INFORMATION COMMUNICATION TECHNOLOGY

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 programs automatically accepting, storing and processing data to produce information that is the result of that processing.

The forms of information processed include:

- Data – e.g. invoices, sales ledger and 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.

2. Why use computers?

Use of computers has become a necessity in many fields. Computers have revolutionized 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 programs are correct, they will always give correct output. A computer is 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, which 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.

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. More specific examples include:

- **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.

- **Organizational 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 organization 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 used
    - as research tools, complex computations
    - for simulation e.g. outer-space simulations, flight simulations
    - as diagnostic and monitoring tools,
    - 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 organizing and disseminating educational resources. Such E-learning and virtual or distributed classrooms have enabled the teaching industry to have a global reach to the students. Computers are also used for test scoring uniform tests done in schools, school administration and computer aided instructions.

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

- **Manufacturing and production** – computer aided design (CAD), computer integrated manufacturing (CIM), process control systems among other technologies are computer systems that have revolutionized the production industry.

- **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 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, a series of breakthroughs in electronics have occurred leading to great improvements in the capacity, processing speed and quality of computer resources.

The evolution of computerization 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.

- **1940s**: Mathematical techniques developed in World War II (operations research) are applied to the decision making 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, 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 program* computer
- 1947 ENIAC (Penn)- first *electronic* stored program 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"

5. Computer Generations

The view of computers into generations is based on the fundamental technology employed. Each new generation is characterized 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 programs 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 programs, input and output

ii. Second Generation Computers (1958 - 1964)

- Replaced vacuum tubes with transistors.
- The transistor is smaller, cheaper and dissipates 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 are smaller than electric tubes and have higher operating speed. They have no filament and require 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, lower cost, larger memory and 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 take its own decision.

6. Classification of computers

Computers can be classified in different ways as shown below:

Classification by processing
This is by 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 by the use to which the computer is put.

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

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

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

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

b) Second generation. 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. Computers of the 1960s. Made use of Integrated Circuits. Speeds of up to 1MHz. Examples include the IBM system 360.

d) Fourth generation. Computers of the 1970s and 1980s. Used Large Scale Integration (LSI) technology. Speeds of up to 10MHz. Examples include the IBM 4000 series.

e) Fifth generation. Computers of the 1990s. Use Very Large Scale Integration (VLSI) technology and have speeds up to 400MHz and above.

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 centralized processing for large commercial organizations. 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 organizations or as the main computer in medium-sized organizations. 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.

7. Data representation in computers

Data exists as electrical voltages in a computer. Since electricity can exist in 2 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)
- Program 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 (American Standard Code for Information Interchange) 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 programs 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

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 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

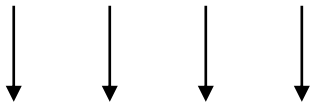
010	001	110	011
↓	↓	↓	↓
2	1	6	3

(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 sixteen 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.

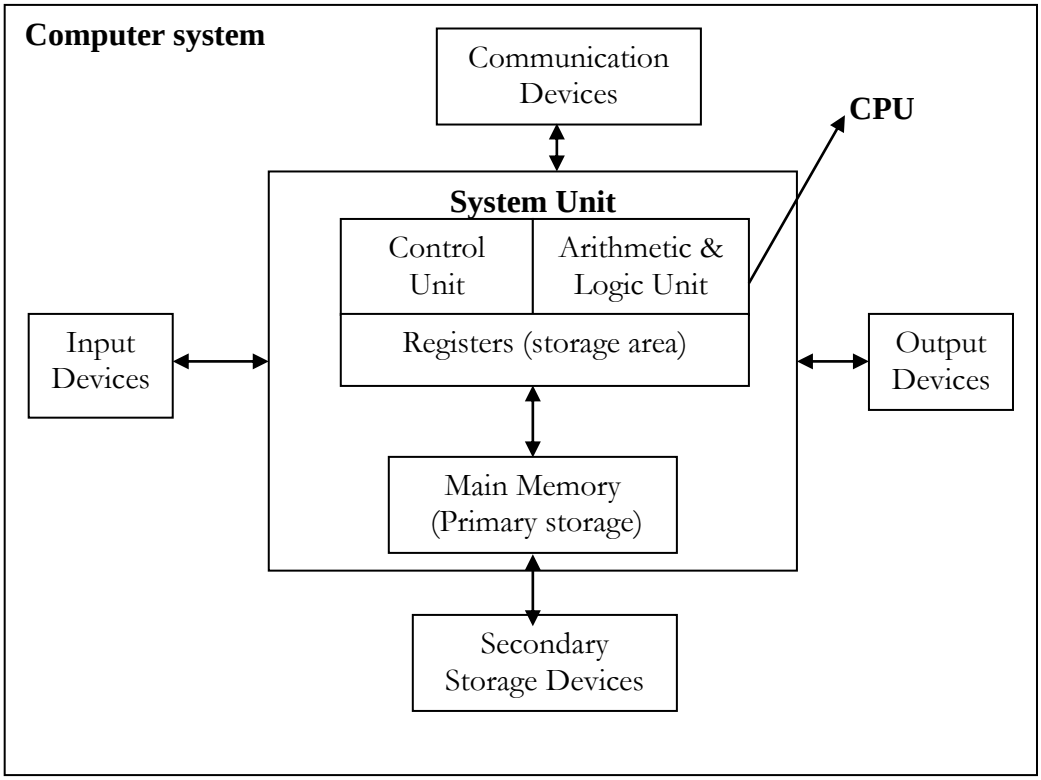
That is 0001 0010 1010 0000



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 program and data into computer system.

- **Central Processing Unit (CPU) -** This is the part of the computer that processes data. Consists of main memory, the control unit and the arithmetic and logic unit.
- **Main Memory** – Temporary storage to hold programs and data during execution/ processing.
- **Control Unit** – Controls execution of programs.
- **Arithmetic Logic Unit (ALU)** – Performs actual processing of data using program instructions.
- **Output devices** – Displays information processed by the computer system.
- **Storage devices** – Permanent storage of data and programs 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 programs), 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 as follows:

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 the home.

- **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 programs 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 or stores. They are popularly used at gas stations for customers to select the grade of gas or request a receipt at the pump (in developed countries), as well as in fast-food restaurants to allow clerks to easily enter orders.

ii. 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, standardized tests, such as the KCPE, SAT or GMAT are scored.

iv. 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 authorized 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 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 CPU (Central Processing Unit)

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 program 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 each other.

(ii) Main Memory

Primary storage, also called main memory, although not a part of the CPU, is closely related to the CPU. Main memory holds program 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 been 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

– Outputs printout on paper often referred to as hard-copy output.
Categorized 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

Forms 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

Forms 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 device s. 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 vocalized sounds to produce output.
- The computer "speaks" synthesized 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, the 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 magnetized 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 fool proof. Most are internal, but disks that use removable cartridge are available. Disk compression can be used to increase capacity but slows 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 written and read more than once. Has a capacity of 650 MB.
    - DVD-ROM (Digital Video Disks) – They are similar to CDs except that it has 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. Uses 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 magnetized 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.

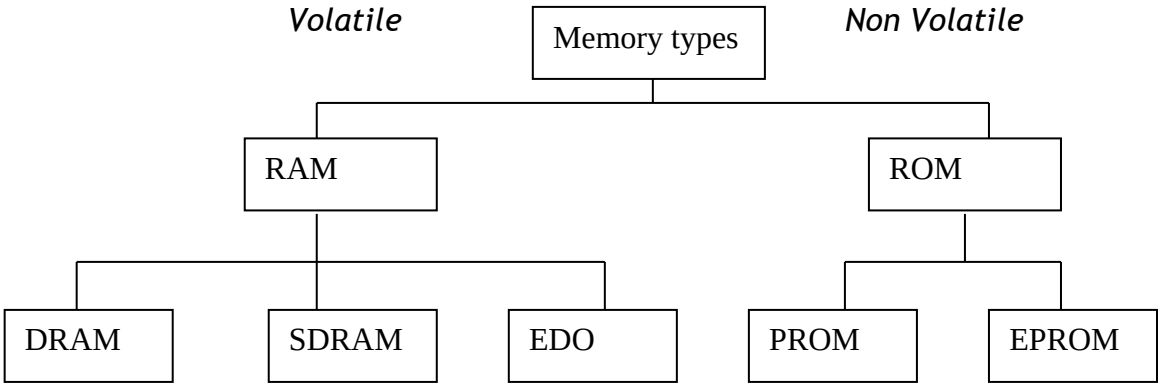
- Fax/modem - basic digital/analog modem enhanced with fax transmission hardware that enables faxing of information from computer to another fax/modem or a fax machine *(NOTE: a separate scanner must be connected to the computer in order to use the fax/modem to transfer external documents)*

Computer Memory

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. Specialized 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



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 programs 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 is non-volatile, so the contents aren't lost if the power is disrupted. ROM provides permanent storage for unchanging data & instructions, such as data from the computer maker. It is used to hold instructions for starting the computer called the bootstrap program.

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) cost effective. 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 - Cache memory 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 program which guide computer hardware. A computer program is a sequence of instructions that tell the computer hardware what to do. Programs are written in programming languages, which consists of a set of symbols combined according to a given syntax.
A program 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

Systems software consists of programs 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 programs manage the "behind the scenes" operation of the computer.

