STUDY MATERIAL

PROFESSIONAL PROGRAMME

INFORMATION TECHNOLOGY AND SYSTEMS AUDIT

MODULE 2

PAPER 4

THE INSTITUTE OF
Company Secretaries of India
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament

ICSI House, 22, Institutional Area, Lodi Road, New Delhi 110 003
tel 011-4534 1000, 4150 4444 **fax** +91-11-2462 6727
email info@icsi.edu **website** www.icsi.edu

TIMING OF HEADQUARTERS

Monday to Friday

Office Timings – 9.00 A.M. to 5.30 P.M.

Public Dealing Timings

Without financial transactions – 9.30 A.M. to 5.00 P.M.

With financial transactions – 9.30 A.M. to 4.00 P.M.

Phones

41504444, 45341000

Fax

011-24626727

Website

www.icsi.edu

E-mail

info@icsi.edu

Laser Typesetting by AArushi Graphics, Prashant Vihar, New Delhi, and
Printed at Tan Prints/July 2014

INFORMATION TECHNOLOGY AND SYSTEMS AUDIT

Technology and Science are transforming our world, changing the way we do business, the way we learn, the way we communicate, and even the way we entertain ourselves. Success in any field – law, medicine, business, education, entertainment, finance and investment – requires a command of technology. As the convergence of Telecommunications and Computing, Information Technology is the foundation of the 21st Century Economy. Company Secretaries Professionals also does not differs from it. In the age of e-filling and XBRL, It is very difficult for a corporate professional like Company Secretaries to survive without knowing the basics of Information Technology and Systems Audit.

Keeping the above in view, the subject Information Technology and Systems Audit have been incorporated at Professional Program. Studying Information Technology and Systems Audit will equip you to understand the basics of Information Technology, E-governance and Information Technology Act. The entire paper has been discussed in eleven study lessons. Every efforts has been made to give a comprehensive coverage of all the topics relevant to the subject and lists, diagrams and examples have been added in the study lesson to make the study easy and understandable.

In order to supplement the information/contents given in the study material, students are advised to refer to the Suggested Readings mentioned in the study material, Student Company Secretary, Business Dailies and Journals. In the event of any doubt, students may write to the Directorate of Academics in the Institute for clarification.

Although care has been taken in publishing this study material, yet the possibility of errors, omissions and/or discrepancies cannot be ruled out. This publication is released with an understanding that the Institute shall not be responsible for any errors, omissions and/or discrepancies or any action taken in that behalf.

Should there be any discrepancy, error or omission noted in the study material, the Institute shall be obliged if the same are brought to its notice for issue of corrigendum in the e-bulletin Student Company Secretary. Students may send their queries at the mail id ***academics@icsi.edu.***

SYLLABUS

MODULE (2) PAPER 4 : INFORMATION TECHNOLOGY AND SYSTEMS AUDIT

Level of Knowledge: Working Knowledge

Objective: *To acquire knowledge of Information Technology Law, Information Systems and Systems Audit.*

Detailed Contents:

1. **Information Technology Law**
   - Information Technology Act – Definitions, Important terms under Information Technology Legislation
   - Digital Signatures
   - Electronic Records
   - Certifying Authority
   - Digital Signature Certificate
   - Cyber Regulation Appellate Tribunal
   - Offences and Penalties
2. **Information Systems**
   - Systems- An Overview,
   - Information and Data: Definition and Distinctions
   - Information as a Corporate Resource
   - Features and Qualities of Information
   - Types of Information
   - Process of Generating Information
   - Value and Cost of Information
   - Information Needs at Various Levels of Management
   - Factors Influencing Information Needs
   - Information Systems: Definition and Elements
   - Information System Activities
   - Types of Information Systems
   - Information Systems in Business Management
   - Recent Trends in Information Systems
3. **Computer Hardware – An Overview**
   - Computers: An Introduction
   - Computer System: Concept, Types, Categories and Emerging Technologies

- Components of a Computer System
- Primary and Secondary Storage, Computer Storage Capacities
- Computer Peripherals – Inputs, Output and Storage Devices

4. Computer Software – An Overview

- Computer Software: An Introduction, Software Trends
- Multi-Programming, Multi-Processing, Time Sharing, Batch Processing
- On-Line and Real Time Processing
- Application Software
- Systems Securities

5. Database Management

- Data Base Concepts
- Data Structure
- Data Base Management System
- Data Base Files
- Data Mining and Warehousing

