

- Improves sharing of data and programmes across the network.
- Offers reliable communication between nodes.

Disadvantages:

- Difficult and costly to install and maintain.
- Difficult to troubleshoot network problems.



Completely connected (mesh) configuration

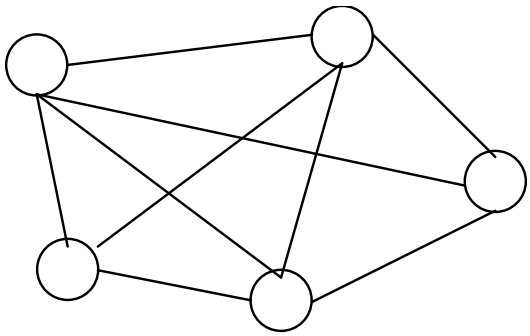
Is a network topology in which devices are connected with many redundant interconnections between network nodes.

Advantages:

- Yields the greatest amount of redundancy (multiple connections between same nodes) in the event that one of the nodes fails where network traffic can be redirected to another node.
- Network problems are easier to diagnose.

Disadvantages

- The cost of installation and maintenance is high (more cable is required than any other configuration)



3.4 Client/Server environment

Use of client/server technology is one of the most popular trends in application development. More and more business applications have embraced the advantages of the client/server architecture by distributing the work among servers and by performing as much computational work as possible on the client workstation. This allows users to manipulate and change the data that they need to change without controlling resources on the main processing unit.

In client/server systems, applications no longer are limited to running on one machine. The applications are split so that processing may take place on different machines. The processing of data takes place on the server and the desktop computer (client). The application is divided into pieces or tasks so processing can be done more efficiently.

A client/server network environment is one in which one computer acts as the server and provides data distribution and security functions to other computers that are independently running various applications. An example of the simplest client/server model is a LAN whereby a set of computers is linked to allow individuals to share data. LANs (like other client/server environments) allow users to maintain individual control over how information is processed.

Client/server computing differs from mainframe or distributed system processing in that each processing component is mutually dependent. The 'client' is a single PC or workstation associated with software that provides computer presentation services as an interface to server computing resources. Presentation is usually provided by visually enhanced processing software known as a Graphical User Interface (GUI). The 'server' is one or more multi-user computer(s) (these may be mainframes, minicomputers or PCs). Server functions include any centrally supported role, such as file sharing, printer sharing, database access and management, communication services, facsimile services, application development and others. Multiple functions may be supported by a single server.

3.5 Network protocols

Protocols are the set of conventions or rules for interaction at all levels of data transfer. They have three main components:

- Syntax – data format and signal types
- Semantics – control information and error handling
- Timing – data flow rate and sequencing

Numerous protocols are involved in transferring a single file even when two computers are directly connected. The large task of transferring a piece of data is broken down into distinct subtasks. There are multiple ways to accomplish each task (individual protocols). The tasks are well described so that they can be used interchangeably without affecting the overall system.

Benefits derived from using network protocols include:

- Smaller user applications – the browser runs HTTP (Hyper Text Transfer Protocol). It isn't aware of how the connection to the network is made.
- Can take advantage of new technologies – one can browse on a wireless palm or cell phone
- Don't have to reinvent the wheel – fewer programming errors, less effort during development of network-oriented application systems as previous components are reused.
- Enhanced uniformity in communication

Common network protocols include:

(i) Three-layer logical model
(ii) TCP/IP (Transmission Control Protocol/Internet Protocol)
(iii) ISO/OSI model (International Organisations for Standards/Open System Interconnection)

Three (3) layer logical model

- Application Layer
  - Takes care of the needs of the specific application
  - HTTP: send request, get a batch of responses from a bunch of different servers
  - Telnet: dedicated interaction with another machine

- Transport Layer
  - Makes sure data is exchanged reliably between the two end systems
  - Needs to know how to identify the remote system and package the data properly

- Network Access Layer
  - Makes sure data is exchanged reliably into and out of the computer.
  - Concerns the physical connection to the network and transfer of information across this connection
  - Software here depends on physical medium used

TCP/IP (Transmission Control Protocol/Internet Protocol)

- **Application Layer**
  - User application protocols
- **Transport Layer**
  - Transmission control protocol
  - Data reliability and sequencing
- **Internet Layer**
  - Internet Protocol
  - Addressing, routing data across Internet
- **Network Access Layer**
  - Data exchange between host and local network

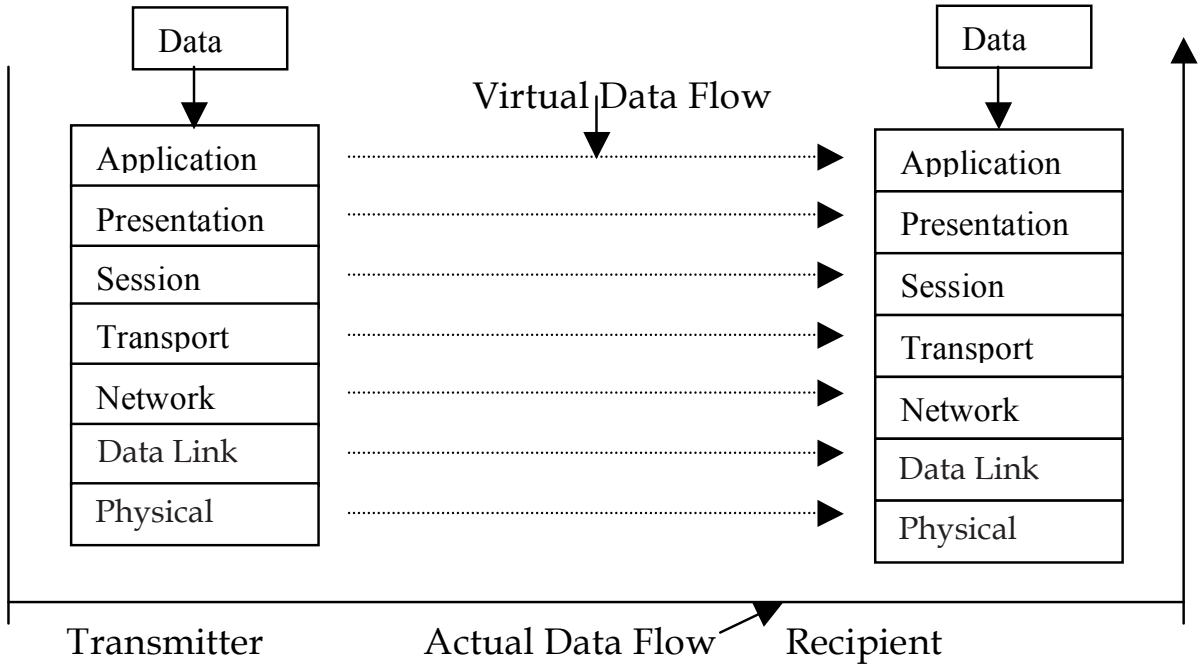
- Packets, flow control
- Network dependent (circuit switching, Ethernet etc)

• Physical Layer
  - Physical interface, signal type, data rate

ISO/OSI Model (International Standard Organisation/Open System Interconnection)

An important concept in understanding data communications is the Open Systems Interconnection (OSI) model. It allows manufacturers of different systems to interconnect their equipment through standard interfaces. It also allows software and hardware to integrate well and be portable on differing systems. The International Standards Organisation (ISO) developed the model.

Data is passed from top layer of the transmitter to the bottom, then up from the bottom layer to the top on the recipient. However, each layer on the transmitter communicates directly with the recipient's corresponding layer. This creates a virtual data flow between layers. The data sent can be termed as a data packet or data frame.



>> 1. Application Layer

This layer provides network services to application programmes such as file transfer and electronic mail. It offers user level interaction with network programmes and provides user application, process and management functions.

>> 2. Presentation Layer

The presentation layer uses a set of translations that allow the data to be interpreted properly. It may have to carry out translations between two systems if they use different presentation standards such as different character sets or different character codes. It can also add data encryption for security purposes. It basically performs data interpretation, format and control transformation. It separates what is communicated from data representation.

>> 3. Session Layer

The session layer provides an open communications path to the other system. It involves setting up, maintaining and closing down a session (a communication time span). The communications channel and the internetworking should be transparent to the session layer. It manages (administration and control) sessions between cooperating applications.

>> 4. Transport Layer

If data packets require to go out of a network, then the transport layer routes them through the interconnected networks. Its task may involve splitting up data for transmission and reassembling it after arrival. It performs the tasks of end-to-end packetisation, error control, flow control, and synchronisation. It offers network transparent data transfer and transmission control.

>> 5. Network Layer

The network layer routes data frames through a network. It performs the tasks of connection management, routing, switching and flow control over a network.

>> 6. Data Link Layer

The data link layer ensures that the transmitted bits are received in a reliable way. This includes adding bits to define the start and end of a data frame, adding extra error detection/correction bits and ensuring that multiple nodes do not try to access a common communications channel at the same time. It has the tasks of maintaining and releasing the data link, synchronisation, error and flow control.

>> 7. Physical Layer

The physical link layer defines the electrical characteristics of the communications channel and the transmitted signals. This includes voltage levels, connector types, cabling, data rate, etc. It provides the physical interface.

3.6 Network cable types

The cable type used on a network depends on several parameters including:

- The data bit rate
- The reliability of the cable
- The maximum length between nodes
- The possibility of electrical hazards
- Power loss in cables
- Tolerance or harsh conditions
- Expense and general availability of the cache
- Ease of connection and maintenance
- Ease of running cables

The main types of cables used in networks are twisted-pair, coaxial and fibre-optic. Twisted-pair and coaxial cables transmit electric signals, whereas fibre-optic cables transmit light pulses. Twisted-pair cables are not shielded and thus interfere with nearby cables. Public telephone lines generally use twisted-pair cables. In LANs, they are generally used up to bit rates of 10 Mbps and with maximum lengths of 100m.

Coaxial cable has a grounded metal sheath around the signal conductor. This limits the amount of interference between cables and thus allows higher data rates. Typically they are used at bit rates of 100 Mbps for maximum lengths of 1 km.

The highest specification of the three cables is fibre-optic. This type of cable allows extremely high bit rates over long distances. Fibre-optic cables do not interfere with nearby cables and give greater security, more protection from electrical damage by external equipment and greater resistance to harsh environments; it is also safer in hazardous environments.

3.7 Internetworking connections

Most modern networks have a backbone, which is a common link to all the networks within an organisation. This backbone allows users on different network segments to communicate and also allows data into and out of the local network.

Networks are partitioned from other networks using a bridge, a gateway or a router. A **bridge** links two networks of the same type. A **gateway** connects two networks of dissimilar type. **Routers** operate rather like gateways and can either connect two similar networks or two dissimilar networks. The key operation of a gateway, bridge or router is that it only allows data traffic through itself when the data is intended for another network, which is outside the connected network. This filters traffic and stops traffic not intended for the network from clogging up the backbone. Modern bridges, gateways and routers are intelligent and can determine the network topology. A **spanning-tree bridge** allows multiple network segments to be interconnected. If more than one path exists between individual segments, then the bridge finds alternative routes. This is useful in routing frames away from heavy traffic routes or around a faulty route.

A **repeater** is used to increase the maximum interconnection length since, for a given cable specification and bit rate, each has a maximum length of cable.

3.8 Network Standards

Standards are good because they allow many different implementations of interoperable technology. However they are slow to develop and multiple standard organisations develop different standards for the same functions.

3.9 Application of computer networks within an organisation

Connectivity is the ability and means to link a microcomputer by telephone or other telecommunication links to other computers and information sources around the world.

The connectivity options that make communication available to end-users include:

- Fax machines (Facsimile transmission machines)
- E-mail (Electronic mail)
- Voice messaging systems
- Video conferencing systems

- Shared resources
- Online services

Fax machines

Fax machines convert images to signals that can be sent over a telephone line to a receiving machine. They are extremely popular in offices. They can scan the image of a document and print the image on paper. Microcomputers use fax/modem circuit boards to send and receive fax messages.

E-mail (electronic mail)

E-mail is a method of sending an electronic message between individuals or computers. One can receive e-mail messages even when one is not on the computer. E-mail messages can contain text, graphics, images as well as sound.

Voice messaging systems

Voice messaging systems are computer systems linked to telephones that convert human voice into digital bits. They resemble conventional answering machines and electronic mail systems. They can receive large numbers of incoming calls and route them to appropriate 'voice mailboxes' which are recorded voice messages. They can forward calls and deliver the same message to many people.

Video conferencing systems

Video conferencing systems are computer systems that allow people located at various geographic locations to have in-person meetings. They can use specially equipped videoconferencing rooms to hold meetings. Desktop videoconferencing systems use microcomputers equipped with inexpensive video cameras and microphones that sit atop a computer monitor.

Shared resources

Shared resources are communication networks that permit microcomputers to share expensive hardware such as laser printers, chain printers, disk packs and magnetic tape storage. Several microcomputers linked in a network make shared resources possible. The connectivity capabilities of shared resources provide the ability to share data located on a computer.

Online services

Online services are business services offered specifically for microcomputer users. Well-known online service providers are America Online (AOL), AT&T WorldNet, CompuServe, Africa Online, Kenyaweb, UUNET, Wananchi Online and Microsoft Network. Typical online services offered by these providers are:

Teleshopping - a database which lists prices and description of products. You place an order, charge the purchase to a credit card and merchandise is delivered by a delivery service.

Home banking – banks offer this service so you can use your microcomputer to pay bills, make loan payments, or transfer money between accounts.

Investing – investment firms offer this service so you can access current prices of stocks and bonds. You can also buy and sell orders.

Travel reservations – travel organisations offer this service so you can get information on airline schedules and fare, order tickets and charge to a credit card.

Internet access – you can get access to the World Wide Web.

Internet

Fast Forward: The movement of information in the Internet is achieved via a system of interconnected computer networks that share data by packet switching using the standardised Internet Protocol Suite (TCP/IP).

The **Internet** is a giant worldwide network. The Internet started in 1969 when the United States government funded a major research project on computer networking called ARPANET (Advanced Research Project Agency NETwork). When on the Internet you move through cyberspace.

Cyberspace is the space of electronic movement of ideas and information.

The **web** provides a multimedia interface to resources available on the Internet. It is also known as WWW or World Wide Web. The web was first introduced in 1992 at CERN (Centre for European Nuclear Research) in Switzerland. Prior to the web, the Internet was all text with no graphics, animations, sound or video.

Common Internet applications

- Communicating
  - Communicating on the Internet includes e-mail, discussion groups (newsgroups), and chat groups.
  - You can use e-mail to send or receive messages to people around the world.
  - You can join discussion groups or chat groups on various topics.
- Shopping
  - Shopping on the Internet is called e-commerce,
  - You can window shop at cyber malls called web storefronts
  - You can purchase goods using cheques, credit cards or electronic cash called electronic payment.
- Researching
  - You can do research on the Internet by visiting virtual libraries and browse through stacks of books.
  - You can read selected items at the virtual libraries and even check out books.
- Entertainment
  - There are many entertainment sites on the Internet such as live concerts, movie previews and book clubs.
  - You can also participate in interactive live games on the Internet.

How do you get connected to the Internet?

You get connected to the Internet through a computer. Connection to the Internet is referred to

as access to the Internet. Using a provider is one of the most common ways users can access the Internet. A provider is also called a host computer and is already connected to the Internet. A provider provides a path or connection for individuals to access the Internet.

There are three widely used providers:

(i) **Colleges and universities** – colleges and universities provide free access to the Internet through their Local Area Networks,
(ii) **Internet Service Providers (ISP)** – ISPs offer access to the Internet at a fee. They are more expensive than online service providers.
(iii) **Online Service Providers** – provide access to the Internet and a variety of other services at a fee. They are the most widely used source for Internet access and less expensive than ISP.