Examples

- Operating systems
- Utility Programs - Utility programs often come installed on computer systems or packaged with operating systems. Utilities can also be purchased individually. Utility programs 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:

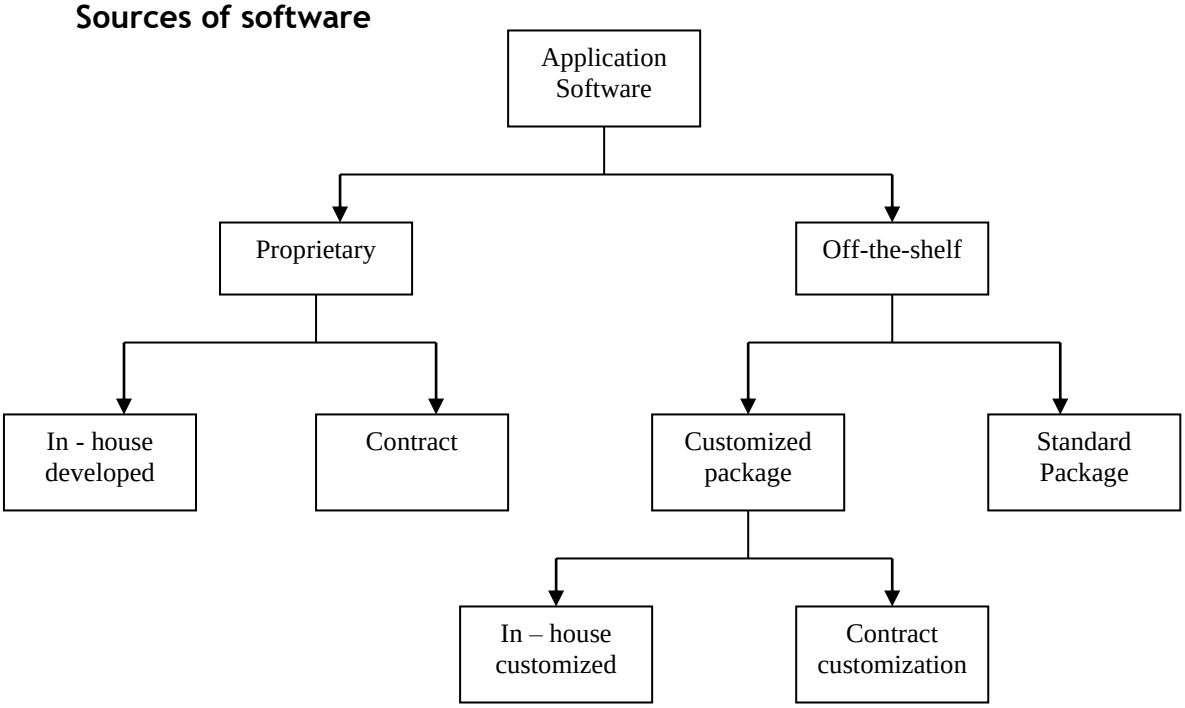
- Perform common hardware functions
  - Accept input and store data on disks and send data to output devices
- Provide a user interface
- Provide hardware independence
- Manage system memory
- Manage processing
- Control access to system resources
  - Protection against unauthorized access
  - Logins and passwords
- Manage 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, XPLinux, Unix, MAC OS, System/7**Application software**

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

Sources of software



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.
- In house 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.

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 organization may have to pay for features that are not required and 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.

General-purpose software

Examples include

- Word processing – Create, edit and print text documents. E.g. MS Word, 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, Quattro Pro.
- Database management systems (DBMS) – Store, manipulate and retrieve data. E.g. Access, FoxPro, dBase.
- Online Information Services – Obtain a broad range of information from commercial services. E.g. America Online, CompuServe
- Communications- Ms Outlook for email
- Browsers e.g Internet Explorer, Eudora
- Graphics – Develop graphs, illustrations and drawings. E.g. PaintShop, FreeHand, Corel
- Project Management – Plan, schedule, allocate and control people and resources needed to complete a project according to schedule. E.g. Project for Windows, 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 programs can also be integrated into published pages. E.g. PageMaker, Publisher.
- Presentation packages like MS PowerPoint

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

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 and ones. 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 it fast in execution of its instructions. Machine language programs directly instructed the computer hardware, so they were not portable. That is, a program 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 program of machine language run very fast because no translation program is required for the CPU.

Disadvantage s

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

Assembly Language (2nd Generation languages)

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

The resulting programs still directly instructed 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 programs 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, programs 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, subtracting etc. A one to one mapping means

that for every assembly instruction there is a 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 program instructions.
- Assembly Language has the same efficiency of execution as the machine level language. Because this is one-to-one translator between assembly language program and its corresponding machine language program.

Disadvantages:

- One of the major disadvantages is that assembly language is machine dependent. A program written for one computer might not run in other computers with 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 compensates for the decrease in speed and efficiency of the resulting programs. Furthermore, programs 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 program instructions, must still 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, while. They are easier to learn but the resulting program 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 that higher-level languages 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 programs 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 or SPSS.

Some fourthgeneration 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 programs that contained procedures to perform operations, such as draw or display, on data elements defined in a file.

Object oriented programs 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, end time, and so on. The time card object would also contain descriptions of such operations as calculate total hours worked or calculate 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 program 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 programs that convert the code originally written by the programmer, called source code, into its equivalent machine language program, called object code.
There are two main types of language translators: interpreters and compilers.

Interpreters

While a program is running, interpreters read, translate, and execute one statement of the program at a time. The interpreter displays any errors immediately on the monitor. Interpreters are very useful for people learning how to program or debugging a program. However, the line-by-line translation

adds significant overhead to the program execution time leading to slow execution.

Compilers

A compiler uses a language translation program that converts the entire source program into object code, known as an object module, at one time. The object module is stored and it is the object module that executes when the program runs. The program 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 material for information is 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 organized 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 a decision. If there were no current or future choices or decisions, 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 usually 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 organizations or individuals prepare has value other than in decision-making. The information may also be prepared for motivation and background building.

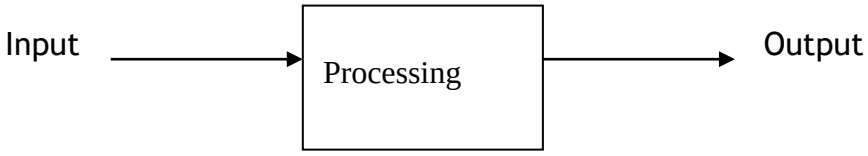
Desirable qualities of information

- Availability – Information should be available and accessible to those who need it.
- Comprehensible – Information 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 – Information should be secure from access by unauthorized users.
- Usefulness – Information 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. In other instances, reliability depends on the source of information.
- Accuracy – Information 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– Information 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, what is described as information. Data processing activities include data collection, classification, sorting, adding, merging, summarizing, 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 any machine takes an input, operates on it and then produces an output.



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 data capture 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. Program 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:

- Record – bring facts into a processing system in usable form
- Classify – data with similar characteristics are placed in the same category, or group.
- Sort – arrangement of data items in a desired sequence
- Calculate – apply arithmetic functions to data
- Summarize – to condense data or to put it in a briefer form
- Compare – perform an evaluation in relation to some known measures
- Communicate – the process of sharing information
- Store – to hold processed data for continuing or later use.
- Retrieve – 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 organized 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 long time period. 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 at first record and read one record after another until end of file or 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 Organization
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 Organization

- 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, 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 organization

- Records are organised in ascending sequence according to a certain key
- Sequential files are accessed sequentially, one record after the next
- 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 requiring 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 organization

- 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, online banking

Problems of traditional file based approach

Each function in an organisation develops specific applications in isolation from other divisions, each application using their 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 filesData isolation — multiple files and formats
- Program-data dependence
    - tight relationship between data files and specific programs used to maintain files

- Lack of flexibility
  - Need to write a new program to carry out each new taskLack of data sharing and availability
- Integrity problems
  - Integrity constraints (e.g. account balance > 0) become part of program code
  - Hard to add new constraints or change existing ones
- Concurrent access by multiple users difficult
  - Concurrent accessed needed for performance
  - Uncontrolled concurrent accesses 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 is related in some manner. It is organized so that relationships within the data are revealed (or revealable). A data file stores several (many) pieces of information about many data objects. The simplest and most efficient metaphor of how data is organized 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 organized collection of (one or more) related data file(s). The way the database organizes 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) & logical (what) aspects of the system
- Physical data independence
  - protects the application programs 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 programs
- 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 user for different types of update to database
- Enforce standards for
    - data representation - useful for migrating data between systems
    - data naming & documentation - aids data sharing & 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 organizing, controlling and using the data needed by application programs. A DBMS provides the facility to create and maintain a well-organized database. It also provides functions such as normalization 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
- ♦ Program and the database
- ♦ Transaction and the database
- ♦ Program and data field
- ♦ User and transaction
- ♦ User and data field

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 – utilizes more resources) – have one copy of the data and avail it to all users and applications
- Maximizes data consistency – users have same view of data even after an update
- Minimizes maintenance cost 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
- Standardizing programming methods

Database structure

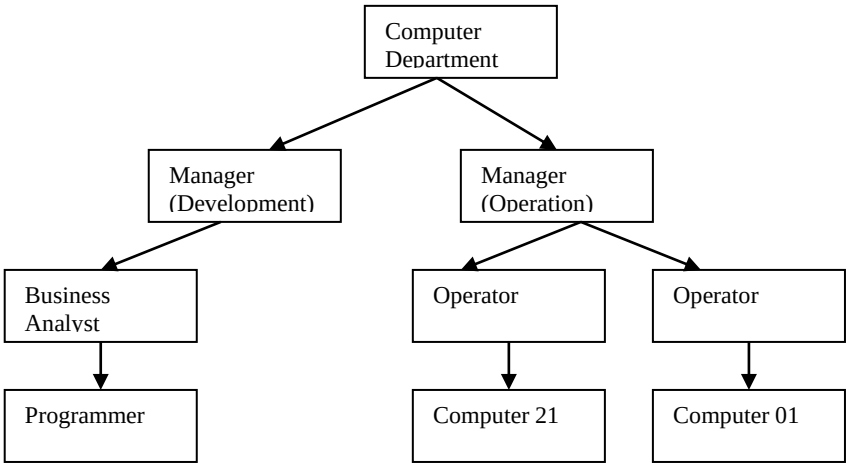
The common database models are:

- 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.