6. Programming – An overview

- Programming: Concepts, Stages of Programming
- Programme Development Approach
- Algorithm, Flow Charting Concepts
- High Level Languages
- Machine Level Languages

7. Internet and Other Technologies

- Internet and World-Wide Web, Intranets, Extranets, Applications Of Internet, Internet Protocols
- E-Commerce - Nature, Types (B2B, B2C, C2C), Supply Chain Management, CRM, Electronic Data Interchange (EDI), Electronic Fund Transfers (EFT), Payment Portal, E-Commerce Security
- Mobile Commerce, Bluetooth and Wi-Fi

8. Management Information Systems – An Overview

- Concept, Evolution and Elements
- Structure
- Computerized MIS
- Approaches of MIS Development
- Pre-requisites of an Effective MIS(a) Statutory corporations
- MIS and Decision Support Systems
- MIS and Information Resource Management

LIST OF RECOMMENDED BOOKS

PAPER 4: INFORMATION TECHNOLOGY AND SYSTEMS AUDIT

READINGS

Information Technology and Systems Audit

1. Ramesh Behl : Information Technology for Management, Tata McGraw Hill Education Private Ltd.
2. Jerome Kanter : Managing with Information, Prentice Hall of India
3. P.K. Sinha : Computer Fundamentals: Concepts, Systems and Applications, B.P.B. Publications
4. D.P. Mittal : Law of Information Technology (Cyber Law) with Information Technology (Certifying Authorities) Rules, 2000, Taxmann Pubilcations Pvt. Ltd.
5. Dr. L.M.Prasad and Usha Prasad : Information Systems & Technology, Sultan Chand & Sons

CONTENTS

PART A: THE INCOME TAX AND WEALTH TAX ACT

LESSON 1

INFORMATION TECHNOLOGY LAW

Page

LESSON 2

INFORMATION SYSTEMS

Page

LESSON 7

INTERNET AND OTHER TECHNOLOGIES

Lesson 1
Information Technology Law

LESSON OUTLINE

- Information Technology Act – Definitions.
- Important terms under Information Technology Legislation.
- Digital Signatures
- Electronic Records
- Certifying Authority
- Electronic Signature Certificate
- Cyber Appellate Tribunal
- Offences and Penalties

LEARNING OBJECTIVES

In present scenario, Computer and Internet has impacted every walk of our lives. Information technology has proved to be boon for humanity and it has benefited the human life in many ways. Since with every positive thing, some negatives also creep in, similarly people also started to misuse the wonders of information technology. In year 2000, information technology Act, 2000 was passed to deal with various matters pertaining to Information Technology, its uses and misuses. Information technology Act, 2000 provides legal recognition to electronic communication, email, digital signatures, computerized documents and it also provides for legal remedies in case of misuse of information technology. After reading this lesson, a student will be able to understand -

- The purpose of enacting Information Technology Act, 2000.
- The meaning of different terms as used in Information technology Act, 2000
- The meaning of digital signatures and electronic records
- The working of certifying authority appointed for issuing digital signatures
- The working of cyber regulation Appellate tribunal

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternative to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the India Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto

INTRODUCTION

The United Nations General Assembly by resolution A/RES/51/162, dated the 30 January 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This is referred to as the UNCITRAL Model Law on E-Commerce. Following the UN Resolution India passed the Information Technology Act 2000 in May 2000, which came into force on October 17, 2000. The Information Technology Act 2000 has been substantially amended through the Information Technology (Amendment) Act 2008 which was passed by the two houses of the Indian Parliament on December 23, and 24, 2008. It got the Presidential assent on February 5, 2009 and came into force on October 27, 2009

The Information technology Act, 2000 was made applicable in India with following objectives

1. To give legal recognition to any transaction which is done electronically or use of internet?
2. To give legal recognition to digital signature for accepting any agreement via computer.
3. To provide facility of filling document online relating to school admission or registration in employment exchange.
4. According to I.T. Act 2000, any company can store their data in electronic storage.
5. To stop computer crime and protect privacy of internet users.
6. To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.
7. To make more power to IPO, RBI and Indian Evidence act for restricting electronic crime.