Connections

There are three types of connections to the Internet through a provider:

- Direct or dedicated
- SLIP and PPP
- Terminal connection

Direct or dedicated

This is the most efficient access method to all functions on the Internet. However, it is expensive and rarely used by individuals. It is used by many organisations such as colleges, universities, service providers and corporations.

SLIP and PPP

This type of connection is widely used by end users to connect to the Internet. It is slower and less convenient than direct connection. However, it provides a high level of service at a lower cost than direct connection. It uses a high-speed modem and standard telephone line to connect to a provider that has a direct connection to the Internet. It requires special software protocol: SLIP (Serial Line Internet Protocol) or PPP (Point-to-Point Protocol). With this type of connection, your computer becomes part of a client/server network. It requires special client software to communicate with server software running on the provider's computer and other Internet computers.

Terminal connection

This type of connection also uses a high-speed modem and standard telephone line. Your computer becomes part of a terminal network with a terminal connection. With this connection, your computer's operations are very limited because it only displays communication that occurs between provider and other computers on the Internet. It is less expensive than SLIP or PPP but not as fast or convenient.

Internet protocols

TCP/IP

The standard protocol for the Internet is TCP/IP. TCP/IP (Transmission Control Protocol/Internet

Protocol) are the rules for communicating over the Internet. Protocols control how the messages are broken down, sent and reassembled. With TCP/IP, a message is broken down into small parts called packets before it is sent over the Internet. Each packet is sent separately, possibly travelling through different routes to a common destination. The packets are reassembled into correct order at the receiving computer.

Internet services

The four commonly used services on the Internet are:

- Telnet
- FTP
- Gopher
- The Web

Telnet

- Telnet allows you to connect to another computer (host) on the Internet.
- With Telnet you can log on to the computer as if you were a terminal connected to it.
- There are hundreds of computers on the Internet you can connect to.
- Some computers allow free access; some charge a fee for their use.

FTP (File Transfer Protocol)

- FTP allows you to copy files on the Internet
- If you copy a file from an Internet computer to your computer, it is called downloading.
- If you copy a file from your computer to an Internet computer, it is called uploading.

Gopher

- Gopher allows you to search and retrieve information at a particular computer site called a gopher site.
- Gopher is a software application that provides menu-based functions for the site.
- It was originally developed at the University of Minnesota in 1991.
- Gopher sites are computers that provide direct links to available resources, which may be on other computers.
- Gopher sites can also handle FTP and Telnet to complete their retrieval functions.

The Web

- The web is a multimedia interface to resources available on the Internet.
- It connects computers and resources throughout the world.
- It should not be confused with the term Internet.

Browser

- A browser is a special software used on a computer to access the web.
- The software provides an uncomplicated interface to the Internet and web documents.
- It can be used to connect you to remote computers using Telnet.
- It can be used to open and transfer files using FTP.
- It can be used to display text and images using the web.
- Two well-known browsers are:

- Netscape communicator
- Microsoft Internet Explorer

Uniform Resource Locators (URLs)

- URLs are addresses used by browsers to connect to other resources.
- URLs have at least two basic parts.
  - Protocol – used to connect to the resource, HTTP (Hyper Text Transfer Protocol) is the most common.
  - Domain Name – the name of the server where the resource is located.
- Many URLs have additional parts specifying directory paths, file names and pointers.
- Connecting to a URL means that you are connecting to another location called a web site.
- Moving from one web site to another is called surfing.

Web portals

Web portals are sites that offer a variety of services typically including e-mail, sports updates, financial data, news and links to selected websites. They are designed to encourage you to visit them each time you access the web. They act as your home base and as a gateway to their resources.

Web pages

A web page is a document file sent to your computer when the browser has connected to a website. The document file may be located on a local computer or halfway around the world. The document file is formatted and displayed on your screen as a web page through the interpretation of special command codes embedded in the document called HTML (Hyper Text Mark-up Language).

Typically, the first web page on a website is referred to as the home page. The home page presents information about the site and may contain references and connections to other documents or sites called hyperlinks. Hyperlink connections may contain text files, graphic images, audio and video clips. Hyperlink connections can be accessed by clicking on the hyperlink.

Applets and Java

- Web pages contain links to special programmes called applets written in a programming language called Java.
- Java applets are widely used to add interest and activity to a website.
- Applets can provide animation, graphics, interactive games and more.
- Applets can be downloaded and run by most browsers.

Search tools

Search tools developed for the Internet help users locate precise information. To access a search tool, you must visit a web site that has a search tool available. There are two basic types of search tools available:

- Indexes
- Search engines

Indexes

- Indexes are also known as web directories.
- They are organised by major categories e.g. health, entertainment, education, etc.
- Each category is further organised into sub-categories
- Users can continue to search of subcategories until a list of relevant documents appear
- The best known search index is Yahoo.

Search engines

- Search engines are also known as web crawlers or web spiders.
- They are organised like a database.
- Key words and phrases can be used to search through a database.
- Databases are maintained by special programmes called agents, spiders or bots.
- Widely used search engines are Google, HotBot and AltaVista.

Web utilities

Web utilities are programmes that work with a browser to increase your speed, productivity and capabilities. These utilities can be included in a browser. Some utilities may be free on the Internet while others can be charged a nominal fee. There are two categories of web utilities:

- Plug-ins
- Helper applications

Plug-ins

- A plug-in is a programme that automatically loads and operates as part of your browser.
- Many websites require plug-ins for users to fully experience web page contents
- Some widely used plug-ins are:
  - Shockwave from macromedia – used for web-based games, live concerts and dynamic animations.
  - QuickTime from Apple – used to display video and play audio.
  - Live-3D from Netscape – used to display three-dimensional graphics and virtual reality.

Helper applications

Helper applications are also known as add-ons. They are independent programmes that can be executed or launched from your browser. The four most common types of helper applications are:

- Off-line browsers – also known as web-downloading utilities and pull products. It is a programme that automatically connects you to selected websites. They download HTML documents before saving them to your hard disk. The document can be read latter without being connected to the Internet.
- Information pushers – also known as web broadcasters or push products. They automatically gather information on topic areas called channels. The topics are then sent to your hard disk. The information can be read later without being connected to the Internet.
- Metasearch utilities – offline search utilities are also known as metasearch programmes.

They automatically submit search requests to several indices and search engines. They receive the results, sort them, eliminate duplicates and create an index.

- Filters – filters are programmes that allow parents or organisations to block out selected sites e.g. adult sites. They can monitor the usage and generate reports detailing time spent on activities.

Discussion groups

There are several types of discussion groups on the Internet:

- Mailing lists
- Newsgroups
- Chat groups

Mailing lists

In this type of discussion groups, members communicate by sending messages to a list address. To join, you send your e-mail request to the mailing list subscription address. To cancel, send your email request to unsubscribe to the subscription address.

Newsgroups

Newsgroups are the most popular type of discussion group. They use a special type of computers called UseNet. Each UseNet computer maintains the newsgroup listing. There are over 10,000 different newsgroups organised into major topic areas. Newsgroup organisation hierarchy system is similar to the domain name system. Contributions to a particular newsgroup are sent to one of the UseNet computers. UseNet computers save messages and periodically share them with other UseNet computers. Interested individuals can read contributions to a newsgroup.

Chat groups

Chat groups are becoming a very popular type of discussion group. They allow direct 'live' communication (real time communication). To participate in a chat group, you need to join by selecting a channel or a topic. You communicate live with others by typing words on your computer. Other members of your channel immediately see the words on their computers and they can respond. The most popular chat service is called Internet Relay Chat (IRC), which requires special chat client software.

Instant messaging

Instant messaging is a tool to communicate and collaborate with others. It allows one or more people to communicate with direct 'live' communication. It is similar to chat groups, but it provides greater control and flexibility. To use instant messaging, you specify a list of friends (buddies) and register with an instant messaging server e.g. Yahoo Messenger. Whenever you connect to the Internet, special software will notify your messaging server that you are online. It will notify you if any of your friends are online and will also notify your buddies that you are online.

E-mail (Electronic Mail)

E-mail is the most common Internet activity. It allows you to send messages to anyone in the world who has an Internet e-mail account. You need access to the Internet and e-mail programme

to use this type of communication. Two widely used e-mail programmes are Microsoft's Outlook Express and Netscape's Communicator.

E-mail has three basic elements:

(i) Header – appears first in an e-mail message and contains the following information
   a. Address – the address of the person(s) that is to receive the e-mail.
   b. Subject – a one line description of the message displayed when a person checks their mail.
   c. Attachment – files that can be sent by the e-mail programme.
(ii) Message – the text of the e-mail communication.
(iii) Signature – may include sender's name, address and telephone number (optional).

E-mail addresses

The most important element of an e-mail message is the address of the person who is to receive the letter. The Internet uses an addressing method known as the Domain Name System (DNS). The system divides an address into three parts:

(i) User name – identifies a unique person or computer at the listed domain.
(ii) Domain name – refers to a particular organisation.
(iii) Domain code – identifies the geographical or organisational area.

Almost all ISPs and online service providers offer e-mail service to their customers.

The main advantages of email are:

- It is normally much cheaper than using the telephone (although, as time equates to money for most companies, this relates any savings or costs to a user's typing speed).
- Many different types of data can be transmitted, such as images, documents, speech, etc.
- It is much faster than the postal service.
- Users can filter incoming email easier than incoming telephone calls.
- It normally cuts out the need for work to be typed, edited and printed by a secretary.
- It reduces the burden on the mailroom.
- It is normally more secure than traditional methods.
- It is relatively easy to send to groups of people (traditionally, either a circulation list was required or a copy to everyone in the group was required).
- It is usually possible to determine whether the recipient has actually read the message (the electronic mail system sends back an acknowledgement).

The main disadvantages are:

- It stops people from using the telephone
- It cannot be used as a legal document
- Electronic mail messages can be sent on the spur of the moment and may be regretted later on (sending by traditional methods normally allows for a rethink). In extreme cases, messages can be sent to the wrong person (typically when replying to an email message, where a messages is sent to the mailing list rather than the originator).
- It may be difficult to send to some remote sites. Many organisations have either no electronic mail or merely an intranet. Large companies are particularly wary of Internet

connections and limit the amount of external traffic.
- Not everyone reads his or her electronic mail on a regular basis (although this is changing as more organizations adopt email as the standard communication medium).

The main standards that relate to the protocols of email transmission and reception are:

- **Simple Mail Transfer Protocol (SMTP) –** which is used with the TCP/IP suite. It has traditionally been limited to the text-based electronic messages.
- **Multipurpose Internet Mail Extension –** which allows the transmission and reception of mail that contains various types of data, such as speech, images and motion video. It is a newer standard than SMTP and uses much of its basic protocol.

Organisational Internets: Intranets and Extranets

An organisation may experience two disadvantages in having a connection to the WWW and the Internet:

- The possible use of the Internet for non-useful applications (by employees).
- The possible connection of non-friendly users from the global connection into the organisation's local network.

For these reasons, many organisations have shied away from connection to the global network and have set-up intranets and extranets.

An organisational Internet is the application of Internet technologies within a business network. It is used to connect employees to each other and to other organisations. There are two types of technologies used in organisational Internets:

- Intranets – a private network within an organization
- Extranets – a private network that connects more than one organization

Firewalls are often used to protect organisational Internets from external threats.

Intranets

Fast Forward: An intranet is built from the same concepts and technologies used for the Internet.

Intranets are in-house, tailor-made networks for use within the organisation and provide limited access (if any) to outside services and also limit the external traffic (if any) into the intranet. An intranet might have access to the Internet but there will be no access from the Internet to the organisation's intranet.

Organisations which have a requirement for sharing and distributing electronic information normally have three choices:

- Use a proprietary groupware package such as Lotus Notes
- Set up an Intranet
- Set up a connection to the Internet

STUDY TEXT

Groupware packages normally replicate data locally on a computer whereas Intranets centralise their information on central servers which are then accessed by a single browser package. The stored data is normally open and can be viewed by any compatible WWW browser. Intranet browsers have the great advantage over groupware packages in that they are available for a variety of clients, such as PCs, Macs, UNIX workstations and so on. A client browser also provides a single GUI interface, which offers easy integration with other applications such as electronic mail, images, audio, video, animation and so on.

The main elements of an Intranet are:

- Intranet server hardware
- Intranet server software
- TCP/IP stack software on the clients and servers
- WWW browsers
- A firewall

Other properties defining an Intranet are:

- Intranets use browsers, websites, and web pages to resemble the Internet within the business.
- They typically provide internal e-mail, mailing lists, newsgroups and FTP services
- These services are accessible only to those within the organization

Extranets

Extranets (external Intranets) allow two or more companies to share parts of their Intranets related to joint projects. For example, two companies may be working on a common project, an Extranet would allow them to share files related with the project.

- Extranets allow other organisations, such as suppliers, limited access to the organisation's network.
- The purpose of the extranet is to increase efficiency within the business and to reduce costs

Firewalls

- A firewall (or security gateway) is a security system designed to protect organisational networks. It protects a network against intrusion from outside sources. They may be categorised as those that block traffic or those that permit traffic.
- It consists of hardware and software that control access to a company's intranet, extranet and other internal networks.
- It includes a special computer called a proxy server, which acts as a gatekeeper.
- All communications between the company's internal networks and outside world must pass through this special computer.
- The proxy server decides whether to allow a particular message or file to pass through.

4. Information superhighway

Information superhighway is a name first used by US Vice President Al Gore for the vision of a global, high-speed communications network that will carry voice, data, video and other forms of

information all over the world, and that will make it possible for people to send e-mail, get up-to-the-minute news, and access business, government and educational information. The Internet is already providing many of these features, via telephone networks, cable TV services, online service providers and satellites.

It is commonly used as a synonym for National Information Infrastructure (NII). NII is a proposed, advanced, seamless web of public and private communications networks, interactive services, interoperable hardware and software, computers, databases, and consumer electronics to put vast amounts of information at user's fingertips.

5. Terminology

>>> Multiplexors/concentrators

Are the devices that use several communication channels at the same time. A multiplexor allows a physical circuit to carry more than one signal at one time when the circuit has more capacity (bandwidth) than individual signals required. It transmits and receives messages and controls the communication lines to allow multiple users access to the system. It can also link several low-speed lines to one high-speed line to enhance transmission capabilities.

>>> Front end communication processors

Are the hardware devices that connect all network communication lines to a central computer to relieve the central computer from performing network control, format conversion and message handling tasks. Other functions that a front-end communication processor performs are:

- Polling and addressing of remote units
- Dialling and answering stations on a switched network
- Determining which remote station a block is to be sent
- Character code translation
- Control character recognition and error checking
- Error recovery and diagnostics
- Activating and deactivating communication lines

>>> Cluster controllers

Are the communications terminal control units that control a number of devices such as terminals, printers and auxiliary storage devices. In such a configuration, devices share a common control unit, which manages input/output operations with a central computer. All messages are buffered by the terminal control unit and then transmitted to the receivers.

>>> Protocol converters

Are devices used to convert from one protocol to another such as between asynchronous and synchronous transmission. Asynchronous terminals are attached to host computers or host communication controllers using protocol converters. Asynchronous communication techniques do not allow easy identification of transmission errors; therefore, slow transmission speeds are used to minimises the potential for errors. It is desirable to communicate with the host computer using synchronous transmission if high transmission speeds or rapid response is needed.