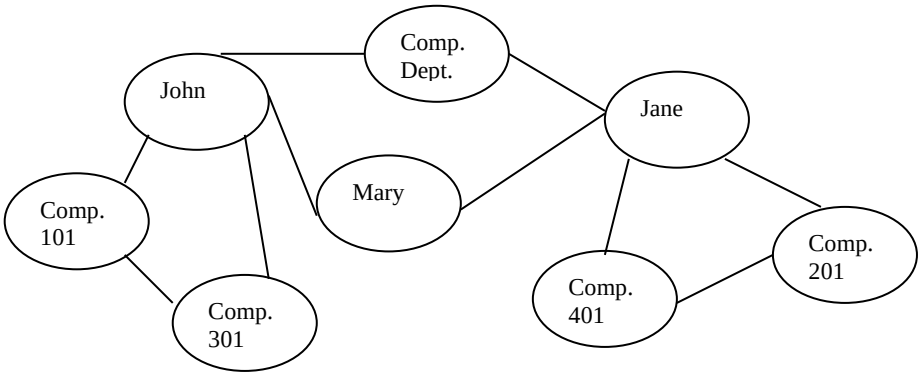
A hierarchical structure has only one root. Each parent can have numerous children, but a child can have only one parent. Subordinate segments are retrieved through the parent segment. Reverse pointers are not allowed. Pointers can be set only for nodes on a lower level; they cannot be set to a node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



Network Database Model

The 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.

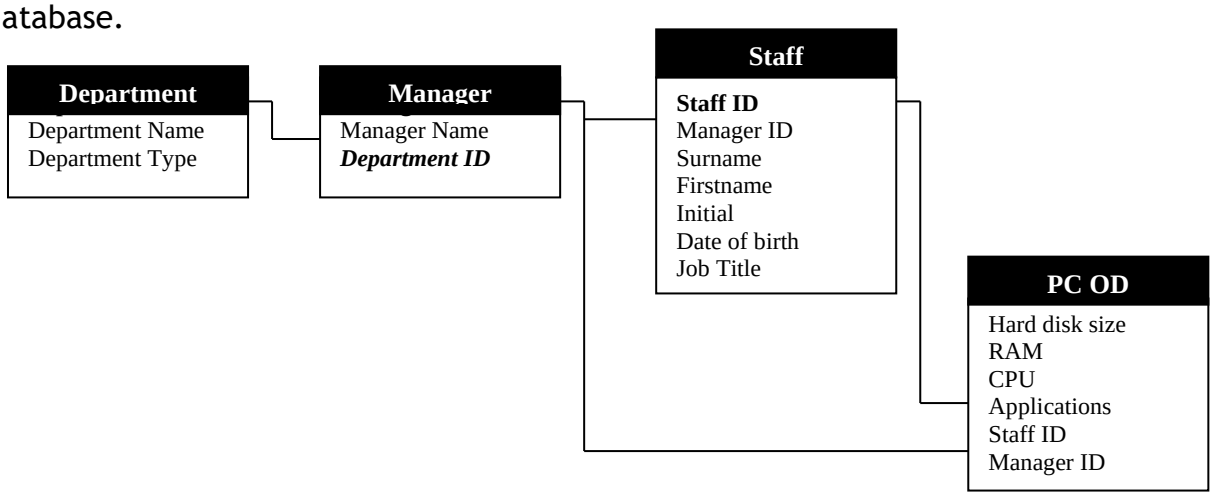


Relational Database Model

The model is independent from the physical implementation of the data structure. The relational database organization 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 minimize the amount of information needed in tables to satisfy users' structured and unstructured queries to the database.



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 unauthorized 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.
- Unauthorized 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 organization

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. Authorization – 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 synchronization 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. Program 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 including
   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 a 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 multidatabase 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.

10. Terminology

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

Multiprocessing

Multiprocessing is the coordinated (simultaneous execution) processing of programs by more than one computer processor. Multiprocessing is a general term that can mean the dynamic assignment of a program to one of two or more computers working in tandem or can involve multiple computers working on the same program 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 program) at a time. The operating system is able to keep track of where you are in these tasks and go from one to the other without losing information. Microsoft Windows 2000, 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 program 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

LESSON FOUR

INFORMATION SYSTEMS

CONTENTS

1. 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 an information system that uses computer technology to perform input, processing and output activities. Due to the massive computerization of manual information systems, computer based information systems are simply referred to as information systems. They are the subject of discussion in this chapter.

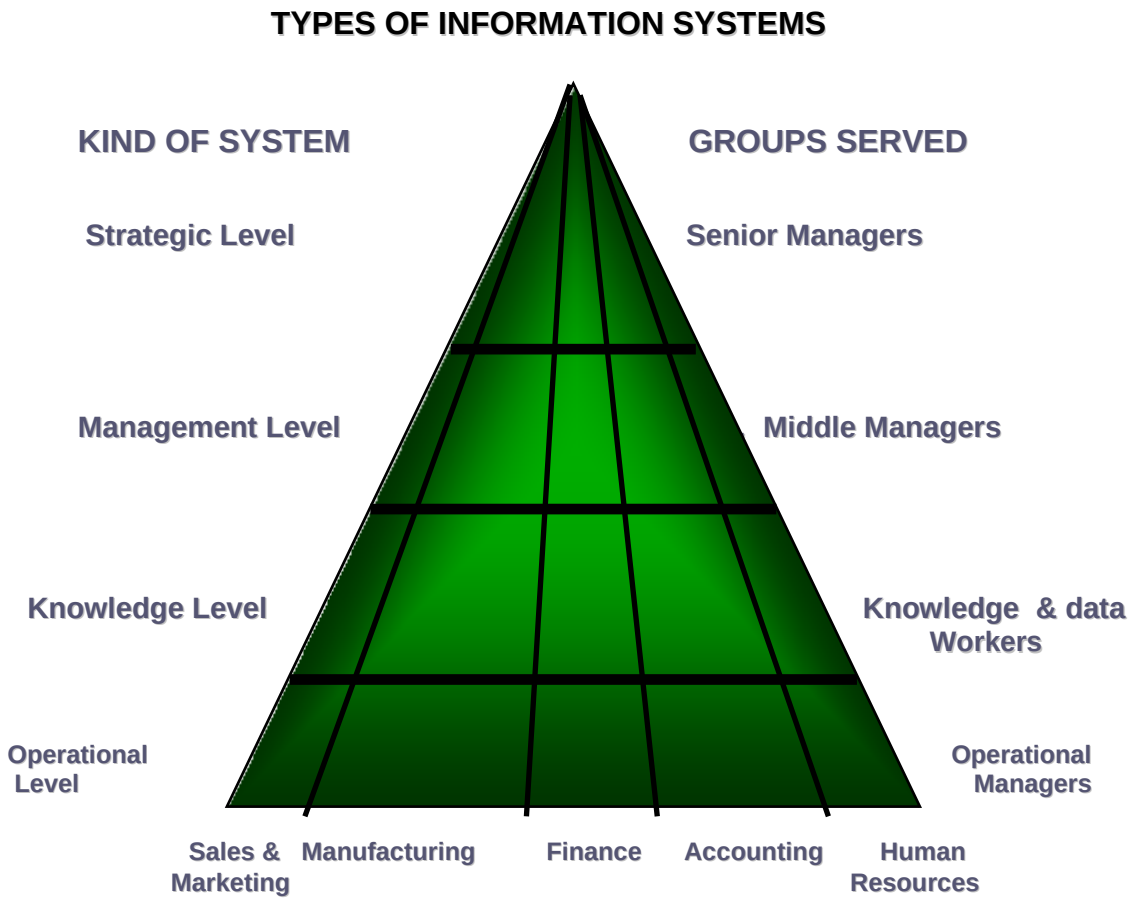
Common examples of information systems include: Automated Teller Machines (ATMs), Point of Sale (POS) terminals used by supermarket checkout clerks,

airline reservation systems or flight schedule systems used by airlines, student registration systems used by colleges etc.

2. Management structure and use of information

Information systems support different types of decisions at different levels of the organizational hierarchy. While operational managers mostly make structured decisions, senior managers deal with unstructured decisions and middle managers are often faced with semi-structured decisions.

For each functional area in the organization, four levels of organizational 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 programs
  - 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 utilized 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 organization 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 organizational 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 – 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 authorized 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 standardized 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

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 organizational 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 systems requirements for support of such decisions are:

- Access to data and various analysis and decision procedures.
- Data retrieval must allow for ad hoc retrieval requests

- Interactive decision support systems with generalized inquiry and analysis capabilities.

Example: Selecting a CEO of a company.

1. 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 organization. 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 organization, 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 organization. Imagine what happens when an airline reservation system fails: all operations stops 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 improve transaction handling by:

- Speeding it up
- Using fewer people
- Improving efficiency and accuracy
- Integrating with other organizational information systems
- Providing information that was not available previously

Examples—Airline reservation systems, Automated Teller Machines (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. A 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. A 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 optimization 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 visualization 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 characterized as one of the types discussed above.

(i) 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.

(ii) 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.

(iii) 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 instantaneous analysed results on huge amounts of financial data and provide access to external databases.

Workflow systems are rule-based programs - (IF 'this happens' THEN 'take this action')- that coordinate and monitor the performance of a set of interrelated tasks in a business process.

(iv) 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.

(v) 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.

(vi) E-Commerce/E-Business Systems

E-Commerce involves business transactions executed electronically between parties. Parties can be companies, consumers, public sector organizations or governments.

(vii) Enterprise Resource Planning (ERP) systems

ERP systems are a set of integrated programs that handle most or all organization's 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.

(viii) 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 organization'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 authorization 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.

(ix) Automated Teller Machine (ATM)

An ATM is a specialized 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 utilize 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 organization 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 org.

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 in house* instead of seeking external resources.

The information technology staff may be categorized 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 organization.
- Liaisons with external parties like auditors and suppliers.
- Setting budgets and deadlines.
- Selecting and promoting IT staff.