Legislative History of Information Technology Act, 2000 (ITA 2000)

Information Technology Act was primarily based on UNICITRAL model law on e-commerce. Attempts were made in year 1998 for introducing law pertaining to Information technology in India but the Information Technology Act was passed only in June, 2000. The Government of India has brought major amendments to ITA-2000 in form of the Information Technology Amendment Act, 2008. ITAA 2008 (Information Technology Amendment Act 2008) as the new version of Information Technology Act 2000 is often referred has provided additional focus on Information Security. It has added several new sections on offences including Cyber Terrorism and Data Protection. A set of Rules relating to Sensitive Personal Information and Reasonable Security Practices (mentioned in section 43A of the ITAA, 2008) was released in April 2011.

Territorial Jurisdiction of the Act

Information technology Act, 2000 extends to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person.

Non Applicability of the Act

IT Act 2000 does not apply to –

(a) A negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;

(b) A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;

(c) A trust as defined in section 3 of the Indian Trusts Act, 1882;

(d) A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;

(e) Any contract for the sale or conveyance of immovable property or any interest in such property;

(f) Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

Important Definition under I.T Act, 2000

2(1) (a) **"Access"** with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

2(1) (b) "**Addressee**" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

2(1) (c) "**Adjudicating officer**" means an adjudicating officer appointed under subsection (1) of section 46;

2(1) (d) **"Affixing digital signature"** with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

2(1) (e) "**Appropriate Government**" means as respects any matter, –

(i) Enumerated in List II of the Seventh Schedule to the Constitution;

(ii) Relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

2(1) (f) "**Asymmetric crypto system**" means a system of a secure key pair consisting of a Private Key for creating a digital signature and a public key to verify the digital signature;

2(1) (g) "**Certifying Authority**" means a person who has been granted a license to issue a Digital Signature Certificate under section 24;

2(1) (h) "**Certification practice statemen**t" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

2(1) (i) "**Computer"** means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

2(1) (j) "**Computer network**" means the interconnection of one or more computers through –

(i) The use of satellite, microwave, terrestrial line or other communication media; and

(ii) Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

2(1) (l) "**Computer system**" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

2(1) (m) "**Controller"** means the Controller of Certifying Authorities appointed under sub-section (l) of section 17;

2(1) (n) "**Cyber Appellate Tribunal**" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

2(1) (o) "**Data**" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being

processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

2(1) (p) "**Digital signature**" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

2(1) *(q)* **"Digital Signature Certificate**" means a Digital Signature Certificate issued under subsection *(4)* of section 35;

2(1) (r) "**Electronic form**" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

2(1) (s) "**Electronic Gazette**" means the Official Gazette published in the electronic form;

2(1) (t) "**Electronic record**" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

2(1) (v) "**Information**" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche:

2(1) (w) "**Intermediary**" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

2(1) (x) "**Key pair**", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

2(1) (Za) "**Originator"** means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

2(1) (Zc) "**Private Key**" means the key of a key pair used to create a digital signature;

2(1) (zd) "**Public key**" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

2(1) (ze) "**Secure system**" means computer hardware, software, and procedure that –

(a) Are reasonably secure from unauthorized access and misuse;

(b) Provide a reasonable level of reliability and correct operation;

(c) Are reasonably suited to performing the intended functions; and

(d) Adhere to generally accepted security procedures;

2(1) (zh) "**Verify**" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether –

(a) The initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

DIGITAL SIGNATURE

As per Section *2(1) (p) of information technology Act* "**Digital signature**" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

Before going into details about provisions relating to digital signature, here it is important to understand the basic concepts relating to digital signature

A Digital signature (standard electronic signature) takes the concept of traditional paper-based signing and turns it into an electronic "fingerprint." This "fingerprint," or coded message, is unique to both the document and the signer and binds both of them together. The digital signature ensures the authenticity of the signer. Any changes made to the document after it is signed invalidate the signature, thereby protecting against signature forgery and information tampering. Digital signatures help organizations sustain signer authenticity, accountability, data integrity and non-repudiation of electronic documents and forms.

A digital signature is issued by a Certification Authority (CA) and is signed with the CA's private key. A digital signature/electronic signature typically contains the: Owner's public key, the Owner's name, Expiration date of the public key, the Name of the issuer (the CA that issued the Digital ID), Serial number of the digital signature, and the digital signature of the issuer. Digital signatures deploy the Public Key Infrastructure (PKI) technology.

In India, recognition to digital signature has been given by Income Tax Act and Companies Act. As per provisions of Companies Act, directors of the companies are required to sign their document by means of digital signature only. Similarly if one file his Income Tax return electronically using digital signature he does not have to submit a physical copy of the return.