>>> Multiplexing

Multiplexing is sending multiple signals or streams of information on a carrier at the same time in the form of a single, complex signal and then recovering the separate signals at the receiving end. Analog signals are commonly multiplexed using frequency-division multiplexing (FDM), in which the carrier bandwidth is divided into sub-channels of different frequency widths, each carrying a signal at the same time in parallel. Digital signals are commonly multiplexed using time-division multiplexing (TDM), in which the multiple signals are carried over the same channel in alternating time slots. In some optical fibre networks, multiple signals are carried together as separate wavelengths of light in a multiplexed signal using dense wavelength division multiplexing (DWDM).

>>> Circuit-switched

Circuit-switched is a type of network in which a physical path is obtained for and dedicated to a single connection between two end-points in the network for the duration of the connection. Ordinary voice phone service is circuit-switched. The telephone company reserves a specific physical path to the number you are calling for the duration of your call. During that time, no one else can use the physical lines involved.

Circuit-switched is often contrasted with packet-switched. Some packet-switched networks such as the X.25 network are able to have virtual circuit-switching. A virtual circuit-switched connection is a dedicated logical connection that allows sharing of the physical path among multiple virtual circuit connections.

>>> Packet-switched

Packet-switched describes the type of network in which relatively small units of data called packets are routed through a network based on the destination address contained within each packet. Breaking communication down into packets allows the same data path to be shared among many users in the network. This type of communication between sender and receiver is known as *connectionless* (rather than *dedicated*). Most traffic over the Internet uses packet switching and the Internet is basically a connectionless network.

>>> Virtual circuit

A virtual circuit is a circuit or path between points in a network that appears to be a discrete, physical path but is actually a managed pool of circuit resources from which specific circuits are allocated as needed to meet traffic requirements.

A permanent virtual circuit (PVC) is a virtual circuit that is permanently available to the user just as though it were a dedicated or leased line continuously reserved for that user. A switched virtual circuit (SVC) is a virtual circuit in which a connection session is set up for a user only for the duration of a connection. PVCs are an important feature of frame relay networks and SVCs are proposed for later inclusion.

>>> Closed Circuit Television (CCTV)

CCTV is a television system in which signals are not publicly distributed; cameras are connected to television monitors in a limited area such as a store, an office building, or on a college campus. CCTV is commonly used in surveillance systems.

>>> Very Small Aperture Terminal (VSAT)

VSAT is a satellite communications system that serves home and business users. A VSAT end user needs a box that interfaces between the user's computer and an outside antennae with a transceiver. The transceiver receives or sends a signal to a satellite transponder in the sky. The satellite sends and receives signals from an earth station computer that acts as a hub for the system. Each end user is interconnected with the hub station via the satellite in a star topology. For one end user to communicate with another, each transmission has to first go to the hub station, which retransmits it via the satellite to the other end user's VSAT. VSAT handles data, voice, and video signals.

VSAT offers a number of advantages over terrestrial alternatives. For private applications, companies can have total control of their own communication system without dependence on other companies. Business and home users also get higher speed reception than if using ordinary telephone service or ISDN.

SUMMARY

There are five kinds of communication channels used for cable or air connections:

- Telephone lines
- Coaxial cable
- Fibre-optic cable
- Microwave
- Satellite

Satellites are used to amplify and relay microwave signals from one transmitter on the ground to another. They orbit about 22,000 miles above the earth. They rotate at a precise point and speed and can be used to send large volumes of data.

There are five principal network topologies:

a) Star
b) Bus
c) Ring
d) Hierarchical (hybrid)
e) Completely connected (mesh)

Web portals are sites that offer a variety of services typically including e-mail, sports updates, financial data, news and links to selected websites.

A web page is a document file sent to your computer when the browser has connected to a website.

Web utilities are programmes that work with a browser to increase your speed, productivity and capabilities.

The four commonly used services on the Internet are:

- **Telnet** - Telnet allows you to connect to another computer (host) on the Internet .

- **FTP** - FTP allows you to copy files on the Internet.
- **Gopher** - Gopher allows you to search and retrieve information at a particular computer site called a gopher site.
- **The Web** - The web is a multimedia interface to resources available on the Internet. It connects computers and resources throughout the world.

There are three types of connections to the Internet through a provider:

- Direct or dedicated
- SLIP and PPP
- Terminal connection

The cable type used on a network depends on several parameters including:

- The data bit rate
- The reliability of the cable
- The maximum length between nodes
- The possibility of electrical hazards
- Power loss in cables
- Tolerance or harsh conditions
- Expense and general availability of the cache
- Ease of connection and maintenance
- Ease of running cables

The connectivity options that make communication available to end-users include:

- Fax machines (Facsimile transmission machines).
- E-mail (Electronic mail)
- Voice messaging systems
- Video conferencing systems
- Shared resources
- Online services

Past Paper Analysis:

6/00, 12/01, 6/02, 12/02, 6/03, 6/04, 12/04, 6/05, 12/05, 6/06, 6/07, 12/07

CHAPTER QUIZ

1. VSAT stands for.....
2. DWDM stands for.....
3. The main standards that relate to the protocols of email transmission and reception are .....and.....
4. ..... is a private network that connects more than one organisation.
5. The Internet uses an addressing method known as the.....

SOLUTIONS TO CHAPTER QUIZ

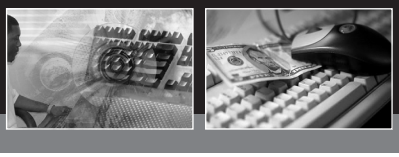
1. Very Small Aperture Terminal
2. Dense Wavelength Division Multiplexing
3. Simple Mail Transfer Protocol (SMTP) and Multipurpose Internet Mail Extension
4. Extranet
5. Domain Name System (DNS).

QUESTIONS

1. a) Identify and describe the main criteria which should be met by a local area network design.
   b) What reasons would you put forward for adopting a database as a basis for an information system?
2. You recently attended a seminar organised by the Institute of Certified Public Accountants of Kenya (ICPAK) on information management into the 21st century. One of the topics covered was on Internet and its impact on the society. Explain to the senior management the effect of Internet on the following sectors of society.
   i) Education.
   ii) Service provision industry.
3. Examine the role of a database administrator in an organisation.
4. Give four examples of industries and business organisations that are currently using computer networking. What are the implications of increased electronic networking on computer security?
   Giving reasons, identify four situations where communication over wireless medium for instance radio and mobile phones may be preferable to guided communication (over cable).

CHAPTER EIGHT

EMERGING ISSUES IN MANAGEMENT INFORMATION SYSTEMS AND E-COMMERCE



CHAPTER EIGHT

EMERGING ISSUES IN MANAGEMENT INFORMATION SYSTEMS AND E-COMMERCE

▶ OBJECTIVES

When you have completed this chapter, you should be able to:

1. Define electronic commerce and relate it to the business world.
2. Describe the different outsourcing practices in organisations.
3. Outline software houses.
4. Appreciate the various computer frauds and their threats.
5. Identify the applications of data mining.

▶ INTRODUCTION

Information technology is a field that changes day-in-day out. Invention of complex technology is facilitated by sophisticated systems required by different firms. This is also enhanced by competition of organisations for clients' satisfaction.

▶ DEFINITION OF KEY TERMS

Electronic Data Interchange (EDI) - is an electronic means for transmitting business transactions between organisations.

Outsourcing is a contractual agreement whereby an organization hands over control of part or all of the functions of the information systems department to an external party.

Software house is a company that creates custom software for specific clients

Hacking - Gaining unauthorised access to computer programmes and data.

▶ EXAM CONTEXT

Most of the questions from this chapter are application questions with regard to inventions currently in use in the various industries. The student will be required to be updated on various technologies in various industries as outlined in magazines, journals, dailies, etc.

▶ INDUSTRY CONTEXT

Electronic commerce that is conducted between businesses is referred to as business-to-business or B2B. B2B can be open to all interested parties (e.g. commodity exchange) or limited to specific, pre-qualified participants (private electronic market). Electronic commerce that is conducted between businesses and consumers, on the other hand, is referred to as business-to-consumer or B2C. This is the type of electronic commerce conducted by companies such as Amazon.com.

Fast Forward: Electronic commerce that is conducted between businesses is referred to as business-to-business or B2B.

1. Electronic commerce

Electronic commerce (e-commerce) is the buying and selling of goods and services over the Internet. Businesses on the Internet that offer goods and services are referred to as web storefronts. Electronic payment to a web storefront can include check, credit card or electronic cash.

1.1 Web storefronts

These are also known as virtual stores. This is where shoppers can go to inspect merchandise and make purchases on the Internet. Web storefront creation package is a new type of programme to help businesses create virtual stores. Web storefront creation packages (also known as commerce servers) do the following:

- Allow visitors to register, browse, place products into virtual shopping carts and purchase goods and services.
- Calculate taxes and shipping costs and handle payment options.
- Update and replenish inventory.
- Ensure reliable and safe communications.
- Collects data on visitors.
- Generates reports to evaluate the site's profitability.

1.2 Web auctions

Web auctions are a recent trend in e-commerce. They are similar to traditional auctions but buyers and sellers do not meet face-to-face. Sellers post descriptions of products at a web site and buyers submit bids electronically. There are two basic types of web auction sites:

- Auction house sites
- Person-to-person sites

Auction house sites

Auction house owners present merchandise typically from companies' surplus stocks. Auction house sites operate in a similar way to a traditional auction. Bargain prices are not uncommon on this type of site and are generally considered safe places to shop.

Person-to-person sites

The owner of site provides a forum for buyers and sellers to gather. The owner of the site typically facilitates rather than being involved in transactions. Buyers and sellers on this type of site must be cautious.

1.3 Electronic payment

The greatest challenge for e-commerce is how to pay for the purchases. Payment methods must be fast, secure and reliable. Three basic payment methods now in use are:

(i) Cheques
- After an item is purchased on the Internet, a cheque for payment is sent in the mail.
- It requires the longest time to complete a purchase.
- It is the most traditional and safest method of payment.

(ii) Credit card
- Credit card number can be sent over the Internet at the time of purchase.
- It is a faster and a more convenient method of paying for Internet purchases.
- However, credit card fraud is a major concern for buyers and sellers.
- Criminals known as carders specialise in stealing, trading and using stolen credit. cards stolen from the Internet.

(iii) Electronic cash
- Electronic cash is also known as e-cash, cyber cash or digital cash.
- It is the Internet's equivalent of traditional cash.
- Buyers purchase e-cash from a third party such as a bank that specialises in electronic currency.
- Sellers convert e-cash to traditional currency through a third party.
- It is more secure than using a credit card for purchases.

STUDY TEXT

2. Electronic Data Interchange (EDI)

EDI is an electronic means for transmitting business transactions between organisations. The transmissions use standard formats such as specific record types and field definitions. EDI has been in use for 20 years, but has received significant attention within recent years as organisations seek ways to reduce costs and be more responsive.

The EDI process is a hybrid process of systems software and application systems. EDI system software can provide utility services used by all application systems. These services include transmission, translation and storage of transactions initialised by or destined for application processing. EDI is an application system in that the functions it performs are based on business needs and activities. The applications, transactions and trading partners supported will change over time and the co-mingling of transactions, purchase orders, shipping notices, invoices and payments in the EDI process makes it necessary to include application processing procedures and controls in the EDI process.

EDI promotes a more efficient paperless environment. EDI transmissions may replace the use of standard documents including invoices or purchase orders. Since EDI replaces the traditional paper document exchange such as purchase orders, invoices or material release schedules, the proper controls and edits need to be built within each company's application system to allow this communication to take place.

3. Outsourcing practices

Outsourcing is a contractual agreement whereby an organisation hands over control of part or all of the functions of the information systems department to an external party. The organisation pays a fee and the contractor delivers a level of service that is defined in a contractually binding service level agreement. The contractor provides the resources and expertise required to perform the agreed service. Outsourcing is becoming increasingly important in many organisations.

The specific objective for IT outsourcing vary from organisation to organisation. Typically, though, the goal is to achieve lasting, meaningful improvement in information system through corporate restructuring to take advantage of a vendor's competencies.

Reasons for embarking on outsourcing include:

- A desire to focus on a business' core activities.
- Pressure on profit margins.
- Increasing competition that demands cost savings.
- Flexibility with respect to both organisation and structure.

The services provided by a third party can include:

- Data entry (mainly airlines follow this route).
- Design and development of new systems when the in-house staff do not have the requisite skills or is otherwise occupied in higher priority tasks.

- Maintenance of existing applications to free in-house staff to develop new applications.
- Conversion of legacy applications to new platforms. For example, a specialist company may enable an old application.
- Operating the help desk or the call centre.

Possible disadvantages of outsourcing include:

- Costs exceeding customer expectations.
- Loss of internal information system experience.
- Loss of control over information system.
- Vendor failure.
- Limited product access.
- Difficulty in reversing or changing outsourced arrangements.

Business risks associated with outsourcing are hidden costs, contract terms not being met, service costs not being competitive over the period of the entire contract, obsolescence of vendor IT systems and the balance of power residing with the vendor. Some of the ways that these risks can be reduced are:

- By establishing measurable partnership enacted shared goals and rewards.
- Utilisation of multiple suppliers or withhold a piece of business as an incentive.
- Formalisation of a cross-functional contract management team.
- Contract performance metrics.
- Periodic competitive reviews and benchmarking/bench-trending.
- Implementation of short-term contracts.

Outsourcing is the term used to encompass three quite different levels of external provision of information systems services. These levels relate to the extent to which the management of IS, rather than the technology component of it, have been transferred to an external body. These are time-share vendors, service bureaus and facilities management.

3.1 Time-share vendors

These provide online access to an external processing capability that is usually charged for on a time-used basis. Such arrangements may merely provide for the host processing capability onto which the purchaser must load software. Alternatively the client may be purchasing access to the application. The storage space required may be shared or private. This style of provision of the 'pure' technology gives a degree of flexibility allowing *ad hoc*, but processor intensive jobs to be economically feasible.

3.2 Service bureaus

These provide an entirely external service that is charged by time or by the application task. Rather than merely accessing some processing capability, as with time-share arrangements, a complete task is contracted out. What is contracted for is usually only a discrete, finite and often small, element of overall IS.

The specialist and focused nature of this type of service allows the bureaux to be cost-effective at the tasks it does since the mass coverage allows up-to-date efficiency-oriented facilities ideal for routine processing work. The specific nature of tasks done by service bureaus tend to make them slow to respond to change and so this style of contracting out is a poor choice where fast changing data is involved.

3.3 Facilities Management (FM)

This may be the semi-external management of IS provision. In the physical sense all the IS elements may remain (or be created from scratch) within the client's premises but their management and operation become the responsibility of the contracted body. FM contracts provide for management expertise as well as technical skills. FM deals are legally binding equivalent of an internal service level agreement. Both specify what service will be received but significantly differ in that, unlike when internal IS fails to deliver, with an FM contract legal redress is possible. For most organisations it is this certainty of delivery that makes FM attractive.

FM deals are increasingly appropriate for stable IS activities in those areas that have long been automated so that accurate internal versus external cost comparisons can be made. FM can also be appealing for those areas of high technology uncertainty since it offers a form of risk transfer. The service provider must accommodate unforeseen changes or difficulties in maintaining service levels.

4. Software houses

A software house is a company that creates custom software for specific clients. They concentrate on the provision of software services. These services include feasibility studies, systems analysis and design, development of operating systems software, provision of application programming packages, 'tailor-made' application programming, specialist system advice, etc. A software house may offer a wide range of services or may specialise in a particular area.

5. Information resource centres

Information Resource Centres co-ordinate all information activities within their areas of interest and expertise. Information within that area is analysed, abstracted and indexed for effective storage, retrieval and dissemination.

6. Data warehousing

A data warehouse is a subject-oriented, integrated, time-variant, non-volatile collection of data in

support of management's decision-making process.