Structure of ICT department

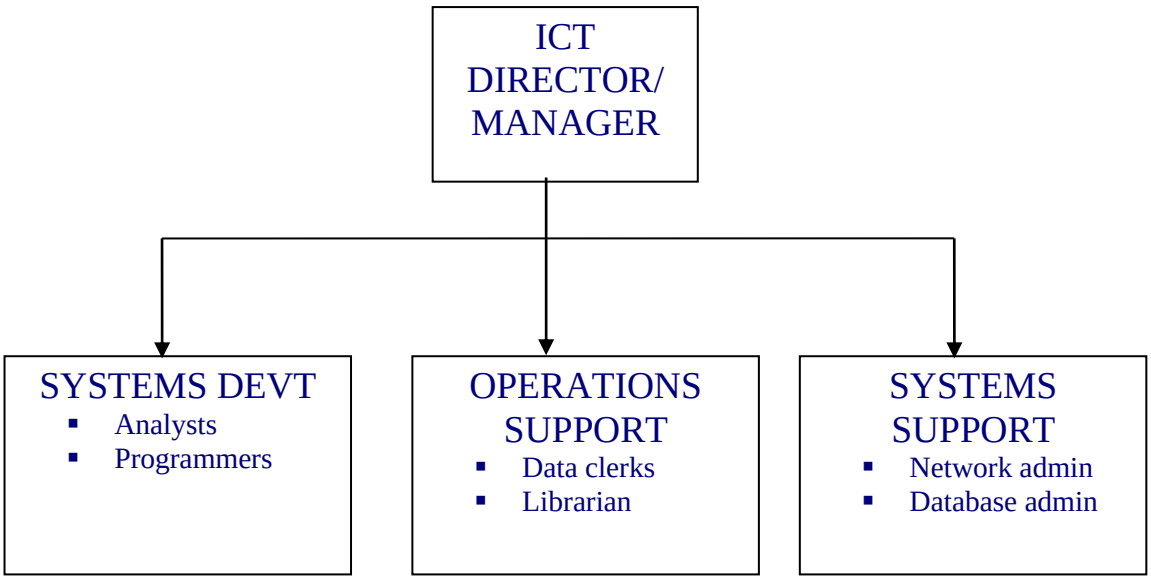
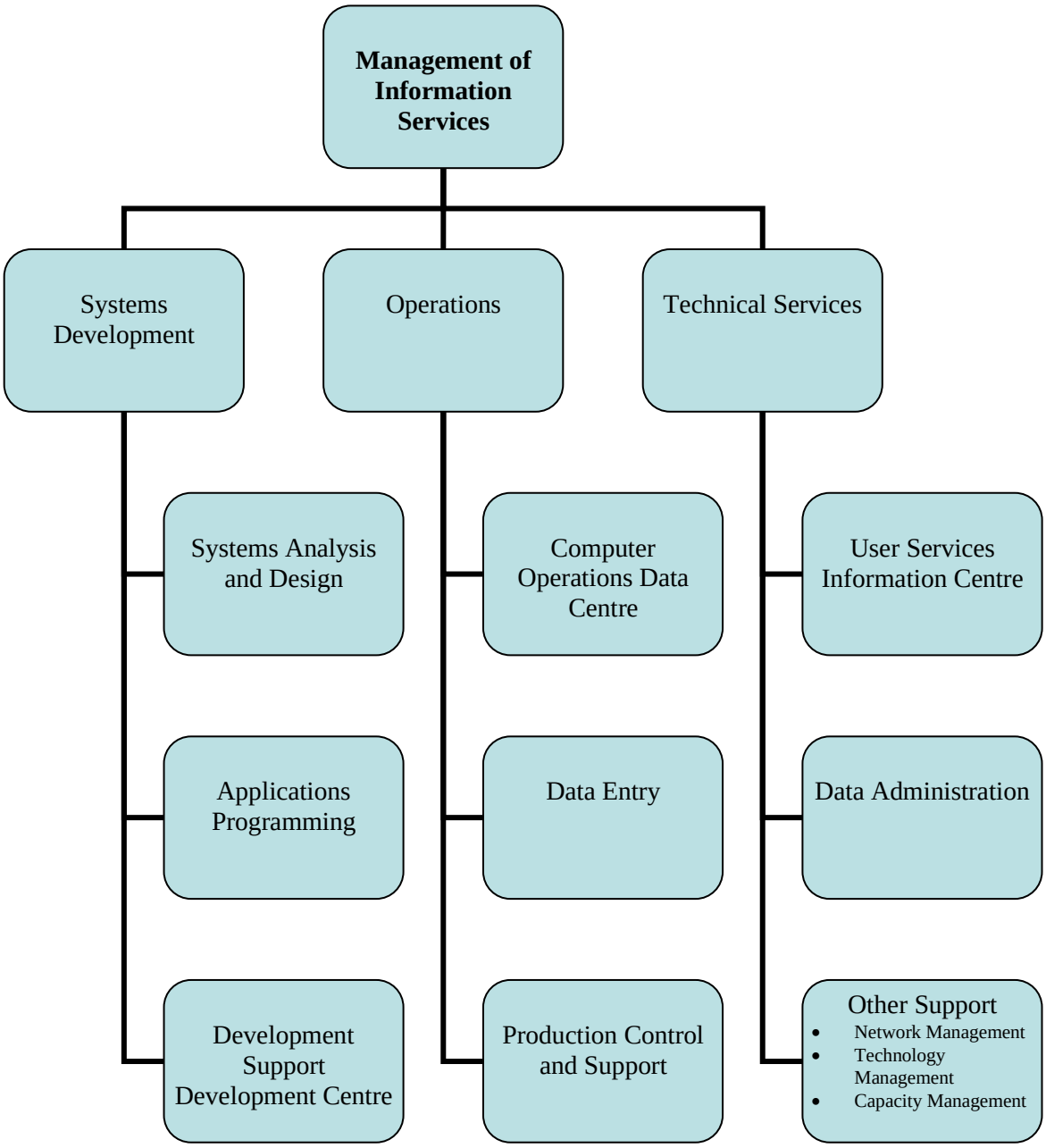


Figure: *Structure of ICT Department in a medium institution*

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 programs.
- Testing programs.
- Maintenance of programs.
- System programmers write and maintain system software. Application programmers write programs or customize 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 does:

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
Controls and operates hardware in the computer room.
Duties include:

- Starting up equipment.
- Running programs.
- Loading peripherals with appropriate media.
- Cleaning and simple maintenance.

Files librarian
Keeps all files organized and up to date. Typical duties are:

- Keeping records of files and their use.
- Issuing files for authorized 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, organization 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

It is important to measure how a system, organization 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.

REINFORCING QUESTIONS

QUESTION ONE

(a) What is an information system? What are the various components of an information system? (6 Marks)

(b) Differentiate between structured and unstructured decisions. Give examples of such decisions. (4 Marks)

(c) Describe the relevance of the following to a Decision Support System (DSS):

(i) Specialized packages (2 Marks)
(ii) Query Languages (2 Marks)
(iii) Database Management System (2 Marks)

(d) Explain what Office Automation System and Knowledge Work System mean. (4 Marks)

(Total: 20 marks)

QUESTION TWO

(a) Propose the type of information system you would recommend for the following applications:

(i) Maintenance of general ledger (1 Mark)
(ii) Formulation of competitive market strategies (1 Mark)
(iii) Financial sensitivity or risk analysis (1 Mark)
(iv) Ticket reservations (1 Mark)

(Question 5c Dec 2002)

(b) Identify the major factors that influence the structure of an information system. (4 Marks)

(Question 5d Dec 2002)

(c) Examine the contribution of information systems in the decision-making or problem solving process. (4 Marks)

(Question 7c May 2002)

(d) Suggest possible uses for an expert system within the Customer Database Department. (6 Marks)

(Question 8b May 2002)

(e) Why do executives need executive information systems? (2 Marks)

(Total: 20 marks)

QUESTION THREE

(a) Organizational information systems are categorized under:

(i) Transaction Processing System (TPS)
(ii) Management Information System (MIS)
(iii) Decision Support System (DSS)
(iv) Executive Information System (EIS)
(v) Expert System (ES)

Required:

Suggest one application of each of the systems types listed above for each of the following areas of business.

- Sales and Marketing (5 Marks)
- Finance (5 Marks)

(Question 1a December 2000)

(b) The general manager of a large organization has asked you to draw up a document identifying eight important characteristics against which managers can evaluate the success of an information system together with a brief explanation of each. What would your document contain? (8 Marks)

(Question 7b December 2000)

(c) What is artificial intelligence? (2 Marks)

(Total: 20 marks)

QUESTION FOUR

(a) Discuss the various components of a Decision Support System. (12 Marks)

(b) When is it appropriate to use a DSS? (8 Marks)

(Total: 20 marks)

QUESTION FIVE

(a) Give a brief definition of an Expert System (ES) (3 Marks)

(b) Describe five properties of an expert system. (10 Marks)

(c) What are the components of an expert system? (7 Marks)

(Total: 20 marks)

CHECK YOUR ANSWERS WITH THOSE GIVEN IN LESSON 9OF THE STUDY PACK

4

Time Allowed: 3 Hours **Attempt any FIVE Questions**

QUESTION ONE

(a) Define fourth-generation languages and list the categories of fourth-generation tools. (10 Marks)

(b) What is the difference between fourth-generation languages and conventional programming languages? (4 Marks)

(c) What is object-oriented programming? How does it differ from conventional software development?
(6 Marks)

(Total: 20 marks)

QUESTION TWO

(a) Discuss the various components of an information system. (5 marks)

(b) Describe the three main levels of decision making within an organization, defining their characteristics and users. Outline the information characteristics for each level. (15 marks)

(Total: 20 marks)

QUESTION THREE

(a) Information systems should be designed and developed to enhance the efficiency and effectiveness of organizational processes. They should therefore be effective and efficient in their use. What factors affect the efficiency and effectiveness of information systems?
(10 Marks)