Provisions relating to Digital Signature and Electronic Signature

As per section 3 of Information Technology Act, 2000 as amended, any subscriber may authenticate an electronic record by affixing his digital signatures. The authentication of the electronic records shall be effected by the use of *asymmetric crypto system and hash function* which envelops and transform the electronic records into another electronic record.

Here one explanation has been added to Section 3 and as per the explanation provided, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known' as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible –

(a) To derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) That two electronic records can produce the same hash result using the algorithm.

Any person by the use of a public key of the subscriber can verify the electronic record or the person signing the document.

The private key and the public key are unique to the subscriber and constitute a functioning key pair. The Public Key Infrastructure (PKI) is maintained by the Certification Authorities (CA) in India.

Electronic Signature

The provisions relating to electronic signature has been added by IT Information Technology (amendment) Act, 2008. Section 3A of amended Act prescribes –

Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (*2*), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable; and may be specified in the Second Schedule. The government has yet not notified the electronic signature or electronic authentication technique.

Any electronic signature or electronic authentication technique shall be considered reliable if –

(*a*) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(*b*) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(*c*) any alteration to the electronic signature made after affixing such signature is detectable;

(*d*) any alteration to the information made after its authentication by electronic signature is detectable; and

(*e*) it fulfils such other conditions which may be prescribed.

(*3*) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(*4*) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule: Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(*5*) Every notification issued under sub-section (*4*) shall be laid before each House of Parliament."

ELECTRONIC RECORDS

As per Section 2(t) of Information Technology Act, 2000 as amended, "**Electronic record**" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

Authentication of electronic records

As per Section 3 of IT Act, 2000 as amended, **any** subscriber may authenticate an electronic record by affixing his digital signature. The authentication of the electronic record are effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. 'Hash function' means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known 'as "hash result". An electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

The private key and the public key are unique to the subscriber and constitute a functioning key pair. The electronic records can be verified by a person by the use of a public key of the subscriber.

Legal Recognition to Electronic Records

Section 4 of IT Act, 2000 as amended provides legal recognition to Electronic Records. As per Section 4 of said Act, Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference.

Use of Electronic Records

As per Section 6 of IT Act, 2000 as amended, where any law provides for the filing of any form application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner; and the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner; and the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

Retention of Electronic Records

Section 7 of the IT Act, 200 as amended provides for retention of records in electronic format. It provides that where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if –

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received. These provisions will not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Audit of Electronic Records

As per Section 7A of IT Act, 2000 as amended where in any law, there is a provision of audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information maintained in the electronic form.

Validity of Contracts formed through electronic means

Section 10A of the IT Act, 2000 as amended provides that where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, are expressed in electronic form or by means of an electronic records, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means are used for that purpose.

Attribution of electronic records

Section 11 of IT Act, 2000 as amended provides that an electronic record shall be attributed to the originator if it was sent by the originator himself; or by a person who had the authority to Act on behalf of the originator in respect of that electronic record; or by an information system programmed by or on behalf of the originator to operate automatically.

Acknowledgment of receipt of electronic record

Section 12 of IT Act, 2000 as amended provides that where the originator has not stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by any communication by the addressee, automated or otherwise; or *any* conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment

must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the Electronic record as though it has never been sent.

Time and place of dispatch and receipt of Electronic record

Section 13 of IT Act, 2000 as amended provides that unless otherwise agreed between the originator and the addressee, the dispatch of an Electronic record occurs when it enters a computer resource outside the control of the originator & the time of receipt of an Electronic record shall be at the time when the Electronic, record enters the designated computer resource (for the cases where the addressee has designated a computer resource for the purpose of receiving Electronic records) and at the time when the Electronic record is retrieved by the addressee (For the cases where the Electronic record is sent to a computer resource of the addressee that is not the designated computer resource). If the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the Electronic record enters the computer resource of the addressee.

Save as otherwise agreed to between the originator and the addressee, an Electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the Electronic record is deemed to have been received under sub-section (3).

In addition to this, if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business and if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business; and “usual place of residence”, in relation to a body corporate, means the place where it is registered.

CERTIFYING AUTHORITY

A Certifying Authority is a trusted body whose central responsibility is to issue, revoke, renew and provide directories of Electronic Certificates. According to section 2(g) of Information Technology Act, 2000 as amended “Certifying Authority” means a person who has been granted a licence to issue Electronic Signature Certificates.