Data warehouses organise around subjects, as opposed to traditional application systems which organise around processes. Subjects in a warehouse include items such as customers, employees, financial management and products. The data within the warehouse is integrated in that the final product is a fusion of various other systems' information into a cohesive set of information. Data in the warehouse is accurate to some date and time (time-variant). An indication of time is generally included in each row of the database to give the warehouse time variant characteristics. The warehouse data is non-volatile in that the data, which enters the database is rarely, if ever, changed. Change is restricted to situations where accuracy problems are identified. Information is simply appended to or removed from the database, but never updated. A query made by a decision support analyst last week renders exact results one week from now.

The business value of data warehousing includes:

- More cost effective decision-making – the reallocation of staff and computing resources required to support *ad hoc* inquiry and reporting.
- Better enterprise intelligence – increased quality and flexibility of analysis based on multi-tiered data structures ranging from detailed transactions to high level summary information.
- Enhanced customer service – information can be correlated via the warehouse, thus resulting in a view of the complete customer profile.
- Enhanced asset/liability management – purchasing agents and financial managers often discover cost savings in redundant inventory, as well as previously unknown volume discount opportunities.
- Business processing reengineering – provides enterprise users access to information yielding insights into business processes. This information can provide an impetus for fact-based reengineering opportunities.
- Alignment with enterprise right-sizing objectives – as the enterprise becomes flatter, greater emphasis and reliance on distributed decision support will increase.

STUDY TEXT

7. Data Mining

Fast Forward: As more data is gathered, with the amount of data doubling every three years, data mining is becoming an increasingly important tool to transform this data into information

This is the process of discovering meaningful new correlations, patterns, and trends by digging into (mining) large amounts of data stored in warehouses, using artificial intelligence and statistical and mathematical techniques.

Industries that are already taking advantage of data mining include retail, financial, medical, manufacturing, environmental, utilities, security, transportation, chemical, insurance and aerospace industries. Most organisations engage in data mining to:

- Discover knowledge – the goal of knowledge discovery is to determine explicit hidden relationships, patterns, or correlations from data stored in an enterprise's database. Specifically, data mining can be used to perform:

    - Segmentation – e.g. group customer records for custom-tailored marketing
    - Classification – assignment of input data to a predefined class, discovery and understanding of trends, text-document classification.
    - Association – discovery of cross-sales opportunities
    - Preferencing – determining preference of customer's majority
- Visualise data – make sense out of huge data volumes e.g. use of graphics
- Correct data – identify and correct errors in huge amounts of data

Applications of data mining include:

- Mass personalisation – personalised services to large numbers of customers
- Fraud detection – using predictive models, an organisation can detect existing fraudulent behaviour and identify customers who are likely to commit fraud in the future.
- Automated buying decisions – data mining systems can uncover consumer buying patterns and make stocking decisions for inventory control.
- Credit portfolio risk evaluation – a data mining system can help perform credit risk analysis by building predictive models of various portfolios, identifying factors and formulating rules affecting bad risk decisions.
- Financial planning and forecasting – data mining provides a variety of promising techniques to build predictive models forecasting financial outcome on a macroeconomic style.
- Discovery sales – for companies that excel in data mining, an innovative source of revenue is the sale of some of their data mining discoveries.

8. Information technology and the law

This is an area that has received little attention in developing countries. However, in developed countries substantial efforts have been made to ensure that computers are not used to perpetrate criminal activities. A number of legislation have been passed in this direction in these countries. In Kenya, the law is yet to reflect clearly how computer crime is to be dealt with.

The Internet does not create new crimes but causes problems of enforcement and jurisdiction. The following discussion shows how countries like England deal with computer crime through legislation and may offer a point of reference for other countries.

8.1 Computers and crime

Computers are associated with crime in two ways:

1. Facilitate the commission of traditional crimes. This does not usually raise new legal issues.

2. They make possible new forms of "criminal" behaviour, which have raised new legal issues.

Computer crime is usually in the form of software piracy, electronic break-ins and computer sabotage be it industrial, personal, political, etc.

Fraud and theft

Computer fraud is any fraudulent behaviour connected with computerization by which someone intends to gain financial advantage. Types of computer fraud includes:

(i) Input fraud – entry of unauthorised instructions, alteration of data prior to entry or entry of false data. Requires few technical skills.
(ii) Data fraud – alteration of data already entered on computer, requires few technical skills.
(iii) Output fraud – fraudulent use of or suppression of output data. Less common than input or data fraud but evidence is difficult to obtain.
(iv) Programme fraud – creating or altering a programme for fraudulent purposes. This is the real computer fraud and requires technical expertise and is apparently rare.

The legal response prior to 1990 was as follows:

- Direct benefit – use of a computer to directly transfer money or property. This is traditional theft. This criminal behaviour is tried under traditional criminal law e.g. governed by Theft Act 1968 in England, common law in Scotland.
- Indirect benefit – obtaining by deception. E.g. Theft Act of 1968 and 1978 deals with dishonestly obtaining property or services by deception.
- Forgery – the Forgery and Counterfeiting Act 1981 defines it as making a false instrument intending to pass it off as genuine.
- Theft of information – unauthorised taking of "pure" information is not legally theft in England and Scotland because information is not regarded as property and offence of theft requires that someone is deprived of his property.

Damage to software and data

It is possible to corrupt/erase data without apparently causing any physical damage. In England, the Criminal Damage Act of 1971 states that a person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage such property, shall be guilty of an offence.

Hacking

Gaining unauthorised access to computer programs and data. This was not criminal in England prior to the Computer Misuse Act of 1990.

Computer Misuse Act 1990

It is not a comprehensive statute for computer crime and does not generally replace the existing criminal law. It, however, creates three new offences.

- **The Unauthorised Access Offence**
  A person is guilty of an offence if he causes a computer to perform any function with

intent to secure access to any programme or data held in any computer and the access he intends to secure is unauthorised, and he knows at the time when he causes the computer to perform the function that this is the case. Maximum penalty is six months imprisonment and/or maximum £5,000 fine.

- **The Ulterior Intent Offence**
  A person is guilty of this offence if he commits the Unauthorised Access Offence with intent to commit an offence or to facilitate the commission of such an offence (whether by himself or another person). Maximum penalty for Ulterior Intent Offence is five years imprisonment and/or unlimited fine.

- **The Unauthorised Modification Offence**
  A person is guilty of this offence if he does any act which causes an unauthorized modification of the contents of any computer and at the time he does the act he has the requisite intent (intent to impair operation or hinder access) and the requisite knowledge (knowledge that actions are unauthorised).

Computers and pornography

Pornography is perceived as one of the major problems of computer and Internet use. Use of computers and the Internet have facilitated distribution of and access to illegal pornography, but have not created many new legal issues. Specific problems and how they are addressed include:

- Pseudo-photographs – these are combined and edited images to make a single image. The Criminal Justice Act 1988 and Protection of Children Act 1978 (if the image appears to be an indecent image of a child) was amended to extend certain indecency offences to pseudo-photographs.
- Multimedia pornography – Video Recordings Act 1984: supply of video recordings without classification certificate is an offence.

Cyberstalking

Using a public telecommunication system to harass another person may be an offence under the Telecommunications Act 1984. Pursuing a course of harassing conduct is an offence under the Protection from Harassment Act 1997.

8.2 Intellectual property rights

These are legal rights associated with creative effort or commercial reputation or goodwill.

Categories of Intellectual property rights

Rights differ according to subject matter being protected, scope of protection and manner of creation. Broadly include:

- Patents – a patent is the monopoly to exploit an invention for up to 20 years (in UK). Computer programme as such are excluded from patenting – but may be patented if applied in some technical or practical manner. The process of making semiconductor chips falls into the patent regime.

- Copyrights – a copyright is the right to make copies of a work. Subject matter protected by copyrights include:
    - Original literary, dramatic, musical and artistic works.
    - Sound recordings, films, broadcasts and cable programme.
    - Typographical arrangement of published editions.

Computer programmes are protected as literary works. Literal copying is the copying of programme code while non-literal copying is judged on objective similarity and "look and feel". Copyright protects most material on the Internet e.g. linking (problem caused by deep links), framing (displaying a website within another site), caching and service provider liability.

- Registered designs
- Trademarks – A trademark is a sign that distinguishes goods and services from each other. Registration gives partial monopoly over right to use a certain mark. Most legal issues of trademarks and information technology have arisen from the Internet such as:
    - Meta tags – use of a trademarked name in a meta tag by someone not entitled to use it may be infringement.
    - Search engines – sale of "keywords" that are also trademarked names to advertisers may constitute infringement.
    - Domain names – involves hijacking and "cyber-squatting" of trademarked domain names.
- Design rights
- Passing off
- Law of confidence
- Rights in performances

Conflicts of Intellectual Property

>> Plagiarism

Increased plagiarism because of the Internet violates academic dishonesty because copying does not increase writing and synthesis of skills. Ideally, one must give credit to the original author.

>> Piracy

In 1994 a student of U.S.A's Massachusetts Institute of Technology (MIT) was indicted for placing commercial software on website for copying purposes. The student was accused of wire fraud and the interstate transportation of stolen property. The case was thrown out on technicality grounds since the student did not benefit from the arrangement and did not download the software himself. His offence also did not come under any existing law.

Software publishers estimate that more than 50% of the software in US is pirated and 90% in some foreign countries. In US, software companies can copyright it and thus control its distribution. It is illegal to make copies without authorisation.

Fast Forward: Copyright infringement (or copyright violation) is the unauthorised use of material that is covered under copyright law.

Repackaging data and databases

A company produced a CD-ROM containing a large compilation of phone numbers. A university student put this CD-ROM on his website. Company sued saying the student had violated the shrink-wrap license agreement that came with the CD-ROM. Did the student infringe pro-CD's claimed copyright in the telephone listings? The court said no. Copying of the data was clearly prohibited by the License Agreement but the court failed to invoke it. Instead, the court stated that the terms of the select phone license agreement were not presented to the student or any other purchaser at the time of sale. The appeal against this case was still pending in The U.S. court by the time of publishing this document.

Governments have been asking for more laws to copyright databases.

Reverse Engineering

Interfaces are often incomplete, obscure and inaccurate, so developers must look at what the code really does. Reverse engineering is often a necessity for reliable software design. Companies doing reverse engineering must not create competing products. Courts have, however, allowed reverse engineering under certain restrictions.

Copying in transmission

"Store and forward networks", a network node gets data in transmission, stores it and forwards to the next node until it reaches its destination. Everybody gets a copy, who archives them? Are the intermediate copies a violation of copyright? If users email pictures or documents, which contain trademarks or copyrighted materials, do email copies on servers put the server's company in jeopardy?

8.3 Liability for information technology

Liability may arise out of sale/supply of defective software or liability for online information.

Liability for defective software may arise out of contractual or non-contractual terms. A contract is a voluntary legally binding agreement between two or more parties. Parties may agree as they may wish subject to legislation such as the Sale of Goods Act. The legislation limits contractual freedom and imposes terms and conditions in certain kind of contracts. The question that usually arises is whether software is 'goods' or 'services'. However, mass produced software packages are generally goods, but custom written or modified software is a service. Non-contractual liability is based on negligence. The law of negligence is based on the principle that a person should be liable for his careless actions where this causes loss or damage to another. To bring a successful action for negligence, the pursuer needs to prove that the defender owed him a duty of care.

Liability for online information involves defective information and defamation. Where a person acts on information given over the Internet and suffers a loss because information was inaccurate, will anyone be liable. Two problems that arise are; one, a person who puts information on the Internet will only be liable if he owes a duty of care to the person who suffers the loss. Two, damage caused in this way will normally be pure economic loss, which cannot usually be claimed for in delict (tort). However, there is a limited exception to this general principle in respect of negligent misstatement. This is where according to Hedley Byrne & Co v Heller & Partners (1964):

- The person giving the advice/information represented himself as an expert.
- The person giving the advice/information knew (or should have known) that the recipient was likely to act on it, and
- The person giving the advice/information knew (or should have known) that the recipient of information was likely to suffer a loss if the information was given without sufficient care.

Can an Internet Service Provider be liable for defective information placed by someone else? ISP may be regarded as a publisher. Traditional print publishers have been held not to be liable for inaccurate information contained in the books they publish. But ISP may be liable if it is shown that they had been warned that the information was inaccurate and did nothing to remove it.

Defamatory statements may be published on the WWW, in newsgroups and by email. Author of the statements will be liable for defamation, but may be difficult to trace or not worth suing. But employers and Internet service providers may be liable. Defamation is a delict (tort) and employers are vicariously liable for delicts committed by their employees in the course of their employment. Many employers try to avoid the possibility of actionable statements being published by their staff by monitoring email and other messages. Print publishers are liable for defamatory statements published by them, whether they were aware of them or not. ISPs could be liable in the same way.

9. Terminology

>>> Data Mart

A data mart is a repository of data gathered from operational data and other sources that is designed to serve a particular community of knowledge workers. In scope, the data may derive from an enterprise-wide database or data warehouse or be more specialised. The emphasis of a data mart is on meeting the specific demands of a particular group of knowledge users in terms of analysis, content, presentation, and ease-of-use. Users of a data mart can expect to have data presented in terms that are familiar.

In practice, the terms *data mart* and *data warehouse* each tend to imply the presence of the other in some form. However, most writers using the term seem to agree that the design of a data mart tends to start from an analysis of user needs and that a data warehouse tends to start from an analysis of what data already exists and how it can be collected in such a way that the data can later be used.

A data warehouse is a central aggregation of data (which can be distributed physically); a data mart is a data repository that may derive from a data warehouse or not and that emphasises ease of access and usability for a particular designed purpose. In general, a data warehouse tends to be a strategic but somewhat unfinished concept; a data mart tends to be tactical and aimed at meeting an immediate need. In practice, many products and companies offering data warehouse services also tend to offer data mart capabilities or services.

SUMMARY

Reasons for embarking on outsourcing include:

- A desire to focus on a business' core activities
- Pressure on profit margins
- Increasing competition that demands cost savings
- Flexibility with respect to both organisation and structure

Some of the ways that outsourcing risks can be reduced are:

- By establishing measurable partnership enacted shared goals and rewards
- Utilisation of multiple suppliers or withhold a piece of business as an incentive
- Formalisation of a cross-functional contract management team
- Contract performance metrics
- Periodic competitive reviews and benchmarking/benchtrending
- Implementation of short-term contracts

Applications of data mining include:

- Mass personalisation – personalised services to large numbers of customers
- Fraud detection
- Automated buying decisions
- Credit portfolio risk evaluation
- Financial planning and forecasting
- Discovery sales – for companies that excel in data mining, an innovative source of revenue is the sale of some of their data mining discoveries.

Kinds of computer fraud include:

(i) Input fraud – entry of unauthorised instructions, alteration of data prior to entry or entry of false data. Requires few technical skills.
(ii) Data fraud – alteration of data already entered on computer, requires few technical skills.
(iii) Output fraud – fraudulent use of or suppression of output data. Less common than input or data fraud but evidence is difficult to obtain.
(iv) Programme fraud – creating or altering a programme for fraudulent purposes. This is the real computer fraud and requires technical expertise and is apparently rare.

Categories of Intellectual property rights

- Patents – a patent is the monopoly to exploit an invention for up to 20 years (in UK). Computer programmes as such are excluded from patenting – but may be patented if applied in some technical or practical manner.
- Copyrights – a copyright is the right to make copies of a work.

Past Paper Analysis:

12/00, 6/01, 12/01, 6/02, 12/02, 6/03, 12/03, 6/04, 6/05, 12/05, 12/07

CHAPTER QUIZ

1. A ..... is a sign that distinguishes goods and services from each other.

2. ..... is making a false instrument intending to pass it off as genuine.