(b) What is an expert system? Discuss its components and the advantages of using an expert system. (10 Marks)

(Total: 20 marks)

QUESTION FOUR

(a) Briefly define what is a Management Information System. Discuss the various reports output by an MIS. (10 Marks)

(b) Define office automation. What are the objectives of office automation?
(10 marks)

(Total: 20 marks)

QUESTION FIVE

(a) List the characteristics of a good software design. (4 Marks)

(b) Differentiate between white box testing and black box testing.
(4 Marks)

(c) Describe Joint Application Development and show its usefulness in software development. (6 Marks)

(d) Briefly describe three areas of feasibility study. (6 Marks)

(Total: 20 marks)

QUESTION SIX

(a) Define CASE and show how it improves productivity in the software development environment. (6 Marks)

(b) Discuss the advantages and disadvantages of the traditional system development life cycle (waterfall model). (6 Marks)

(c) Define prototyping and list various advantages and disadvantages of prototyping. (8 Marks)

(Total: 20 marks)

QUESTION SEVEN

(a) Differentiate between formal and informal information systems. (4 Marks)

(b) Once the system has been constructed and tested the system needs to be delivered to the users and made operational. Briefly describe four activities done during the implementation of a system. (8 Marks)

(c) The user interface is becoming more important as systems become more and more interactive. Discuss four principles of good user interface design. (8 Marks)

(Total: 20 marks)

QUESTION EIGHT

(a) Identify five reasons that contribute to late completion and delivery of software. (5 Marks)

(b) Name five factors that are to be considered when acquiring hardware. (5 Marks)

(c) List five factors that should be considered when selecting a hardware supplier. (5 Marks)

(d) List five tools and techniques used in the documentation design of a system. (5 Marks)

(Total: 20 marks)

END OF COMPREHENSIVE ASSIGNMENT No.2
NOW SEND YOUR ANSWERS TO THE DISTANCE LEARNING CENTRE FOR MARKING

APPLICATION OF INFORMATION TECHNOLOGY

CONTENTS

1. 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 organization. IT basically represents the modern merger of computer technology with telecommunications technology.

The business environment is changing and as a result organizations 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 organizations. 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. Organizations 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 organization; 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 organization
- Mostly for predefined, structured tasks
- Can have strategic consequences (e.g. airline reservation system)
- Most have high volumes of input and output
- Summarized 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:

- Organizational 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 computerized.

5.1 OPERATIONAL-LEVEL ACCOUNTING IS

Operational accounting information systems produce the routine, repetitive information outputs that every organization finds necessary, including pay cheques, cheques to vendors, customer invoices, purchase orders, stock reports, and other regular forms and reports.

The heart of an organization'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 computerized 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, provides managers with

- Periodic accounting reports and statements, such as income statement and balance sheet
- Support for budgeting
- Creation of general ledger accounts and definition of the organization'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 the other long-term assets an organization 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 organization. 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 organization'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 organization

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
- 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 federal, 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 organization. By computerizing these operational-level systems, organization 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 organization 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 computerized 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 are prepared.

Cash Management Systems
Cash Management Systems help managers

- Ensure that the organization 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 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 organization's investments in

- Stocks
- Bonds
- Other securities

Whatever their source of investment funds, most organizations invest money in securities of one kind or another. Careful management of these investments is necessary to ensure the achievement of organizational goals.

5.3 STRATEGIC ACCOUNTING AND FINANCIAL IS

Strategic-level Information Systems are goal oriented and are designed to support organization 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 organization (new investment opportunities or the mix of capital sources used to fund the organization)

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 organization and makes it possible to explore ways of improving the organization's financial condition.

Long-Range Forecasting Systems
Long-Range Forecasting Systems provide forecasts on a variety of factors that will affect organization 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 organization 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 mangers 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. Specialized 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 template, 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 organization

In addition, many computerized 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 COMPUTERIZED AUDITING SOFTWARE

A number of computerized auditing programs are available to assist auditors when they evaluate or monitor a computerized accounting system. Generalized audit software :

- Provides access to the computer files
- Lets EDP auditors create audit files
- Extract data
- Analyse data statistically
- Sorts, summarizes, 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 specialized software products assist the financial manager in developing and analysing the capital budgeting needs of the organization. Others assist the investment manager in monitoring and analysing the organization's investment portfolio. The financial manager can use specialized software products to help manage the cash flow of the organization.

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 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 ancillary 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 summarize.

Telemarketing Systems
Use of the telephone to sell products and services, or telemarketing systems, has become a common and important means by which organizations 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 reach many more customers in a given time period than they could have through other means.

Direct-Mail Advertising Systems
Many organizations 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 organizations.

Inquiry Information Systems
Inquiry Information Systems record, process and store the inquires when customers inquire about the products and services the organization offers. It is important to compile information about the actual or potential customer 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 organization 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 organization can deliver its products is an important customer service.
If the organization 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 utilize 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 mangers 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

Product pricing Information Systems 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 organization, 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 organization 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 organization
- 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), specialized marketing software can be classified into five categories. That which will:

1. Help salespeople sell the organization's products and services
2. Help sales managers manage sales personnel
3. Help manage the telemarketing program
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 supports for salespeople. Document support features may include:

- A package of form letters 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
- To compare salesperson performance by product and customer type
- To compare salesperson performance against salesperson goals
- To analyse salesperson calls within territories or by customer type
- To identify trends in customer purchase
- To identify potential shortages or excess stock in inventory
- To perform other planning, controlling, and organizing 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
Customer Support Software provides information to salespeople about the previous experiences of customers with the organization 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 analyze 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
Integrated Marketing Software combines programs 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 organization by drawing on data not only from salespeople but also from the organization'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 organization. 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, or MRP.

Just-in-Time Systems
The just-in-Time (JIT) system is not a tactical information system, but a tactical approach to production. The just-in-time approach was created by the Toyota Motor Company of Japan and has generated many advantages to organizations, 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 assure 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 categorized 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 computerized 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 programs 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 programs are available that aid the engineer in choosing materials for the product under design. These programs are called materials selection programs, 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 organizational 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, or 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

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 its 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 check 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 program, 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.

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 organization's positions and employees and about governmental regulations.

Employee Information Systems

The human resource department must maintain information on each of the organization's employees for a variety of decision 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 organization-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 organization, 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 applicant selection and placement information system is to assist human resource staff in these tasks.

Performance Management Information Systems

Performance Management Information Systems include performance appraisal data and productivity information data. Performance management information systems 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 emphasize 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 labor unions, competitors, and government from sources external to the firm, such as labor 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 organization 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 organization's productivity. Tying employee productivity to pay or encouraging increased productivity with incentive pay plans can often improve an organization'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 organization 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

Organization 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 analyze the organization'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 labor negotiations.

Specialized 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 organize the various human resource information systems into integrated software referred to as human resource information systems, or HRIS, software.

In general, the computerization 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 programs 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 program 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 programs designed by human resource department for training specific employees in-group and independent study programs. 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.

10. Important definitions

- **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.

REINFORCING QUESTIONS

QUESTION ONE

(a) Briefly describe Computer Integrated Manufacturing (CIM). (3 Marks)
(b) What are the goals and benefits of CIM? (8 Marks)
(c) Discuss three techniques used to support CIM. (9 Marks)
(Total: 20 marks)

QUESTION TWO

(a) Define Enterprise Resource Planning (ERP) systems and what are its various components and functions in an organization. (4 Marks)
(b) Which organizational level do the following systems support?

(i) Machine control
(ii) Pricing analysis
(iii) Sales trend
(iv) Production Planning
(v) Accounts receivable
(vi) Compensation analysis

(6 Marks)
(c) Describe how information systems facilitate supply chain management.
(6 Marks)
(d) Name the major components of supply chain management systems. (4 Marks)
(Total: 20 marks)

QUESTION THREE

Discuss five types of information systems to support the operational level of human resource management. **(Total: 20 marks)**

QUESTION FOUR

Discuss five types of information systems to support the tactical level of manufacturing and production management. **(Total: 20 marks)**

QUESTION FIVE

(a) Define telemarketing software and discuss its impact in the sales and marketing functions of an organization. (6 Marks)
(b) What is customer relationship management and what are its goals in an organization.
(4 Marks)
(c) Discuss the various advantages and disadvantages of online banking.
(10 Marks)
(Total: 20 marks)

CHECK YOUR ANSWERS WITH THOSE GIVEN IN LESSON 9OF THE STUDY PACK

COMPUTER SECURITY ISSUES

CONTENTS

1. Definition of computer security – threats, hazards and controls
   1.1. Security goals
   1.2. Hazards (exposures) to information security
   1.3. Threats to information security
   1.4. Vulnerability
   1.5. Security controls
   1.6. Administering security
2. Security in the application level: Application controls
   2.1. Input/origination controls
   2.2. Processing validation and editing
   2.3. Output controls
   2.4. Data integrity testing
3. Security in operating system: Access control function
   3.1. Identification
   3.2. Authentication
   3.3. Authorization
4. Logical security
   4.1. Logical access issues and exposures
   4.2. Access control software
   4.3. Logical security features, tools and procedures
5. Physical security
   5.1. Physical access exposures
   5.2. Physical access controls
6. Personnel issues
7. Network security
   7.1. LAN security
   7.2. Dial up access controls
   7.3. Client/server security
   7.4. Internet threats
   7.5. Encryption
   7.6. Firewall security
   7.7. Intrusion detection systems (IDS)
8. Environmental exposures and controls
9. Computer ethics
10. Terminology

1. Definition of computer security - threats, hazards and controls

Information is a strategic resource and a significant portion of organizational 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 unauthorized access, unauthorized disclosure and interference of information.

Assets can be categorized 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 organizations 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 unauthorized 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 authorization. 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:

- Unauthorized access resulting in a loss of computing time
- Unauthorized disclosure – information revealed without authorization
- 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 programs that have threats (erroneous programs) 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 by an organization to ensure that users only do that which they have been authorized 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 organizes the security activities of an organization.
- 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 organization 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 computerized information should be based on a documented 'need-to-know, need-to-do' basis.