Application for becoming certifying Authority

Any person may make an application, to the Controller, for a licence to issue Electronic Signature Certificates provided he fulfills the Central Government prescribed requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Electronic Signature Certificates.

A license granted for issuing Electronic signature certificate is valid for 5 years and it is not transferable or heritable; it is subject to the terms and conditions as prescribed by Information Technology (Certifying Authorities) Rules, 2000.

Every application for issue of a licence shall be in such form as may be prescribed by Schedule-I Information Technology (Certifying Authorities) Rules, 2000 and shall be accompanied a certification practice statement; a statement including the procedures with respect to identification of the applicant; Payment of fees of twenty-five thousand rupees and Such other documents, as prescribed by Information Technology (Certifying Authorities) Rules, 2000.

Renewal of licence

A certifying Authority can apply for renewal of license not less than forty-five days before the date of expiry of the period of validity of licence and comply all the rules of Information Technology (Certifying Authorities) Rules, 2000 which are applied in case of fresh application for becoming certifying Authority.

The Controller may, on receipt of an application for appointment as certifying authority, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application: No application for becoming certifying Authority shall be rejected under unless the applicant has been given a reasonable opportunity of presenting his case.

Suspension of licence of a Certifying Authority for issuing electronic signature certificates

The Controller of Certifying Authority may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has made a false or incorrect statement in material particulars in, or in relation to, the application for the issue or renewal of the licence and/or it has failed to comply with the terms and conditions subject to which the licence was granted and/or it has failed to maintain the standards as specified and/or contravened any provisions of the Act, rules, regulations or order made there under, revoke the licence. However no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

The Controller of certifying authority may, if he has reasonable cause to believe that there is any ground for revoking a licence, by order suspend such licence pending the completion of any inquiry ordered by him provided no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension. The Certifying Authority whose licence has been suspended will not issue any Digital Signature Certificate during such suspension.

Certifying Authority to follow certain procedures

Every Certifying Authority shall make use of hardware, software and procedures that are secure from intrusion and misuse and it will provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions. It will adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and observe such other standards as may be specified by regulations.

Disclosures by Certifying Authority

Every Certifying Authority shall disclose in the manner specified by regulations – (a) its Electronic Signature (b) any certification practice statement relevant thereto; (c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and (d) any other fact that materially and adversely affects either the reliability of a Electronic Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Electronic Signature Certificate was granted, then, the Certifying Authority shall use reasonable efforts to notify any person who is likely to be affected by that occurrence; or act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

Controller of Certifying Authority

As per Section 17 of IT Act, 2000 as amended, The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities and such number of Deputy Controllers and Assistant Controllers as it deems fit for the purpose of this Act.

The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government and The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

Functions of the Controller

The Controller may perform all or any of the following functions, namely:–

(a) Exercising supervision over the activities of the Certifying Authorities;

(b) Certifying public keys of the Certifying Authorities;

(c) Laying down the standards to be maintained by the Certifying Authorities;

(d) Specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(e) Specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) Specifying the contents of written, printed or visual materials and Advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;

(g) Specifying the form and content of a Digital Signature Certificate and the Key,

(h) Specifying the form and manner in which accounts shall be maintained by The Certifying Authorities;

(i) Specifying the terms and conditions subject to which auditors may be Appointed and the remuneration to be paid to them;

(j) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) Specifying the manner in which the Certifying Authorities shall conduct their Dealings with the subscribers;

(l) Resolving any conflict of interests between the Certifying Authorities and the Subscribers;

(m) Laying down the duties of the Certifying Authorities;

(n) Maintaining a data base containing the disclosure record of every Certifying Authority

(o) Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Recognition of foreign Certifying Authorities

The Controller of Certifying Authority may recognize the foreign certifying authority with the prior approval of the Central Government provided they fulfill the prescribed conditions and restrictions. Where any Certifying Authority is recognised, the electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act. The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under subsection (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

ELECTRONIC SIGNATURE CERTIFICATES

The provisions relating to Electronic Signature Certificate are contained in Section 35-39 of IT Act, 2000 as amended. It provides that Certifying Authority will issue Electronic Signature Certificate on an application by a person in the form prescribed by the Central government. The application should be accompanied by a fee not exceeding Rs. 25,000/- and a certificate practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