3. A copyright is the monopoly to exploit an invention for up to 20 years
   a. True
   b. False

4. ..... refers to gaining unauthorised access to computer programmes and data.

5. ..... is a company that creates custom software for specific clients.

SOLUTIONS TO CHAPTER QUIZ

1. Trademark
2. Forgery
3. b. False that is a Patent
4. Hacking
5. Software house

QUESTIONS

1. Write short descriptive notes on the following:
   a) Electronic Data Interchange
   b) Client/server computing
   c) System specification
   d) Electronic point of sale system

2. Explain the contribution that an information resource centre might make towards end-user computing.

3. (a) What factors should guide a systems designer when designing the user interface for a particular application?
   (b) Currently, there has been a general trend to consolidate previously separate data centres into larger centres or the move from classic decentralisation as a proliferation of mini-data processing departments into centralised information system providers.
   Explain the factors influencing re-centralisation of information systems

4. Explain the meaning of the following terms:
   (i) Down-sizing. (2 marks)
   (ii) Cyber-cafe.

5. It is envisaged that the World Wide Web (WWW) will enable institutions to take services closer to the people.

Required:
   (i) As a close advisor of ABC Tutorial College you are required to explain how WWW can make this a reality.
   (ii) Suggest any two managerial issues that are critical for its successful implementation

ANSWERS

TO CHAPTER QUESTIONS

ANSWERS TO CHAPTER QUESTIONS

CONTENTS

Chapter 1

1. A typical DBMS package would feature
   - The ability to create, amend and delete records, ie basic file maintenance and record control
   - The access of individual records or the contents of a whole file
   - Protection against unauthorised access and corruption, recovery and restart
2. **Problems which may be experienced:**
   - Difficulty in developing, installing and maintaining large monolithic systems.
   - Performance which was below the expected standard.
   - High overhead costs and low intensity of use.

   Advantages which are sometimes claimed:
   - The data reflects the corporate view allowing expert system and DSS use.
   - Better data integrity and reduced data redundancy.
   - Faster development of applications once the database has been set up.
   - Data interdependence allows changes in technology and changes in application to be insulated from each other.
3. **There are four main types of file organisation:**
   a. Serial – a new record is written to the end of the existing file. Each record must be read in turn to access a particular data item. It is suitable for transaction files e.g. customer orders taken during the day, or a workfile or spoolfile.
   b. Sequential – records are stored in ascending or descending order of key, e.g. account number. A customer masterfile may be in this form.
   c. Indexed sequential – these are accessed through a smaller secondary file called index. Overflow must be catered for. IS files may be on disk or tape, and may be used for almost any type of file in a batch processing environment.
   d. Random – most often used with on-line systems where records need to be accessed directly, as in airline booking system.
4. **The following are some of the areas that computers are used:**

   (a) Retailing – computers are used in point of sale systems and credit card payment systems as well as stock inventories.
   (b) Home appliances – computers (especially embedded computers or microprocessors) are included in household items for reasons of economy and efficiency of such items. Major appliances such as microwave ovens, clothes washers, refrigerators and sewing machines are making regular use of microprocessors.
   (c) Reservation systems – guest booking, accommodation and bills accounting using computers in hotels have made the process to be more efficient and faster.

Airline computer reservation systems have also enhanced and streamlined air travel across major airlines. Major players in the industry have also adopted online reservation systems.

(d) Health care and medicine – computers have played an important role in the growth and improvement of health care that the use of computers in medicine has become a medical specialty in itself. Computers are used in such areas as maintenance of patient records, medical insurance systems, medical diagnosis, and patient monitoring.

5. Classification by power and size/configuration

a) Supercomputers - the largest and most powerful. Used to process large amounts of data very quickly. Useful for meteorological or astronomical applications. Examples include Cray and Fujitsu.
b) Mainframe computers - Large computers in terms of price, power and size. Require a carefully controlled environment and specialist staff to operate them. Used for centralised processing for large commercial organisations. Manufacturers include International Business Machine (IBM).
c) Minicomputers - Their size, speed and capabilities lie somewhere between mainframes and microcomputers. Used as departmental computers in large organisations or as the main computer in medium-sized organisations. Manufacturers of minicomputers include IBM and International Computer Limited (ICL).
d) Microcomputers - These are the personal computers commonly used for office and leisure activities. Examples include Hewlett Packard (HP), Compaq and Dell. They include desktops, laptops and palmtops.

Chapter 2

1. The question addresses the organisation at micro level, proposing five layers:

(a) Corporate (relating to strategic management decisions), e.g. corporate plans, budgets, etc.
(b) Unit level or division, differentiated by product, geography or management structure.
(c) Functional (relating to middle management) including organisational sub-systems e.g. financial planning, manpower planning, etc.
(d) Departmental, at the level of tactical activities, e.g. quality management.
(e) Operational, the day-to-day activities, e.g. adding to and withdrawing from stock.

2. The four factors affecting integration are:

(a) The quality of the data captured; the need for verification and validation; data redundancy and data reduction; problems of noise.
(b) Transmission/reception quality; effect of data capture; coding methods and standards; use of technology.
(c) Channel quality, transmission media, interface, distortion and noise.
(d) Feedback loops, message checking and repetition, batch totals and check digits; data redundancy and possible increase in noise and distortion.

3. The question could be answered by naming and describing six elements met in the analysis and design of information systems.

(a) Inputs
- Information quality and content.
- Interfaces with other systems.
- The need to capture or produce data.

(b) Processes
- Conversion of input to output;
- System protocols and interaction;
- Standards and quality.

(c) Outputs:
- Users' information requirements;
- Media choices;
- Messages sent to other sub-systems.

(d) Environment:
- Other sub-systems;
- Monitoring output

(e) Channels:
- Choice of channel/media;
- Overcoming interference, noise and distortion.

(f) Feedback:
- Use of system control loop(s);
- Predicting situations where control is required.

4. Importance of systems theory:

(a) It provides a theoretical framework for study of performance of businesses

(b). It stresses the fact that all organisations are made up of subsystems, which must work together harmoniously in order that goals of the overall system can be achieved.

(c). It recognises the fact that conflicts can arise within a system, and that such conflicts can lead to sub-optimisation and that, ultimately, can even mean that an organisation does not achieve its goals.

(d). It allows the individual to recognise that he/she is a subsystem within a larger system, and that the considerations of systems concept apply to him/her, also.

(e). Given the above factors, it is clear that information-producing systems must be designed to support the goals of the total system, and that this must be borne in mind throughout their development.

5. Lawrence and Lorsch theory

The two studied the operations of a number of firms to assess the effects on the tasks and attitudes of managers in various functions operating with different structures and environment. Some of the major contributors to this approach are:

a. The more volatile and diverse the environment, the more task differentiation, and consequent integration, is required to achieve successful organisation.

b. More stable environment does not require much differentiation but still requires substantial integration within the functions that exist.

c. It is more difficult to resolve conflict in organisations with a high degree of differentiation between the functions that exist.

d. Better methods of conflict resolution result in higher performance and lead to types of

differentiation and integration that suit the organisations environment.

e. In a predictable environment integration is achieved through the management hierarchy, particular at higher levels and through rules, procedures, budgets, etc. In an uncertain environment, integration is achieved at lower levels mainly through personal interrelationship with only a moderate use of administrative methods.

In spite of some criticism, the Lawrence and Lorsch study received, it played an important role in development of organisations theory, which took account of change, uncertainty and the interaction of key variables.

Chapter 3

1.Types of benefit may include:

(a) Direct benefits such as reduced costs, or increased turnover or output.
(b) Indirect benefits such as better decision-making, control, or freedom to innovate or grow.

The former affect cash flow immediately, the latter affect profitability gradually. Costs fall into three areas:

(a) Development including users' and analysts' time, hardware specification and tendering.
(b) Implementation including acquisition and recruitment.
(c) Running including maintenance and salaries.

2. Commonly applied evaluation techniques include:

(a) Breakeven analysis which recognises fixed or period costs and variable (marginal) or unit costs. Break-even point may be derived graphically or by formula.
(b) Payback which attempts to measure the time taken to recoup the initial investment in the system. The method favours safe, short – term projects and stresses liquidity at the expense of profitability.
(c) Net present value uses discounted cash flow techniques. Internal rate of return also exploits the techniques.

3. The question addresses the issues of efficiency and effectiveness in the planning and control of projects.

(a) Efficient utilisation of:
- Time – a key parameter. There will be an overall project deadline and, within this, milestones at which specified deliverables will be required. Failure to achieve completion by these dates will incur resource costs.
- Resources – may be material or human. Material resources (hardware and software) entail acquisition and production decisions and facilities.
- Costs – will be influenced by factors 1 and 2. Cost management will entail forecasting and estimating, monitoring and rescheduling project activities to meet budgetary constraints.

(b) Types of judgements and decisions:
- Time management – may involve decisions on simplifying project tasks, acquiring

extra resources (e.g. extra staff or overtime) and reducing non-productive activities.
- Quality management – often a decision trade-off between cost, time and the effectiveness of the completed system or software.
- Resource management – often decisions involve trying to optimise the use of resources with constraints of cost and time.
- Cost management – central to decisions on time, cost, quality and resources.

4. The question asks for details on four components:

(a) Team leaders – a leader of an information systems project team will be responsible for planning and organising, co-ordinating and supervising, advising the team, reporting to sponsors and implementing changes to project schedules.
(b) User group – the project user group will consist of a cross-section of stakeholders in the project. The component is a vehicle for expressing concerns, resolving queries and discussing solutions. The user group is non-executive, matters for action being communicated to the steering committee.
(c) Steering committee – this body may be temporary or permanent and will include users and project staff. The committee's role is central in securing senior management involvement, monitoring the effectiveness of planning and resource allocation, and approving changes in the project.
(d) Project manager – the person in overall charge of the project will operate at all levels of management and will attempt to achieve maximum efficiency and effectiveness by directing the team leaders in line with the wishes of the steering committee. The project manager integrates all aspects of the project.

5. CPA is a sequential approach to project planning and control. The major stages are:

(a) Programming – the project must be broken down into tasks, which may be decomposed into greater detail. The tasks are sequenced by establishing the interdependences and may then be composed into a CPA diagram. An estimate of the duration of each task is made, which may be arrived at by a single estimate or by aggregation as in PERT. The project schedule is then drawn up, e.g. earliest start, latest finish dates, and the project free time or float is calculated.
(b) Evaluation – the overall project duration will now be known, as will the critical path. The project plan may now be examined for possible improvements involving decisions on resource levels and the placement of activities in some other sequence.
(c) Review – the plan must be kept relevant by constant monitoring and updating. Actual completion dates will be fed into the plan and milestone reports and meetings will be conducted. The plan will be amended in line with actual performance.

Chapter 4

1. The question may be answered by considering the role of an individual who would work in the following way:

(a) Through a committee structure to co-ordinate activity throughout the relevant part(s) of the organisation.
(b) To develop information resources.
(c) To acquire new information resources.

(d). To control the technology migration, i.e. the change from one technology or information use to another.
An example of the role might be to investigate and advise on the introduction of a stand-alone microcomputer system to replace a previously centralised one.

2. The concept of an information centre may be explained by referring to the following issues:

(a) An information centre is a point of interface between the information system and its users.
(b) The job of an information centre is to use data transformation to make information available in its most useful form.
(c) Although an information centre may own the hardware and software, it does not own the data/information.
(d) The information centre should be integrated into the management structure.
(e) An information centre reflects the nature of its user and the type of use to which it will be put.

3. It is first necessary to describe the management services function:

(a) The MS department may contain advisors or experts in particular fields; usually in the functions of the organisation, e.g. accountancy or in the general area of problem-solving.
(b) MS staff tend to combine a tactical role with an organisation-wide mobility. They may have access to all areas, although the MS department may be linked to the DP or systems department.
(c) The MS department may be a formally constituted team or an *ad hoc* body called up for special purposes such as systems development. As such, MS would be an adjunct of the organisation's steering committee.
(d) MS must be seen to be neutral. Often the head of MS will report directly to the managing director.

4. Components of an information system include:

I. People – These use the system to fulfil their informational needs. They include end users and operations personnel such as computer operators, systems analysts, programmers, information systems management and data administrators.
II. Computer Hardware – Refers to physical computer equipment and devices, which provide for five major functions.
   b. Input or data entry
   c. Output
   d. Secondary storage for data and programmes
   e. Central processor (computation, control)
   f. Communication

I. Computer Software – Refers to the instructions that direct the operation of the computer hardware. It is classified into system and application software.
II. Telecommunication System/Communication network
III. Databases – Contains all data utilised by application software. An individual set of stored data is referred to as a file. Physical storage media evidences the physical existence of

stored data, that is: tapes, disk packs, cartridges, and diskettes.

IV. Procedures – Formal operating procedures are components because they exist in physical forms as manuals or instruction booklets. Three major types of procedures are required.
   a. User instructions – for application users to record data, to use a terminal for data entry or retrieval, or use the result.
   b. Instructions for preparation of input by data preparation personnel.
   c. Operating instructions for computer operations personnel.

5. The number of people working in the ICT department and what they do will depend on:

(a) The size of the computing facility. Larger computers are operated on a shift work basis.
(b) The nature of the work. Batch processing systems tend to require more staff.
(c) Whether a network is involved. This requires additional staff.
(d) How much software and maintenance is done in house instead of seeking external resources.

Chapter 5

1. This question concerns the relationship between an organisation's objectives and practical performance criteria. The five dimensions would be:

(a) Environment – the things outside the organisation with which it interacts e.g. local people, the trade community, the government, etc. To some extent, this is a public relation function.
(b) Competitive edge or distinctive competence – the way in which the management decides to differentiate its product(s) and/or service(s) in terms of price, quality or reputation.
(c) Marketing thrust – how the organisation seeks to promote itself through advertising, sponsoring, etc. A measure of effectiveness may be the size of the client base or turn over.
(d) Operating efficiency – this is determined by the ratio of internally generated costs of income. Ultimately, control of these costs e.g. labour, overheads, stock, etc., affects profitability.
(e) Human factors – the organisation will seek to create and maintain a human image for the benefit of employees, consumers generally and potential customers.

2. This question addresses the concept of the information systems as a series of interrelated activities in the following areas:

(a) The reason for which the data is needed or used – this may be a permanent requirement, e.g. regular postings to an accounts ledger, or be a response to a transient problem e.g. to combat the effects of a strike. Not all data needs can be predicted.
(b) How data is captured to meet the given need – the design of the data capture system must reflect the timing and the processing requirements.
(c) How the data is processed – i.e. how it is turned into information or made useful. This

will include storage, access, calculating, sorting and presentation e.g. exception reports, level of detail, etc.

(d) The users of the system (or its information) are the people who add value to the data or achieve benefits. If items 1 to 3 are primary data processing, then item 4 onward is secondary information processing. The way in which an accountant will interpret or modify information produced by a computer is an example of this.

(e) The results of the user having the information, e.g. improved knowledge, actions, decisions or any change in behaviour – often these will be intangible. Information has no intrinsic value. Its value lies only in the results, which it can bring about.

(f) The control or feedback of results, which is applied to the system often from the user. This may modify the behaviour of the system to better achieve the needs of the user e.g. improved methods of stock control.

3. The question is about the development of information technology, its applications to information systems and the resultant effect on organisation. This involves the socio-technical systems, i.e. the interface between human and computer base systems. A suitable answer should include some reference to the benefits and dangers.

(a) Benefits:
- Greater efficiency, money saving, enhanced human resources.
- Better decision making through higher information quality
- Increased flexibility and responsiveness e.g. better use of query languages.
- Better user access e.g. user computing and user driven systems development.
- Data sharing across organisation boundaries e.g. the use of a database.
- Increased involvement by the user in information systems development e.g. user computing and prototyping.
- Better communications, internally and externally.