- Compliance with relevant legislation and regulations
- Access authorization – the data owner or manager responsible for the accurate use and reporting of the information should provide written authorization for users to gain access to computerized information.
- Reviews of access authorization – 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 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

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 authorized 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 authorization

Input authorization verifies that all transactions have been authorized and approved by management. Authorization of input helps ensure that only authorized data is entered into the computer system for processing by applications. Authorization 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

authorized data remains unchanged. This can be accomplished through various accuracy and completeness checks incorporated into an application's design.

Types of authorization include:

- Signatures on batch forms provide evidence of proper authorization
- Online access controls ensure that only authorized individuals may access data or perform sensitive functions
- Unique passwords are necessary to ensure that access authorization cannot be compromised through use of another individual's authorized 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, 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 recognized 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, greatly impact the completeness and accuracy of the data. Corrections to data should be processed through the normal data conversion process and should be verified, authorized 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 error 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 program 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 program 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 computerized table that matches the code to a city name.
- Existence check – data is entered correctly and agree 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 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, is 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 sixteen 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 program instruction or subroutine that tests for accurate, complete and valid input and updates in an application.
- Run-to-run totals – run-to-run 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 program could display messages instructing that the proper file and version be used.
- Reasonableness verification of calculated amounts – application programs 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 program 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 authorized 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 authorized 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 authorized 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 unauthorized 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 unauthorized 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 authorization – proper authorization for file updating and maintenance is necessary to ensure that stored data are adequately safeguarded, correct and up-to-date. Application programs 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 programs 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 authorized 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 unauthorized 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 authorization.

- Balancing and reconciling – data processing application program 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 program 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 authorization 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 authorized 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. Computerized 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 programs, 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 authorized accesses are allowed, e.g.

- Protect the system from access by intruders

- Protect system resources from unauthorized 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 categorized into identification, authentication and authorization 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 program from interfering with another i.e. any form of unauthorized access to another program's memory space.

3.1 Identification

Involves establishing identity of the subject (who are you?). Identification can use:

- ID, 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 Authorization

Involves determining the access rights to various system objects/resources. The security requirement to be addressed is the protection against unauthorized access to system resources. There is need to define an authorization policy as well as implementation mechanisms. An authorization policy defines activities permitted or prohibited within the system. Authorization mechanisms implement the authorization 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 authorized 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 authorization 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 organization'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 unauthorized alteration and manipulation of data and programs. Exposures that exist from accidental or intentional exploitation of logical access control weaknesses include technical exposures and computer crime.

Technical exposures

This is the unauthorized (intentional or unauthorized) 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 program. This hidden code will be executed whenever the authorized program is executed. A classic example is the Trojan horse in the payroll-calculating program 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 computerized 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 unauthorized account. Since the amounts are so small, they are rarely noticed.
4. **Salami techniques** involve the slicing of small amounts of money from a computerized transaction or account and are similar to the rounding down technique. The difference between them is that in rounding down the program 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 program.
5. **Viruses** are malicious program 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 programs that may destroy data or utilize tremendous computer and communication resources but do not replicate like viruses. Such programs 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 specialized 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 authorized program that allow insertion of specific logic, such as program interrupts, to permit a review of data during processing. These holes also permit insertion of unauthorized 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 authorized person through a secured door or electronically attaching to an authorized 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.

Viruses

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 programs. 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 program 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 program can be used to wipe the virus from the hard disk. Sometimes eradication programs can kill the virus without having to delete the infected program or data file, while other times those infected files must be deleted. Still other programs, sometimes called inoculators, will not allow a program 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 programs. 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 program 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 program that is then stored in a database file. The number is called a cyclical redundancy check or CRC. When that program is called to execute, the checker computes the CRC on the program 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 program has occurred. A change in the program could mean a virus within it. Integrity checkers take advantage of the fact that executable programs and boot sectors do not change very often, if at all.

Computer crime exposures

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 unauthorized 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 computerized 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 organization. Loss of customers, embarrassment to management and legal actions against the organization 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 organization should consider when developing security policies and procedures. These laws can protect the organization but can also protect the perpetrator from prosecution. In addition, not having proper security measures could expose the organization 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 organizations, 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 organization by threatening to exploit the security breach.

- **Disclosure of confidential, sensitive or embarrassing information** - such events can damage an organization'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 organization 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 authorized and unauthorized employees
c) Information system personnel – these individuals have the easiest access to computerized 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
    - Organized 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 unauthorized access to data, use of system functions and programs, unauthorized 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
- Authorization of access to defined resources
- Restriction of users to specific terminals
- Reports on unauthorized attempts to access computer resources, data or programs

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 clam 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 the following information:
    - Remembered information such as name, account number and password
    - Processor 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 computerized information, transactions, programs 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 authorization.

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 organizations 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 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 computerized 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 authorized 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 memorized 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 utilized 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 you 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 the 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 assure the integrity of the information, by protecting it from unauthorized 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 organization. Its unauthorized disclosure could seriously and adversely impact the organization's image in the eyes of the public e.g. application program source code, project documentation etc.
- Private – applies to personal information that is intended for use within the organization. Its unauthorized 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 authorized 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 unauthorized 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 program 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, programs 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 unauthorized 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:

- Unauthorized 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 authorized or unauthorized access who are:
  - Disgruntled (upset by or concerned about some action by the organization 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, organized 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 organization from unauthorized access. They reduce exposure to theft or destruction of data and hardware. These controls should limit access to only those individuals authorized by management. This authorization may be explicit, as in a door lock for which management has authorized 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 unauthorized 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 unauthorized 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 utilized 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 organization 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 organization.

- **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 unauthorized person follows an authorized 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 unauthorized 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 organization'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 programs and files supporting the network operations. Control is accomplished through a network control terminal and specialized 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 unauthorized 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 unauthorized 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, NetPass etc.

7.1 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 program integrity through unauthorized 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 programs, 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 minimize 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 authorized 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 utilize 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, centralized 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 unauthorized access. By securing the automatic boot or start up batch files, unauthorized 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 programs and the organization 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 organizations 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.
- Unauthorized 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, unauthorized and unapproved changes to systems or data.
- Unauthorized 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) Unauthorized 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, unauthorized 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 generic 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 unauthorized interception and manipulation
- Protect information stored on computers from unauthorized 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 organization'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 organizations 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 organization by creating a virtual private network over the Internet.

Problems faced by organizations 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 i.e. it will detect 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 programs, 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 localize 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 pressurized 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 pressurized 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 on 3rd, 4th, 5th or 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 unauthorized 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 organization, 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 emphasize human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation, 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 jeopardized through faulty computing systems and/or unethical behaviour by computing professionals
  - Computing systems can change the way people work: it can be 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: minimize 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 programs 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 authorization. Unauthorized 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 civilization. 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 authorized 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 become 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 authorized to do so

- **Organizational leadership imperatives**

  - Articulate social responsibilities of members of an organizational 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 authorized uses of an organization'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 organization 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 organizations 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

.

REVISION QUESTIONS

QUESTION ONE

(a) Information security management is about viewing and managing risks in terms of the causes, effects and therefore costs of loss of security.

Required:

Identify and briefly describe the stages involved in systematic management of information systems. (8 Marks)

(Question 1b December 2002)

(b) Identify six threats to Internet security and briefly describe solutions to these threats.

(12 Marks)

(Total: 20 marks)

QUESTION TWO

(a) What is intrusion detection? List the main intrusion detection functions.(8 Marks)

(b) Define a security system and briefly explain the main security goals. (8 Marks)

(c) List four examples of sources of threats to system security. (4 Marks)

(Total: 20 marks)

QUESTION THREE

(a) Briefly discuss three security goals. (6 Marks)

(b) List examples of threats to information security. (6 Marks)

(c) Identify key components of a security policy. (8 Marks)

(Total: 20 marks)

QUESTION FOUR

(a) Define the following data validation edits:

(i) Sequence checks (3 Marks)

(ii) Limit checks (3 Marks)

(iii) Range checks (3 Marks)

(iv) Validity checks (3 Marks)

(b) Define the following terms:

(i) Data diddling (2 Marks)

(ii) Rounding down (2 Marks)

(iii) Salami technique (2 Marks)

(iv) Piggybacking (2 Marks)

(Total: 20 marks)

QUESTION FIVE

(a) Identify the various policies and procedures that can be adopted to control spread of viruses. (6 Marks)

(b) Name six threats to a business as a result of computer crime. (6 Marks)

(c) Access control software is designed to prevent unauthorized access to data, use of system functions and programs, unauthorized updates/changes to data and to detect or prevent an unauthorized attempt to access computer resources. Identify the tasks performed by access control software. (4 Marks)

(d) Passwords are the most common security mechanisms. What format rules are usually prescribed for passwords to make them a strong security mechanism? (4 Marks)

(Total: 20 marks)

CHECK YOUR ANSWERS WITH THOSE GIVEN IN LESSON 9 OF THE STUDY PACK

COMPREHENSIVE ASSIGNMENT NO.3

.

Time Allowed: 3 Hours **Attempt any FIVE questions**

QUESTION ONE

The rapidly increasing connectivity and use of the Internet has introduced security threats and exposures to many organizations, and therefore the need to have security measures to safeguard against such exposures. One of the major Internet threat to an organization is the presence of hackers.