(b) Dangers:
- Data redundancy and lack of consistency due to poor system design.
- Installing excessively expensive technology.
- Systems which are too complicated for the intended users.
- Lack of user involvement in systems leaving the experts to take over
- Security problems and the possibility of fraud or accidental information loss.
- Sub-optimality, i.e. parts of the system are managed to achieve their individual objectives at the expense of the whole system – also known as islands of automation.

4. The stages are as follows:

(a) A trigger or event which starts the activity – usually the input of data or information, e.g. a stock level report or quality control reject.

(b) Problem definition or analysis – the identification of the cause of problems and the separation of cause and effect.

(c) Problem structuring during which a mathematical or conceptual model is constructed, e.g. linear programming and the objectives of the decision process are defined.

(d) Information requirement definition – the decision as to the data which must be captured and processed in order to solve the problem.

(e) Information analysis using mathematical techniques, e.g. regression analysis, or the application of qualitative preferential criteria. One possible result of this stage may be the decision whether enough information of the right quality is at hand or whether further

data capture is required.

(f) The decision itself – the selection of a course of action, change in behaviour or commitment of resources.

5. Conventionally, a three level model of management is accepted:

(a) Strategic or top management.
(b) Tactical or middle management.
(c) Operational or supervisory management.

The character of the decisions could be:

(a) Strategic or top management decisions:
- Very long time horizon, e.g. five – 10 years.
- Radical implications for the whole organisation, e.g. new products new markets.
- Very uncertain outcomes e.g. adoption of new technology.
- High risk, e.g. investment in overseas markets.
- Non-routine, e.g. setting up a new company.

(b) Tactical or middle management decisions:
- Medium time horizon e.g. less than five years.
- Implication for a function under control e.g. accounting or production.
- Moderately uncertain outcome involving the possible use of forecasting techniques and information technology.
- Possible routine decisions, e.g. quarterly budgets.
- Moderate risks as the level of investment is smaller and the decisions are more predictable e.g. manning levels.

(c) Operational or supervisory decisions:
- Short time scale, e.g. 1 day to 1 week.
- Routine and specific outcomes, e.g. achievement of production targets.
- Low levels of risk with much decision support.
- Predictable, well documented information requirements, e.g. office procedures.

STUDY TEXT

Chapter 6

1. The question refers to factors which must be insured against when designing the physical system. In report form an answer would contain:

(a) Vulnerability – this refers to the possibility of a system or its data being wrongly used. Things which place a system at a greater risk include the accessibility to hardware and whether the configuration is centralised or distributed. Further, whether access to files can be made without leaving a trace (as in an access log), and whether the DP centre is located in a high risk area. The recruitment and turnover of staff is also an important factor in increasing vulnerability.

(b) Risk – risk analysis attempts to classify and quantify an organisation's exposure to threats. The quantification is based on probability of an unwanted event occurring, the cost of avoidance, and the cost of loss if the event does occur. Risk factors are often classified by source (e.g. internal/external) or by the method of control (e.g. acceptance, avoidance or insurance).

2. The activities being addressed are those of security planning as a team activity:

(a) The security planning team will involve contributions from:
- Finance department – costings and appraisals.
- Internal auditor – for review.
- Legal department – statutory requirements.
- Public relations – press releases, etc.
- Personal department – changes in jobs.
- Production department – continued working.
- Outside consultants – advice and experience

(b) The detailed work of a team will be:
- Fact-finding and a security audit of the hardware distribution, storage, software requirements and systems controls.
- Producing and evaluating alternative disaster scenarios, with risk analysis performed for critical applications.
- Laying down strategies to cope with the requirements of the disaster scenarios, and producing recovery plans.
- Monitoring and reviewing the plans.

3. This question requires a knowledge of fraud in computer based information systems.

(a) A person may be motivated to commit fraud by a variety of factors including:
- The intellectual challenge of beating the system
- Greed and selfishness
- High levels of debt due to aberrant personal circumstances e.g. gambling or addiction.
- Resentment of the perpetrators' perceived lack of reward
- Jealous of other employees or the organisation itself.

(b) Fraud may be concealed by some or all of the following methods:
- Confusing the situations, e.g. creating a system crash;
- Diverting attention from the actual fraud, e.g. planting evidence of fraud elsewhere in the system, perhaps implicating another individual;
- Delaying the discovery, e.g. by breaking an audit trail;
- Preventing discoveries, e.g. by destroying evidence.

4. Factors which may affect the cost analysis may include:

(a) The probability of a disaster occurring, and the likelihood of a significant loss – a failure to quantify should not justify a failure to set up counter measures.
(b) The unwillingness of management to invest in security, which can show no positive returns under normal circumstances.
(c) The lack of a basis upon which to compare costs.
(d) The fact that some departments may be reluctant to admit their reliance upon the DP functions.
(e). A level of uncertainty about the costs and effectiveness of providing system back-–up.

5. The decisions, which must be made within an organisation that becomes involved in setting up security procedures are in the areas of logical and physical security. The main decision areas would be:

(a) Fall-back systems and continued manual operations.
(b) Alternative hardware provision.
(c) Re-commissioning and restart facilities.

Decisions in these areas would include:

(a) The likely duration of disruption before critical damage to the business occurred.
(b) Whether a full service should be provided to a restricted and/or rotating number of users.
(c) Whether to allow partial service to all users.
(d) Whether to make mutual arrangements with another user running a similar configuration or bureau.
(e) The setting up of emergency facilities.

Chapter 7

1. (a) Main criteria that should be met by a local area network design:

A local area network refers to a transmission process involving computer terminals and peripherals, which are physically linked within a room(s) in a building or one site.

A local area network design should meet the following criteria:

1. It should enhance the sharing of experience resources. For example, management at various levels should be able to share information and as such, design making should be fast and effective. It should also allow programme sharing.
2. It should help in faster data processing and retrieval. This means that the design should facilitate faster access to data from the file servers so as to help in the faster transaction processing.
3. The network should also help in reducing data processing costs. Costs may be saved due to minimised job queue.
4. It should allow sharing of work loads in that the various terminals can be used to process data and transmit it through the network to the required terminal.
5. It should help in decentralisation of data processing activities. Activities can be easily performed in the terminals and transmitted through the network to the head office or to the main data office.
6. The network should enable the communication of one system to another so as to detect multi-accessing and curtail unauthorised access.

1. (b) Reasons for adopting a database as a basis for an information system.

A database is a collection of structured data. It is a non-redundant collection of logically related files organised in a manner that satisfies the needs of an organisation, especially administrative duties.

A database:

- Fulfils the organisation's information needs
- Is designed in such a way that it is only accessible to authorised persons.
- It is organised to enable access and updating of records made by different people in different ways without changing its design.

I would adopt a database as a basis of an information system due to the following reasons:

1. A database avoids the problem of data duplication or redundancy by allowing a single data element to be used in a number of applications. Unlike the traditional approaches whereby data files are created when need arises resulting to a lot of duplication and wastage of storage space.
2. With database as a basis of information system, it is easier to update files as and when need arises. This process may be very tiresome and time consuming in case of traditional file processing approaches.
3. Database enhances data integrity as only those who are authorised to make changes in the files can gain access to the system.
4. Data is independent of the programmes, which use it. Thus database remove data and programme dependence.
5. Database form of information system ensures consistency in an organisation's use of data since all data is integrated and homogeneous in nature.
6. It brings about greater formality over security control, especially over access to the system.

2. Effects of the ?Internet on the following sectors

The Internet is the name given to the technology that allows any computer with telecommunications link to exchange information with other similarly equipped computers. The following are the effects of Internet on the following sectors of the society: -

i) Education

1. The Internet is emerging as a major educational tool. For example, many magazines, newspapers and journals are now available on the web thus availing users of internet a lot of information.
2. The Internet also facilitates education by availing information cheaply to users through the web pages. Users are not required to pay anything to access the information.
3. It also facilitates exchange of information and ideas between various persons thus facilitating sharing of ideas.

ii) Service provision industry

1. The Internet reduces the need for paperwork and all clerical work that accompanies it in the service industry. For example, the printing postage, processing and handling mail costs related to the service are not necessary. For example, a traveller does not require to send mails or travel to a booking office to have a reservation. All he requires is to send an email.
2. The Internet reduces the overall costs incurred by players in the service provision industry in that cost of stationery and staff needed to take orders over the telephone. There are also reduced telecommunication costs and transaction costs because of the automation. This makes business more efficient and economical thus improved profitability.
3. Internet can transform local industries into global players. For example, services consumers will be able to know of the existence of a company and the services it offers by accessing the web.
4. It improves customer relationship as it brings closer the service providers and their customers. Customers can access computers of their suppliers thus it helps them to do their job better. This leads to increased business and thus profitability.

5. Internetworking reduces transaction time thus saving valuable time. In the end, the customer gets improved services with efficiency.
6. The ease of use of online markets is characterised by the fact that systems are so easy to use compared with placing manual service provision requests. Orders can be entered at any time in 24 hours a day with confirmations arriving almost immediately. Customers can check their account status at any time and do not have to wait for monthly statements. This positively affects the operations of the service provision business. For example, an industrialist onlyneeds to access his machine technician's web and call upon him in case of machine failure.

3. Role of database administrator

i) To maintain the database. The database administrator is responsible for making additions, deleting unnecessary information and ensuring that there is no duplication of data.
ii) Maintaining the data dictionary. A data dictionary is an index of data held in a database, which can be used in the maintenance and access of the database. It contains a pool of information concerning a database.
iii) Helping users to overcome the problems that they may encounter when using the database.
iv) Resolving conflicts between users and the technical people.
v) Overseeing the database security.
vi) Evaluating the Database Management System's (DBMS) performance so as to determine whether it meets the organisation's needs.
vii) Enhancing backing up of data and making sure that a data recovery system is in place.
viii) Ensuring compliance with the rules and regulations, for example, statutory legislation such as. Data Protection Act.

4. Industries and business organisations using computer networking

1. Banking industry
   Networking in the banking industries is used to provide such services as CHAPS and BACS.
2. Retailing industry
   Chain stores and supermarkets use computer networking to facilitate branch accounting by linking branches with the head office.
3. Service provision industries
   These industries are networked with their customers so as to facilitate faster delivery of services.
4. Educational institutions
   These may use networking so as to have homogeneous information regarding every aspect. For example, fees collected form students.

   Implications of increased electronic networking on computer security.
   Computer security refers to the protection of data and programmes from threats, which may cause unauthorised changes and modifications of data or programmes as well as protection of information systems to ensure that the system operate as designed.

Electronic networking affects computer security in that: -

1. It may result to unauthorised access to personal or confidential information.

2. It may result to deliberate modification of important data to act as cover-ups to illegal activities.
3. Electronic networking exposes data held in computers which can hurt businesses by exposing their secrets.
4. It could lead to system degradation, for example, where viruses, worms and computer related crimes are transmitted through networks.

5. Situations whereby wireless communication is favourable over guided communication:

1. When there are **geographical barriers** to be encountered e.g. mountains, rivers, and oceans. Geographical barriers hinder cable installation but they do not affect wireless communication. Hence wireless communication is suitable for sites where such barriers are to be found.

2. **Area of coverage is large** e.g. global coverage. Wireless communication would be suitable because there are no cabling costs involved as compared to the high cabling costs that would be incurred with the guided communication.
3. When the **sender and receiver are mobile** e.g. in mobile telephony. Wireless communication would be suitable because it can accommodate the movements of sender and receiver since there is no guided link to tie down the sender and receiver to a specific location.
4. When the **risk of sabotage** must be reduced. Wireless communication is less susceptible to sabotage because of the absence of a cable link between two communicating nodes.
5. **Broadcast communication** e.g. Television broadcasts. Using wireless communication would reduce cabling costs.
6. **Fast deployment is required** e.g. news reporting, seminars, etc. In such an instance, installing a wireless communication network would be faster than installing a guided communication network.
7. **Where cabling may not be run** e.g. listed buildings.

Chapter 8

1.

a) Electronic Data Interchange (EDI)

This refers to a form of computer-to-computer data interchange through agreed standards by all parties. The concept of one computer communicating to another can be faced with major difficulties such as: -

i) Each business organisation wants to produce documents to its own individual requirements and structure.
ii) Different makes of computers cannot easily communicate to one another due to compatibility problems.
iii) Businesses may be working at different time schedules especially when engaged in international trade.

Thus, to ensure electronic communication is possible, agreed formats for these electronic documents recognisable by all parties to the transactions are agreed upon.

The advantages of EDI are:

1. If an organisation is decentralised, EDI can expedite internal billing
2. If an organisation's paperwork is intricate and complex, EDI can speed it up.

The disadvantages are:

1. Joining EDI network is quite expensive
2. There may be problems with deciding which categories of information are to be sent or received.
3. Problem in adapting internal systems so that they match up with EDI translation software.

a) Client-server computing

Client-server computing refers to a way of describing the relationship between the devices in a network whereby the tasks that need to be carried out are distributed among various machines on the network.

A client is a machine, which requests a service. For example, a PC running a word processing application which the user wishes to print out.

A server is a machine that is dedicated to providing a particular function or service requested by a client. They include file server, print server, and fax servers.

A client server system allows computer power to be distributed where it is most needed. This approach has the following advantages:

i) It reduces network communication costs
ii) It allows the central computer to be used for administrative tasks such as network management.
iii) The technological flexibility of this type of system allows the use of sophisticated applications such as multimedia.

b) System specifications

This refers to a complete documentation of the whole system, which is properly maintained or updated as parts of the system are changed or added to. Problems arise in computer installations because of inadequate systems and programme documentation and controls must be set up to ensure that updating procedures are always carried out.

Specifications involve a complete description of a programme usually including flow charts, programme listings, test data and expected results. System specifications are drawn up by the system analyst. There should be programme specifications and hardware specifications for every individual programme or hardware in the system.

c) Electronic point of sale system

This is a terminal unit or a system capable of selling, processing and receiving sales and stock particulars by selling transactions. They are mostly used in retail outlets as terminals connecting the cashier to the computer database containing the stock and sales data. It comprises of three

units namely:

- Bar code scanner
- Cash register keyboard
- Cash register visual screen panel or VDU

When a customer presents an item to the cashier, the cashier either enters the keyboard numbers through the keyboard or uses the scanner to read the bar code. The information is then sent to computer memory, which interprets the information and retrieves the data from the magnitude containing the stock and sale. The system calculates the total amount of purchases and sales before reconciling the stock. It also gives out the itemised receipt and change to customer.

The advantages of this system include: -

1. It is very fast and convenient to both the cashier and customer.
2. It gives more accurate and reliable services.
3. It reduces the need for oriental personnel.
4. It provides automatic control of stock and sales data.

However, the system suffers the following drawbacks:

1. It is vulnerable to mechanical and power failure.
2. It is very expensive and requires large organisation with substance data processing requirements.
3. Updating or alteration of stock or sales data involves a lot of work and cost.

2. The contribution made by information resource centres towards end user computing include:

1. Encouraging users who wish to develop their own applications and providing them with technical assistance.
2. Encouraging users to conform to any hardware or software or programming standards that the organisation might use. For example, to make sure that all microcomputers purchased by the organisation are compatible and so could be moved around from department to department if necessary.
3. Ensuring that applications developed are replicated by others in the organisation where this will be of benefit to the organisation.
4. Advising end users on ways of getting better use out of their existing systems. Computer users might be unaware of what their system is capable of doing or how to set about making use of the system capabilities.
5. The resource centres should be readily available to end users and the centre's staff should try to keep a high profile with end user departments. This enhances adequate support. This can be achieved through the use of a telephone "hot line" or a drop-in advice centre.

3. Factors that guide a systems designer when designing the user interface for a particular application.

User interface refers to the interaction between users and the system. The primary purpose of user interface is to enable communication to and from the user and the computer. The most important feature of computer user interface is that it should be user friendly and, as the name

suggests, user friendly interface is one that the end user finds helpful, easy to learn and easy to use. In this case then, the system designer should consider the following factors in designing user interface.

i) It should be relatively easy for the user to start using the application.
ii) As far as possible, the application should be self-contained so that the user is not forced into accessing manuals or dealing with things that should be kept outside the system.
iii) The amount of effort and information required of the user to get the system to complete required tasks should be kept to a minimum.
iv) The user should be insulated from unexpected or spurious system actions. This includes protection against being the cause of a system failure and implies that the system should also be robust and reliable.
v) The system should be able to feel in control of what is going on in the application.
vi) The system should behave in a logical and consistent manner thus enabling users to reason about what is going on and apply what has been learned.
vii) The application should make it easier to access secondary documents.

Factors influencing re-centralisation of information systems.

Re-centralisation or upsizing refers to the process of consolidating distributed data processing centres into one central processing centre.

1. Systems management is considerably more complex than for centralised systems. For example, systems thatoperate across different platforms, are few and far apart.
2. Distributed systems involve the use of networks. This, therefore, brings about the problem of network management due to lack of appropriate software.
3. Systems administration is also made easier by re-centralisation thus the organisation can adequately provide such. Vital features as system security, database administration, backup and restore, and software distribution.
4. Online maintaining of systems, fault detection tracking and resolution is made easier by re-centralisation.
5. Data and systems security is improved since data is held centrally and is not vulnerable to degradation or other risks associated with computer networking.
6. Re-centralisation helps to reduce communication costs for remote terminals. For example, there is no need for such devices as modems and internet access costs for inter-networked systems.

4. Downsizing

This refers to the process of transferring applications from large computers to smaller ones e.g. from a mainframe environment to a client/server network with many personal computers. Client/server computing refers to a model for computing that splits processing between “clients” and “servers” on a network, assigning functions to the machine most able to perform the function.

Cyber-café

This refers to a facility that enables an individual to access services related to computing and communication such as browsing the Internet, printing, word-processing, photocopying, CD writing and faxing at a cost.

5. World Wide Web (WWW)

This refers to a system with universally accepted standards for storing, formatting and displaying

information in a networked environment. Information is stored as electronic "pages" that contain text, graphics, animations, sound and video.

(i) How the WWW can take services closer to people:

1. WWW enables **online teaching/instruction.** A tutor of ABC College could conduct a class for many students of the college located in different geographical areas. The students simply need to log-on to ABC's website and access the live streaming video of the class, which is being conducted at ABC's head quarters.

2. WWW can facilitate **sharing of information to online users.** The information could be placed in web pages and links provided between webpages to enable easy access to the information. Thus, ABC College could, for instance, share study packs online to registered students thus enabling distant students to easily access study resources.

3. WWW makes it possible for students of ABC College to easily participate in **discussion forums.** A discussion group facility could be implemented in the College's website to enable students to post their views via e-mail. Students need not travel to the College to participate in discussion forums.

4. WWW can enable students to sit for tests/exams at their own convenient locations through **online testing.** Students only need to go to the closest exam centre as opposed to going all the way to ABC's headquarters.

(ii) Managerial issues critical for the successful implementation of WWW:

1. Proper planning of resources e.g. funds, hardware, and software required, personnel required, etc
2. Adequate control mechanisms have to be put in place to ensure security of the system.
3. Training of staff to ensure they are competent with the system.
4. Education of staff on the importance of WWW so as to reduce potential resistance to the introduction of WWW into an organization.
5. Reengineering of business procedures to accommodate WWW where possible in order to ensure maximum utilisation.

KENYA ACCOUNTANTS AND SECRETARIES NATIONAL EXAMINATIONS BOARD

CPA PART II

SYSTEMS THEORY AND MANAGEMENT INFORMATION SYSTEMS

1 December 2004. **Time Allowed: 3 hours.**

Answer any FIVE questions. **ALL questions carry equal marks.**

QUESTION ONE

(a) Certain employees will always be placed in positions of trust, for example senior systems analysts, database administrators and information systems security managers. Such employees can, therefore, compromise the security of information systems if they so wish.

Required:

(i) Explain three control measures that an organisation should institute over these employees and guarantee the security of the information systems. (6 marks)

(ii) Every individual in an organisation has some opportunity to commit computer fraud. The potential for which they can do so depends on a number of factors. Examine three of these factors. (6 marks)

(b) Ethical principles can help in evaluating the potential harms or risks in the use of information communication technology.

Required:

Explain ant two principles of technology ethics. (4 marks)

(c) Explain the advantages to an organisation in having users involved in developing an information systems application (4 marks)

(Total: 20 marks)

QUESTION TWO

(a) Some of the major challenges facing the convergence of networks in businesses is performance, that is, the network can at times be painfully too slow and result in high interconnectivity costs.

Required:

(i) Explain the meaning of the terms “bandwidth” and “ interconnectivity costs”. (4 marks)

(ii) Examine four factors that can determine the extent to which network performance degrades or slows down. (8 marks)

((iii) Explain two strategies that business organisations can adopt to keep network costs low. (4 marks)

(b) Identify any four common reasons for losing data in computer-based systems. (4marks)

(Total 20 marks)

QUESTION THREE

(a) Quality assurance and testing are important in developing and delivering information systems.

Required:

Briefly describe four characteristics of quality assurance you would expect to find in a software product. (8 marks)

(b) It is always recommended that any new system should have a graphical user interface (GUI) to make it easier to use than current character-based systems.

Required:

Briefly describe what is meant by a graphical user interface (GUI). (2 marks)
Discuss two limitations associated with the implementation and use of GUI. (6 marks)

(c) Identify four major factors that influence the structure of an information system (4 marks)

(Total 20 marks)

QUESTION FOUR

(a) Transaction processing systems capture and process data resulting from the occurrence of business transactions, to update organisational databases in order to produce a variety of information products.

Required:

Explain the five stages of a transaction processing cycle. (10 marks)

(b) A data dictionary is a repository of information about data.

Explain the characteristics of a data dictionary. (4 marks)

(c) The concept of an intelligent workstation is a combination of a personal computer and access to a local or wide area network. The hardware, software and communication are integrated into one facility.

Required:

Define and differentiate functional integration and physical integration in a workstation environment. (6 marks)

(Total 20 marks)

QUESTION FIVE

(a) The company you work for intends to computerise its payroll application.
Explain the functional capabilities that the system should have for it to serve the intended purpose. (8 marks)

(b) Outline four features of a word processing software package. (4 marks)

(c) Explain the importance of documenting and agreeing on the information systems requirements. (6 marks)

(d) Name the basic requirements for internet connectivity. (2 marks)

(Total 20 marks)

QUESTION SIX

(a) Wanjeshi Sacco Ltd. is intending to introduce a corporate database to support a variety of its information needs.

List two organisational, technical and human factors to be considered in the process of establishing the corporate database environment. (6 marks)

Propose two database models that can act as design alternative options. (2 marks)

Explain four database areas in which the company would be justified in restricting employee acce ss. (8 marks)

(b) Explain four network management functions. (4 marks)

(Total 20 marks)

QUESTION SEVEN

(a) Give four reasons that may make an organisation abandon an information systems project. (8 marks)

(b) List four problems that are faced when using standard files for data processing systems. (4 marks)

(c) Name four modern computer-based information systems' structures that support the sharing of data or information and other resources. (4 marks)

(d) Differentiate between deterministic and random systems giving examples in each case. (4 marks)

(Total 20 marks)

QUESTION EIGHT

(a) The owner of a chain of auto-accessory shops in five different towns inputs sales figures into a computer model that displays the selling trends of each store. She uses her own observation form visits to the shops and information gained from the model to make ordering decisions for each store.

Required:

Are the ordering decisions she makes structured, semi-structured or unstructured? Briefly explain the reasons for your choice and outline what product related variables are involved in the ordering decisions. (10 marks)

(b) Certain financial problems such as simplified bread-even analysis models for predicting profits can be computerised.

$P = (S_p - V_c) U - F_c$

Where:

P	=	Profits
S_p	=	Selling price per unit
V_c	=	Variable cost per unit
U	=	Number of units of sales
F_c	=	Fixed cost

Required:

Using the above model, describe any three decisions that management can make from the break-even analysis model. (6marks)

Why do organisations automate reasoning or decision-making tasks which human beings are naturally better able to perform than computers? (4 marks)

(Total: 20 marks)

MODEL ANSWERS

MODEL ANSWERS TO
THE CPA PAPER SET IN
DECEMBER 2004

MODEL ANSWERS TO PAST CPA EXAMINATION PAPERS

MODEL ANSWERS TO THE CPA PAPER SET IN DECEMBER 2004

QUESTION ONE

(i) These employees perform the following jobs.
Senior Systems Analysts – Heads of system analysts. These employees analyse the existing system with a view to their computerisation. They design systems and oversee their implementation and review. They are actively involved in the upgrading of the system.

Database administrators – they ensure that the data in the database meets the information needs of the organisation involved in retrieving data and structuring reports, which are appropriate to the organization.

Systems security managers – they are involved in ensuring the security of the system is not compromised. They ensure that no outsiders or unauthorised persons access the information.

From the above information, it can be seen that these employees access valuable information and if they are compromised then the firm can suffer. The following measures are put in place to curb this.

1. Administrative controls – they include.
   (a) Policies – policies outlining and requiring each employee to do certain things and not others. Things not authorised to be done are threats to security.
   (b) Administrative procedures – put in place by an organisation to ensure that users only do what they are authorised to.
   (c) Legal provisions – these serve as security controls by laying down legal penalties which may be suffered in case of breaches in security.
   (d) Ethics – a strict code of conduct by the organisation to be followed by the employees can boost security.

2. Logical security controls – these are measures incorporated within the system to provide for security against the employee. This includes the need for passwords to access any information.
3. Physical controls –includes lockups. The offices should be locked at the end of the day and no employee should access the others office. It also encompasses employing security guards to prevent unauthorised access.
4. Rotation and Compulsory Leave – an employee should not be allowed to stay in one place for long but should be rotated. Due to this threats of fraud are discovered in advance. Compulsory leave should be given and work reviewed in case of any perceived threat on security.
5. Good remuneration – the employees should be paid well to guard against being compromised.

(ii) Every individual in an organisation can commit fraud. The potential of an employee committing fraud depends on the following: -

1. Security – inadequate security and loopholes in the security system can be a potential motivator to an individual to commit fraud. An employee who knows that he can commit fraud without being found out would be greatly motivated.
2. Remuneration – individuals who are poorly paid are highly susceptible to committing fraud to make their ends meet.

3. Company policies – if employees are aware that the organisation policies are not stringent, then they are likely to be involved in fraud. Absence of policies like rotation of employees or compulsory leave will be driving factors as chances of being caught are low.
4. Ethics – the code of conduct of a company also plays a major role. In organisations where there is laxity then the chances are high that employees will engage in fraud.
5. Legal provisions – where no legal sanctions are imposed on the employees if found guilty of fraud, they could engage in fraudulent activities.

B) Principles of technological ethics include: -

(a) Honesty and trustworthy – a honest computing professional should not make deliberate or deceptive claims about a system or systems design, but should instead provide full disclosure of all pertinent system limitations and problems.
(b) Privacy - it is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. Data should be protected from unauthorised access.
(c) Integrity – the information users and professionals should maintain integrity in use of the information. This ensures the accuracy and reliability of the information stored in computers.
(d) Confidentiality – this involves respecting of data which touches on individuals. This is to respect all obligations of confidentiality to employers, clients and users unless disclosure is required by law.

C) Advantages of users being involved in developing an information system application:

(i) Users know the internal quirks of the system in order to get required information.
(ii) Improves relationship between users, management and developers
(iii) Improves system literacy of users and subject understanding of developers.
(iv) Conflict resolution becomes the responsibility of both users and developers. This eases conflict resolution.
(v) Improves the system analyst's time by focusing on work relations and gathering project resources simultaneously.
(vi) Lowers cost of system development by defining requirements completely and correctly in a short time period.
(vii) Increases team satisfaction confidence and support
(viii) Reduces maintenance time due to earlier application completeness and correctness of information.

QUESTION TWO

2 (i) Bandwidth – bandwidth is the bits-per-second (bps) transmission capability of a communication channel. It also refers to the amount of data that can be transmitted in a fixed amount of time. There are three types:-

(i) Voice band – bandwidth of standard telephone lines.
(ii) Medium band – bandwidth of special leased lines used.
(iii) Broadband – bandwidth of microwave, satellite coaxial cable and fibre optic.

Interconnectivity costs
These are costs incurred in running a network. These costs basically include the subscribing costs which run when the network is interacting with other networks. It also includes unquantifiable costs like security threats.

(ii) Factors that determine the extent to which network performance degrades or slows down: -

i) bandwidth – the size of the bandwidth will determine the speed of network. A large bandwidth will be sufficient to support a large number of network users without slowing down the network.
ii) Software - For example, a network operating system with a high performance (e.g. linux operating system) can be able to provide a high network performance.
iii) Hardware – different hardware have different capability thus if the hardware is outdated

then the network will slow down.

iv) Dedication of the servers – when a server is connected to different networks then it will be painfully slow down as so many users are using the server. As such servers should be connected in a way to serve limited networks for optimum performance.

Software – the software of the components of a network will have influence on the network.

QUESTION THREE

3 (i) Strategies – are plans made to improve the position of a situation. The strategies to be adapted are:-

Dedication of servers – servers in the organisation should perform specific functions to reduce overload on the server leading to slowness and thus decrease the costs that arise when the network is down.

Working offline – the organisation should do most of the work offline and only go online when sending or in need of information online.

Use updated software – make use of modern software, which do the work faster and better. This could be done by either updating the software or just getting new software.

Common reasons for losing data

(i) Ignorance – a software user may delete data files maintained by a software because he/she does not know how to operate the software or is unaware of the consequences of deletion.
(ii) Accidents – a user may accidentally delete data files maintained by software due to mistaken identity of files.
(iii) Fraud – employer may access and delete security log files to cover any illegal activities taking place.
(iv) Malice – hackers may delete organisational data in order to bring down the operations of an organisation.
(v) Poor management of data stores – could result in the theft of companies' diskettes containing sensitive data.

3 (a) Quality assurance – involves the entire software development process. It is the monitoring and improving the process making sure that any agreed procedures are followed and problems are found and dealt with. The characteristics are:-

(i) Reliability – the software should fit the users' requirements and perform the functions they are designed for.
(ii) Documentation – the software should be accompanied by a manual, which is easy to understand. This helps in use and maintenance of the software.
(iii) User friendliness – the software should be easy to use with clear on screen prospects, menu driven and extensive screen help facilities.
(iv) Controls – it should have in-built controls which may include passwords, options, validation checks.
(v) Up-to-date - the software should be updated.
(vi) Modification- the software should be modifiable to fit the requirement of users.
(vii) Compatibility of software - it should integrate easily with other software in use in the system.

(b) Graphical User Interface (GUI) – refers to the interaction between end users and the computer based upon a graphical display. These are tools designed to enhance personal computing work. They are mostly fitted on work stations or personal computers with graphical adaptors able to support high resolution graphics.

Limitations of Graphical User Interfaces:

i) System slows down – when you open so many windows, which have the GUI facility, the system will slow down.
ii) Too much information – the user cannot focus on all the information presented to him on

the GUI

iii) Inflexible icons – the icons take you to specific location and if you want to change your cursor you have to go back to the first window, which is cumbersome in a way.