Required:

(a) Define the terms exposures, threats and vulnerability giving an example of each.
(6 Marks)

(b) What is meant by the term hacking? Identify four exposures that can be caused by hackers. (8 Marks)

(c) Describe three major factors that vulnerability of a system to hacking will depend on.
(6 marks)

(Total: 20 marks)

QUESTION TWO

(a) Distinguish an active attack from a passive attack to security. (4 Marks)

(b) Briefly describe the following systems:

(i) CAD/CAM (4 Marks)
(ii) Image Management Software (4 Marks)
(iii) Automated Materials Handling Software (4 Marks)
(iv) CIM (4 Marks)

(Total: 20 marks)

QUESTION THREE

(a) A trap door is a secret and undocumented entry point within a program which typically bypasses normal methods of authentication, and usually included for debugging purposes but may be forgotten or left deliberately. Trap doors can also be inserted by intruders who have gained access. Suggest four counter measures of controlling trap doors. (8 Marks)

(b) Identify six types of operational information systems in a bank. (6 Marks)

(c) Briefly describe three advantages of implementing an online banking system. (6 Marks)

(Total: 20 marks)

QUESTION FOUR

(a) Discuss four processing control procedures. (8 Marks)

(b) Define authentication. Using examples, identify five forms of personal authentication.
(12 Marks)

(Total: 20 marks)

QUESTION FIVE

(a) Define the following terms:

(i) Virus (3 Marks)
(ii) Worm (3 Marks)
(iii) Logic bomb (3 Marks)
(iv) Denial of service (3 Marks)

(b) Identify four hardware tactics of controlling viruses in an organization. (8 Marks)

QUESTION SIX

(a) Name five business threats experienced as a result of computer crime exposures. (10 Marks)

(b) Identify four aspects of risk management as relates to protection of data and resources in an enterprise. (8 Marks)

(c) Suggest two operational level systems that can be implemented by an airline. (2 Marks)

(Total: 20 marks)

QUESTION SEVEN

(a) What is access control software? Discuss its various functions. (8 Marks)
(b) Identify five syntax/format rules required of a strong password. (5 Marks)
(c) What is a smart card? (3 Marks)
(d) Define a digital signature. (4 Marks)

(Total: 20 marks)

QUESTION EIGHT

(a) List ten controls over environmental exposures. (10 Marks)
(b) Define intrusion detection system. (4 Marks)
(c) What is a firewall and what functions does it perform in relation to organizational network security. (6 Marks)

(Total: 20 marks)

DATA COMMUNICATION & COMPUTER NETWORKS

CONTENTS

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
- Fiber-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 is now replacing it.

Coaxial cable

Coaxial cable 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.

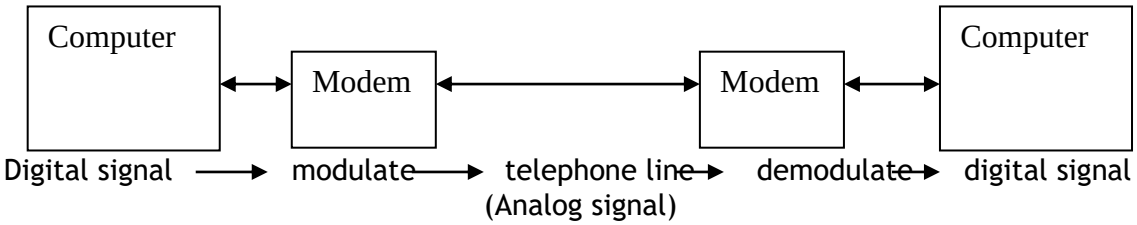
Satellite
Satellites are used to amplify and relay microwave signals from one transmitter on the ground to another. They orbit about 22,000 miles above the earth. They rotate at a precise point and speed and can be used to send large volumes of data. Bad weather can sometimes interrupt the flow of data 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 quantized to given levels: this adds an error called quantization error. The larger the number of bits used to represent each sample, the smaller the quantization error.

2.1 Modem
A modem is a hardware device that converts computer signals (digital signals) to telephone signals (analog signals) and telephone signals (analog signals) back to computer signals (digital signals).
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 synchronized clock to enable transmission at timed intervals.

Protocols
Protocols are sets of communication rules for exchange of information. Protocols define speeds and modes for connecting one computer with another computer. 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 Organization. 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 specialized 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 each other.

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 decentralized organizations (each office has its own computer system but is networked to the main computer).
- Host computer – a large centralized 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 fiber-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 bus organization 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 expand 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
- Specialized 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

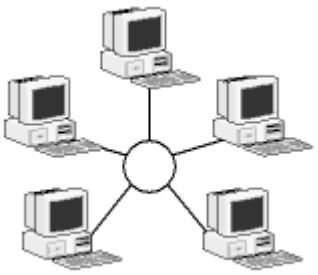
In a star network there are a number of small computers or peripheral devices linked to a central unit called a main hub. The central unit may be a host computer or a file server. All communications pass through the central unit and control is maintained by polling. This type of network can be used to 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

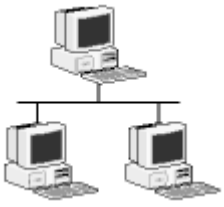
In a bus network each device handles its communications control. There is no host computer; however there may be a file server. All communications travel along a common connecting cable called a bus. It is a common arrangement for sharing data stored on different microcomputers. It is not as efficient 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

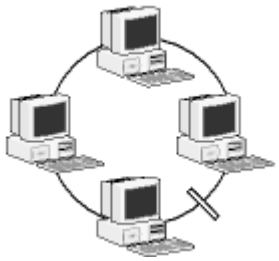
Disadvantages:

- Heavy network traffic can also slow 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 decentralized organization 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

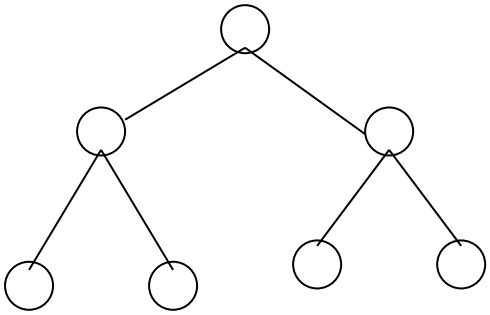
A hierarchical network consists of several computers linked to a central host computer. It is similar to a star. Other computers are also hosts to other, smaller computers or to peripheral devices in this type of network. It allows various computers to share databases, processing power, and different output devices. It is useful in centralized organizations.

Advantages:

- Improves sharing of data and programs 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

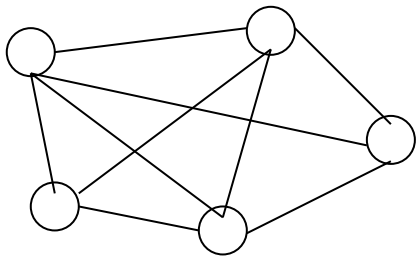
Is a network topology in which devices are connected with many redundant interconnections between network nodes.

Advantages:

- Yields the greatest amount of redundancy (multiple connections between same nodes) in the event that one of the nodes fail 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 sub tasks. 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) 3 layer logical model
(ii) TCP/IP (Transmission Control Protocol/Internet Protocol)
(iii) ISO/OSI model (International Organizations 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)

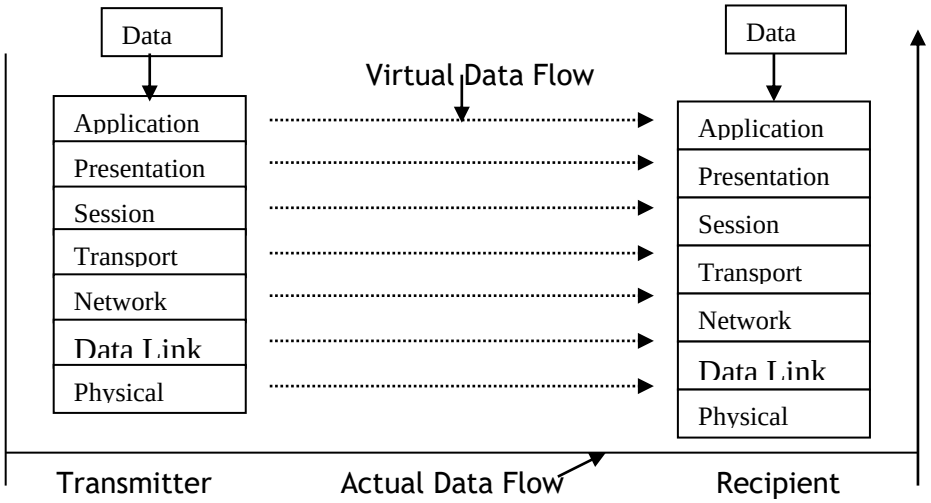
- **Application Layer**
  - User application protocols
- **Transport Layer**
  - Transmission control protocol
  - Data reliability and sequencing
- **Internet Layer**
  - Internet Protocol

- 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 Organization/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 Organization (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 programs such as file transfer and electronic mail. It offers user level interaction with network programs 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 packetization, error control, flow control, and synchronization. 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, synchronization, 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; they are 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 organization. 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 organizations develop different standards for the same functions.

3.9 Application of computer networks within an organization

Connectivity is the ability and means to connect 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 organizations 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

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 checks, 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 for 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 for 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 organizations 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 programs 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 organized by major categories e.g. Health, entertainment, education etc
- Each category is further organized 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 organized like a database
- Key words and phrases can be used to search through a database
- Databases are maintained by special programs called agents, spiders or bots
- Widely used search engines are Google, HotBot and AltaVista.

Web utilities

Web utilities are programs 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 for a nominal charge. There are two categories of web utilities:

- Plug-ins
- Helper applications

Plug-ins

- A plug-in is a program 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 and helper applications. They are independent programs 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 program that automatically connects you to selected websites. They download HTML documents and saves 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 programs. 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 programs that allow parents or organizations 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 organized into major topic areas. Newsgroup organization 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 program to use this type of communication. Two widely used e-mail programs 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 program

(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 organization
(iii) Domain code – identifies the geographical or organizational 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 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 messages is sent to the mailing list rather than the originator).
- It may be difficult to send to some remote sites. Many organizations 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.

Organizational Internets: Intranets and Extranets
An organization 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 organization's local network.

For these reasons, many organizations have shied away from connection to the global network and have set-up intranets and extranets.