(c) Information System – refers to a collection of components that collect, process, store analyse and disseminate information for specific purposes. The factors influencing its structures are:-

(i) Cost – a complex information system is expensive so a firm will design a system they can afford to run.
(ii) Requirement – the information requirement will determine the structure or the information system of an organisation.
(iii) Level of training – the knowledge of users will also determine the structure of an information system. A complex system structure will require more training thus a company may decide to have a less complex one to limit training costs.
(iv) Existing software – the availability of software that can support a system will have an impact on the structure of the system.
(v) Availability of staff – the number of staff with knowledge to run a system will have an impact on the structure of the system.
(vi) Availability of hardware to support the system. If such hardware is unavailable then the company will search for an alternative structure.

QUESTION FOUR

4 (a) Stages of a transaction processing cycle.

(i) Processing of inquiries – the system processes the inquiries made using the database.
(ii) Processing the transaction – depending on the outcome of the inquiries, the system processes the activity such as buying or selling
(iii) Making decisions – the system uses application to support systems for planning, analysis and decision making. Decisions are made on the transaction e.g. at what price to sell.
(iv) Update master file – the system then stores the information relating to the transaction.
(v) Produce reports – the system winds up by producing a report on the transaction.

Inquiries

Processing

Decision

Storage

Report

4 (b)

Data dictionary is an automated manual tool for storing and organising information about the data maintained in a database. A data dictionary is a file, which defines the basic organisation of a database. It contains a list of all files in the database, the number of records in each file and the name and types of each field. All data elements contained in data dictionary are accompanied with a short description on what they are.

Its characteristics are:

(i) A query facility - this is both for administrators and users. It helps users to perform searches on items like business definitions, user descriptions or even synonyms.
(ii) Automated input facilities:- these are to enable loading of records
(iii) Security features:- to help in protecting the information contained in the data dictionary
(iv) Comprehensive data reporting language for user designed reports.
(v) Language inter-phase, to allow, for example standard record layouts to be automatically incorporated into programmes during the compiling process.
(vi) Help facility – this helps to instruct users on how to use the data dictionary.

(c) (i) Functional integration – this is the dividing of the functions among individuals in a work station. An individual is only allowed to perform particular duties and not others. It differs from physical

integration in that one machine can be used by different persons. In functional integration, individuals will be involved in different duties.

(ii) Physical integration – this is the allocation of work machines to individuals to use in the firm. A particular person is assigned a machine to work on and no sharing of machines takes place. However, people can perform the same functions under this form of.

QUESTION FIVE

5) Functional requirements required

(i) User requirements – the system should be able to meet the needs of the firm and its users as closely as possible.
(ii) Processing time – it should have a short response time. A faster system will be appropriate.
(iii) User friendliness – the system should be easy to use with clear on screen prompts menu driven and extensive on screen help facilities.
(iv) Controls – the system should have in built controls, which may include passwords, validation checks, audit trails, etc., to boost information and data integrity.
(v) Flexibility – the system should allow for future modification in case of requirement changing.
(vi) Compatibility – the system should be compatible with other system to allow simulations with user systems
(vii) Portability – the software should be able to run on the firms different machines.

5 (b) Four features of a word processing software package:

(i) A drawing tool bar to enable one to accommodate various shapes and lines in word processed documents.
(ii) Automated formatting such as bolding, italicising, underlining, capitalising, indenting and paragraphing of text.
(iii) Print previews, which enable one to see the output and identify areas of improvement in the formatting and layout.
(iv) CV, letter, memo and other document wizards, which guide one through the document creation process.
(v) Help to provide assistance to users.

5 (c)

a) Documentation – this is the description of a software in written form after its development. The importance of documentation includes:

(i) It guides the development team at various stages of the development life cycle.
(ii) Can be used as a system back-up copy should something happen to its implementation.
(iii) It aids or assists during system maintenance since it guides in identification of system modules to be changed.
(iv) Effectively provides a check list of items to be covered during subsequent system audit maintenance.
(v) Guides against loss of system understanding particularly when the author leaves the company or dies.
(vi) Acts as a training guide for users.

b) Importance of agreeing on the information system requirement:

(i) Improves relationship between users, management and developers. It ensures that potential dispute areas are reduced.
(ii) Lowers the cost of system development by defining the requirement time completely and correctly.
(iii) Increases team satisfaction, confidence and support.
(iv) It makes it easier to plan to project as the total costs can be estimated with more accuracy.

c) Basic requirement for the internet connection

(i) Modem – a transmitter which decodes the information.
(ii) Computer – the source and destination for the data.
(iii) Wire a complex network – this is the transmission system

(iv) Internet service provider (ISP) – provides access to the internet at a periodic cost.

QUESTION SIX

6 (a) **Factors to be considered in the process of establishing the corporate database**

Firm/Organisation:

(i) Requirements by the organisation.
(ii) Effect of the system on the existing organisation structure.
(iii) Implication to the company as a result of the new system.
(iv) Effect on the current working practise.

(v) Technical

(i) Hardware and software requirement of the system.
(ii) The current technology and whether it can support the system.
(iii) Whether there are specialised persons to handle the system once installed.

Human

(i) Redundancy or retrenchment, implication to the company as a result.
(ii) The reaction of individual both from within and without the organisation.
(iii) Necessity of training.

Hierarchical Data Model – it presents data to users in a tree like structure.

Network Data Model – a logical database model that is useful for depicting many-to-many relationship.

Relational Data Model – a type of model that treats data as if they were stoned in two dimensional tables. Related data is stored together or near each other.

Database areas which need to be restricted.

Sensitive data – applies to information that requires special precautions to assure the integrity of the information, by protecting it from unauthorised modification or deletion. It is data that requires a higher than normal assurance of accuracy and completeness e.g. passwords, on encryption parameters.

Confidential data – applies to the most sensitive business information that is intended for strict use within an organisation. Its unauthorised disclosure could seriously and adversely impact the organisations image in the eyes of the public e.g. application programme same code, project documentation, etc.

Private data – applies to personal data intended for use within the organisation. Its unauthorised disclosure could seriously and adversely impact the organisation and/or its customers e.g. customers account data, e-mail messages, etc.

Public data – applies to data that can be accessed by the public but can be updated/deleted by authorised people only e.g. company web pages and monetary transaction limit data.

(b) Network management functions include: -

(i) Resolving conflict between users and technical people when using the system.
(ii) Overseeing the network security
(iii) Evaluating the network performance to see whether it meets the organisational needs.
(iv) Ensuring compliance to rules by the network.
(v) Maintaining the network and ensuring its operation is up to date.

QUESTION SEVEN

7 (a)

(i) Failure to establish upper-management commitment to the project.
(ii) Lack of organisations commitment to the system development methodology.
(iii) Taking shortcuts through or around the system development methodology can lead to system failure and hence abandonment.
(iv) Insufficient resources both financial and otherwise.
(v) Failure to adhere to the set budget, time and finances.
(vi) Premature commitment to a fixed budget and schedule.
(vii) Obsoleteness of the system under development.

7 (b)

(i) The standard files are inflexible hence may not adapt to your requirements.
(ii) It limits creativity as you have to adhere to set rules.
(iii) Does not give competitive advantage over rivals, as the features are same.
(iv) It is hard to get standard files which fit all your requirements.
(v) Its security controls are not so effective thus can be infiltrated easily.

Problems faced when using standard files for data processing systems:-

(i) Data redundancies and confusion in data storage
(ii) Difficult to effectively secure data.
(iii) Difficult to modify data due to data redundancies.
(iv) They require a lot of storage resources due to data redundancies.

7 (c)

(i) **Management Information System (MIS)** – provides continuous information to decision makers to make structured, recurring and routine decisions.
(ii) **Decision Support Systems** – provides problem–specific support for non-routine dynamic and often complex decisions a problem.
(iii) **Expert system** – it is knowledge system which provides information when interacted with.
(iv) **Data Management System** – it's a system that stores data for use by various individuals.
(v) **Virtual Reality System** – it is a 3–dimensional simulation software where the user is immersed in a simulated environment using special hardware.

7 (d)

Deterministic systems – it's a system in which various steps/activities follow one another in a sequential manner in a totally predictable way e.g. A will happen, then B then C.

Examples of such systems are :-

(a) Fully automated production process.
(b) Computer programme.

In such a system, there is predictable input and output as the system reacts in a predictable way.

Random systems – also known as probabilistic or stochastic system. It is one in which some steps/ activities can be predicted with certainty and other will occur with varying degrees of probability. There are many probabilistic systems in a business organisation e.g. provision of bad debts.

QUESTION EIGHT

8 (a)

Structured decisions – these are repetitive and defined decisions. A standardised pre-planned approach is used to make the decision and a specific methodology is applied routinely.

Semi structured decision – the information requirement and the methodology to be applied are often known, but some aspects of the decision still rely on the manager. As such the manager can exercise some discretion in the making of decisions.

Unstructured decision – tends to be unique. The information needed for decision–making is unpredictable and no fixed methodology exists. Here, the manager exercises a lot of discretion.

From the above definitions, it's clear that the decision made by the owner of this classic stone is semi-structured. She incorporates the information from the computer, which is automated and uses judgment to make decisions. The product related variables in making orderly decisions are :-

(i) The quality of the products.
(ii) The quantity to be ordered.
(iii) The availability of the products needed.
(iv) The availability of supplies and reliability.
(v) Availability of cash to purchase.

8 (b) Decisions that management may make from the break-even analysis model:

- Decision on the selling price of the products in order to obtain a certain profit.
- Marketing decision in order to make the required sales.
- Determining the variable costs of the products in order to make required profits. This could be by buying cheaper raw materials.
- Decide the number of unit to be produced.

(ii) An expert system is a system that acts as an expert consultant to users. Reason for its use include: -

- For consistency in the decision-making process.
- Speed - the expert system is faster than a human being expert.
- Permanence – the experts can die or leave but an expert system can be used for a long time, use will only stop if it is changed.
- Remote areas – expert system can be used in areas where human beings fear going e.g. Arid areas, bad climate area etc
- Objectivity – decisions made by expert systems are not guided by passions or feelings. As such, decisions are always in the best interest of the organisation.
- Experts are costly to maintain, expert systems on the other hand involve only one-off costs (their acquisition).

GLOSSARY

GLOSSARY

ALGOL (ALGOrithmic Language) – a high level programming language based on algebraic principles that are used frequently in developing mathematically based applications**.**

Algorithm – a sequence of predefined rules, procedures and selection criteria which may be applied to resolve problems with a predictable structure.

Analogue computer – a computing device which operates on data represented in the form of physical measures such as temperatures or air pressures as opposed to digital computers which utilize data in numeric forms.

Applications software – programs designed to process data for particular user needs, e.g. payroll application, word processing, etc.

Artificial Intelligence – application of computer-based technologies to mimic certain problem-solving abilities of humans, usually related to structured or semi-structured problem situations.

Batch processing – aggregating similar types of data requiring similar processing into groups or batches and processing these together rather than individually, thus deriving economies of scale in the processing of the data.

Baud – measure of the speed at which data is communicated along a channel, the number of signal pulses per second.

Buffer – either an insert to separate one block of data from another, or an area of storage which is used to store transitory data, e.g. the CPU can supply data to a printer device faster than the printer can physically operate, hence the CPU transmits blocks of data for printing to the printer's buffer store and the printer reads the data as required from its buffer store.

CAD/CAM (Computer Aided Design and Computer Aided Manufacture) a generic term applied to the development and design of systems to support design work and to control manufacturing operations.

Central Processing Unit (CPU) – main unit of the computer which holds the software instructions and data, performs the execution of these instructions and controls all the associated peripheral devices.

Closed system – a system which has no interaction with its environment.

COBOL (Common Business-Oriented Language) – a high-level programming language primarily designed for the development of commercial or business data processing applications and, despite its antiquity, still used extensively.

Computer schema – the overall structure of a database expressed in logical terms and used in database design and development.

Console – the interface unit between the user and the computer, typically in the form of a typewriter keyboard but also employing other ergonomically efficient devices, e.g. mouse.

Database – a collection of data in the form of records, usually appropriate to more than one user application, which are held centrally and accessed and updated by different users.

Database Management System (DBMS) – software used to build, maintain and control user access to the database files.

Decision Support System (DSS) – collection of data, software, tools and techniques designed to aid decision-makers to analyse problems, and to evaluate and select appropriate solutions.

Encryption – a way of encoding data by using hardware and/or software processes that is designed to enhance the security of data during transmission and storage; it usually requires the reversal of the coding process at the receiving end, **decryption.**

External schema – the user's view of the structure and contents of the data elements in a database, applied in database construction and development.

FORTRAN (FORmula TRANslator) – high-level programming language used primarily for mathematical computations.

Heuristics – rules of thumb or intuitive approaches to problem-solving.

Information centre – a location within the organization at which the users may gain access to information to support their operational needs.

Internal schema – definition of the internal physical structure or organization of the database to be constructed.

Network – system of communication channels interconnecting users at different locations.

Normalisation – a term applied in relational database design referring to the process of simplifying the logical relationships within the database structure.

Protocol – a set of rules or standards governing the format and methods employed in the transmission of data, necessary to ensure the effective exchange of data between devices within a computer system or users within a network.

Prototype – the initial model of the system to be developed incorporating sample input and output screen layouts, information content and operating guidelines etc; it is used to facilitate user trials and record observations.

Query Language – programming language designed to construct the user's interrogation enquiries in a database system.

Relational database – database system structured on the basis of the relationships between the data elements and records within the system.

Spooling – the use of secondary devices (e.g. disk or tape) to act as an interim buffer store between input and output peripheral devices (e.g. keyboards or printers) to reduce delays in processing due to slow operating speeds of these peripherals relative to the central processing unit, i.e. it creates a queue.

Systems Development Life Cycle (SDLC) – the stages involved in the initiation, analysis, development and implementation of an information system.

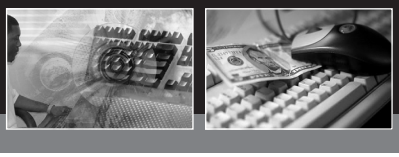
Timesharing – a common variety of operating system within a computer which slices up the central processor time available and allocates access in rotation to each user for the slice of time.

WIMP (Windows, Icons, Mouse and Pull-down menus) relates to a combination of these features in developing the human interface between the user and the computer system.

Workbenches – collection of software and hardware tools and facilities designed to support the work systems analysts, designers and programmers; usually integrated within a single workstation.

Workstation – standalone computer or terminal which provides a combination of hardware and software facilities to support the specialist activities of particular types of users

INDEX



Index

REFERENCES

REFERENCES

ACCA: Paper 2.1 **Information Systems** Foulks Lynch, 1999

Eardley, A; Marshall, D V & Ritchie, R L: **Management Information Systems**, ACCA

French, C. S.: **Data Processing and information technology 10th Ed** DP Publications, 2004

Laudon, K.C. and Laudon J.P.: **Management Information Systems: Managing the Digital Firm, 7th ed**., New Jersey: Prentice-Hall, 2002

Lucey, T**.: Management Information Systems.** 8th ed. London, DP Publications, 1998.

O'Brien, J.: **Management Information Systems: Managing Information Technology in the E-Business Enterprise.** 5th Ed. Boston, McGraw Hill-Irwin inc, 2002.

O'Leary, T. J.: **Computers and information systems** Benjamin/ Cummings, 2001

Turban, E, McLean, E. & Wetherbe, J.: **Information Technology for Management.** 3rd ed. John Wiley & Sons, 2002.

Zwass, V.: **Foundation of Information Systems***,* Boston: Irwin/McGraw Hill, 1997