An organizational Internet is the application of Internet technologies within a business network. It is used to connect employees to each other and to other organizations. There are two types of technologies used in organizational Internets:

- Intranets – a private network within an organization
- Extranets – a private network that connects more than one organization

Firewalls are often used to protect organizational Internets from external threats.

Intranets
Intranets are in-house, tailor-made networks for use within the organization 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 organization's intranet.

Organizations 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

Groupware packages normally replicate data locally on a computer whereas Intranets centralize 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 organizations, such as suppliers, limited access to the organization'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 organizational networks. It protects a network against intrusion from outside sources. They may be categorized 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 minimize 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 fiber 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**

Closed circuit television (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.

- **VSAT**

VSAT (Very Small Aperture Terminal) 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 antenna 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.

REVISION QUESTIONS

QUESTION ONE

(a) There are three main types of network topologies namely; star, ring and bus. As a network administrator, you have been asked to produce a briefing document that discusses each topology in terms of cabling cost, fault tolerance, data redundancy and performance as the number of nodes increases. (12 Marks)

(Question 1a December 2002)

(b) There is a global trend towards adopting digital communication as opposed to analogue systems. Analogue data has therefore to be converted to digital data in a process known as digitisation. Why is it advantageous to digitise data? (8 Marks)

(Total: 20 marks)

QUESTION TWO

(a) (i) Describe how fiber optic systems are used in communications systems. (5 Marks)

(ii) Why has the use of fiber optic systems become popular in the recent past? (6 Marks)

(b) Define the following terms:

(i) Attenuation (3 Marks)
(ii) Delay distortion (3 Marks)
(iii) Noise (3 Marks)

(Total: 20 marks)

QUESTION THREE

(a) Identify the seven layers of the ISO/OSI reference model. (7 Marks)
(b) Identify the main components of a Local Area Network (LAN) (5 Marks)
(c) (i) What is middleware (4 Marks)
(ii) Explain the following Internet address: http.africaninstitute.com (4 Marks)

(Total: 20 marks)

QUESTION FOUR

(a) Differentiate between:

(i) Serial transmission and parallel transmission (4 Marks)
(ii) Half-duplex and full-duplex communication (4 Marks)
(iii) Asynchronous and synchronous transmission (4 Marks)

(b) Briefly define a star network and discuss its advantages and disadvantages. (8 Marks)

(Total: 20 marks)

QUESTION FIVE

(a) What is a network protocol? (3 Marks)
(b) Briefly describe the main components of a protocol. (6 Marks)
(c) Discuss the various benefits derived form the use of network protocols. (8 Marks)
(d) List three examples of network protocols. (3 Marks)

(Total: 20 marks)

CHECK YOUR ANSWERS WITH THOSE GIVEN IN LESSON 9 OF THE STUDY PACK

CURRENT TRENDS IN INFORMATION TECHNOLOGY

CONTENTS

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

Web storefronts 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 program 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

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) Checks

- After an item is purchased on the Internet, a check 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 specialize 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 specializes 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

2. Electronic Data Interchange (EDI)

EDI is an electronic means for transmitting business transactions between organizations. 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 organizations 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 organization hands over control of part or all of the functions of the information systems department to an external party. The organization 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 organizations.

The specific objective for IT outsourcing vary from organization to organization. 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 organization 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
- Utilization of multiple suppliers or withhold a piece of business as an incentive
- Formalization of a cross-functional contract management team
- Contract performance metrics
- Periodic competitive reviews and benchmarking/benchtrending
- 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 bureaus 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 organizations 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 specialize 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 organize around subjects, as opposed to traditional application systems which organize 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.

7. Data Mining

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 organizations 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
- Visualize 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 personalization – personalized services to large numbers of customers
- Fraud detection – using predictive models, an organization 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 has 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 deals 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. Kinds of computer fraud includes:

(i) Input fraud – entry of unauthorized 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) Program fraud – creating or altering a program 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 – unauthorized 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

Possible to corrupt/erase data without apparently causing any physical damage. In England the Criminal Damage Act 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 unauthorized access to computer programs and data. This was not criminal in England prior to 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 Unauthorized 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 program or data held in any computer and the access he intends to secure is unauthorized, and he knows at the time when he causes the computer to perform the function that this is the case. Maximum penalty is 6 months imprisonment and/or maximum £5,000 fine.

- The Ulterior Intent Offence

A person is guilty of this offence if he commits the Unauthorized 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 5 years imprisonment and/or unlimited fine.

- The Unauthorized 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 unauthorized).

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) 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 twenty years (in UK). Computer programs 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 programs
    - Typographical arrangement of published editions

Computer programs are protected as literary works. Literal copying is the copying of program 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 be infringement
    - Domain names – involves hijacking and "cybersquatting" 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. One must give credit to the original author.

Piracy

In 1994 an MIT student was indicted for placing commercial software on website for copying purposes. Student was accused of wire fraud and the interstate transportation of stolen property. The case was thrown out on a technicality ground 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 authorization.

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. 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 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:

- 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 specialized. 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 emphasizes 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.

REVISION QUESTIONS

QUESTION ONE

(a) Define the term e-commerce (3 Marks)
(b) List and describe the main forms of e-commerce (8 Marks)
(c) Discuss the main advantages and disadvantages of e-commerce (9 Marks)
(Total: 20 marks)

QUESTION TWO

(a) Information Technology and Information Systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change and thus threaten existing distributions of power money rights and obligations. Discuss five moral dimensions and the impact of the information age on them. (10 Marks)
(b) Name and briefly define two major legal issues associated with management of Information Systems. (4 Marks)
(c) Discuss the impact of the following aspects to information technology.
(i) Fair use (3 Marks)
(ii) Gate keeping (3 Marks)
(Total: 20 marks)

QUESTION THREE

(a) Define the following terms:
(i) End user computing (3 Marks)
(ii) Electronic Data Interchange (3 Marks)
(iii) Data warehouse (3 Marks)
(iv) Data mining (3 Marks)
(v) Information centre (3 Marks)
(b) Name the disadvantages associated with outsourcing of information technology services. (5 Marks)
(Total: 20 marks)

QUESTION FOUR

(a) Many small-scale enterprises do not have elaborate computerized information systems and many rely on manual systems. Discuss the issues that complicate access of information technology by small-scale enterprise (8 Marks)
(b) What options are available to small-scale enterprises utilization of and access to information technology with no in-house software development staff to develop and implement information systems? (6 Marks)
(c) List the measures of information system success. (6 Marks)
(Total: 20 marks)

QUESTION FIVE

(a) Not only can information systems help an organization to potentially gain competitive advantage but can be used deliberately to do so. Briefly describe the five-step process for using strategic planning of information systems. (10 Marks)
(b) How can the illegal use of software be reduced? (10 Marks)
(Total: 20 marks)

CHECK YOUR ANSWERS WITH THOSE GIVEN IN LESSON 9 OF THE STUDY PACK

COMPREHENSIVE ASSIGNMENT NO.4

Time Allowed: 3 Hours **Attempt any FIVE questions**

QUESTION ONE

(a) Name the goals that are achieved through the implementation of a computer network. (5 Marks)

(b) Define the following terms:

(i) Circuit switching networks (3 Marks)
(ii) Packet switching networks (3 Marks)
(iii) Message switching networks (3 Marks)
(iv) Non switching networks (3 Marks)

(c) List three advantages of adopting network protocols. (3 Marks)

(Total: 20 marks)

QUESTION TWO

(a) What does ISO/OSI reference model stand for and what is its significance in computer networks? (4 Marks)

(b) List the various layers of the ISO/OSI reference model and identify one functionality of each layer.
(14 Marks)

(c) List two advantages of managing computer communication through layered protocols. (2 Marks)

(Total: 20 marks)

QUESTION THREE

(a) Briefly define e-commerce. (3 Marks)

(b) The common models of e-commerce are B2C (Business-to-Customer) and B2B (Business to Business). Describe three emerging areas of e-commerce. (9 Marks)

(c) Describe the unique features of e-commerce as opposed to traditional commerce. (8 Marks)

(Total: 20 marks)

QUESTION FOUR

(a) List four factors that have led to the surge and popularity of the Internet. (8 Marks)

(b) Expand the following acronyms:

(i) TCP/IP
(ii) FTP
(iii) HTTP
(iv) HTML
(v) WWW (5 Marks)

(c) Describe the Client/Server Model. (7 Marks)

(Total: 20 marks)

QUESTION FIVE

(a) Define Information Resource Centre (IRC). (3 Marks)

(b) What is a software house? (3 Marks)

(c) (i) List the reasons as to why businesses engage in outsourcing. (4 Marks)

(ii) Name the risks associated with outsourcing and suggest possible ways of eliminating or reducing such risks. (10 Marks)

(Total: 20 marks)

QUESTION SIX

(a) Internet addresses are classified by domains. Most domain names are general categories of the type of organization. What do the following Internet address extensions mean:

(i) .edu
(ii) .com
(iii) .gov
(iv) .mil
(v) .net
(vi) .org

(6 Marks)

(b) What is software piracy? Suggest three ways of reducing software piracy. (8 Marks)

(c) Clearly define privacy and confidentiality. What different aspects of privacy do different government legal instruments and legislation handle? (6 Marks)

(Total: 20 marks)

QUESTION SEVEN

(a) Differentiate between a distributed system and a computer network. (4 Marks)

(b) Define information superhighway. (4 Marks)

(c) Briefly describe four types of computer crime. (8 Marks)

(d) List four services offered by online service providers (4 Marks)

(Total: 20 marks)

QUESTION EIGHT

(a) Define the following terms:

(i) Multiplexors (2 Marks)
(ii) Front end processors (2 Marks)
(iii) Cluster controllers (2 Marks)
(iv) Protocol converters (2 Marks)
(v) Spools (2 Marks)
(vi) Buffers (2 Marks)

(b) E-mail communication has become a popular mode of communication. What advantages do users of e-mail gain from using this mode of communication? (8 Marks)

(Total: 20 marks