On receipt of an application, the Certifying Authority may, after consideration of the certification practice statement or the other prescribed statement and after making such enquiries as it may deem fit, grant the electronic Signature Certificate or for reasons to be recorded in writing, reject the application:

Provided that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

Representations upon issuance of Digital Signature Certificate

Section 36 of IT Act, 2000 as amended provides that –

A Certifying Authority while issuing a Digital Signature Certificate shall certify that –

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder,

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(ca) The subscriber holds a private key which is capable of creating a digital signature:

(cb) The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber;

(d) the subscriber's public key and private key constitute a functioning key pair,

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

Suspension of Digital Signature Certificate

The provisions relating to Suspension of Digital Signature Certificate are contained in Section 37 of IT Act, 2000 as amended. This provides that the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate, –

(a) on receipt of **a request** to that effect *from* –

(i) the subscriber listed in to Digital Signature Certificate; or

(ii) any person duly authorised to act on behalf of that subscriber,

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest

A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Revocation of Digital Signature Certificate

The provisions relating to revocation of Digital Signature Certificate are contained in Section 38 of IT Act, 2000 as amended.

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it –

(a) where the subscriber or any other person authorised by him makes a request to that effect; or

(b) upon the death of the subscriber, or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that –

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent **or** dead or where a subscriber is a firm or a company, which has been dissolved, wound-up **or** otherwise ceased to exist

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Notice of suspension or revocation

Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be in all such repositories.

CYBER APPELLATE TRIBUNAL (CAT)

Cyber Appellate Tribunal has been established under the Information Technology Act under the aegis of Controller of Certifying Authorities (C.C.A.). The Tribunal initially known as the Cyber Regulations Appellate Tribunal (C.R.A.T.) started functioning from October 2006.

The Cyber Regulations Appellate Tribunal after the amendment of the IT Act in the year 2008 is known as the Cyber Appellate Tribunal (CAT). The Information Technology Act, 2000 has empowered the Central Government to establish one or more Cyber Regulations Appellate Tribunal.

The Act requires that a Cyber Appellate Tribunal shall consist of one person only to be referred as the Presiding Officer of the Cyber Appellate Tribunal who is to be appointed, by notification, by the Central Government. The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years. Subject to certain provisions, any person aggrieved by an order made by controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter. The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings. Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order

Composition of Cyber Appellate Tribunal

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he-

(a) is, or has been, or is qualified to be, a Judge of a High Court; or

(b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

Term of Office of Presiding Officer

The Presiding Officer of a Cyber Appellate shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty five years, whichever is earlier.

Resignation and removal

(1) The Presiding Officer of a Cyber Appellate Tribunal may, be notice in writing under his hand addressed to the Central Government, resign his office :

Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his officer sooner, continue to hold office until expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his terms of office, whichever is the earliest.

(2) The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his officer except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid presiding Officer.

Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings

No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

Staff of the Cyber Appellate Tribunal

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officer and employees as that Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

Appeal to Cyber Appellate Tribunal

Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal jurisdiction in the matter within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved. But no appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties. Every appeal shall be in such form and be accompanied by such fee as may be prescribed. The Cyber Appellate Tribunal may entertain an appeal after the expiry of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

The appeal filed before the Cyber Appellate Tribunal shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

Procedure and Powers of the Cyber Appellate Tribunal

The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sitting.

The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely : -

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses of documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it ex parte;

(g) any other matter which may be prescribed.

Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

Civil court not to have jurisdiction

No court shall have jurisdictions to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Appeal to High Court

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order : Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within 45 days, it may allow it to be filed within a further period not exceeding sixty days.

OFFENCES AND PENALTIES UNDER INFORMATION TECHNOLOGY ACT, 2000

Computer related offence [section 66 read with section 43]:

Section 66 of IT Act, 2000 as amended deals with computer related offences. Computer related offences have been defined in section 43 of IT Act, 2000 as amended. Section 43 of IT act provides that If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, –

(a) accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there- under;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or any other computer source code used for a computer resource with an intention to cause damage;

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to 5 lakh rupees or with both. (Section 66).

A explanation has been added for the purpose of this section which provides, –

(i) ''Computer contaminant'' means any set of computer instructions that are designed –

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) ''computer data base'' means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) ''computer virus'' means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates wh n a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) ''damage'' means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Compensation for failure to protect data

As per section 43A of IT Act, 2000 as amended, where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss

or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

An explanation has been given with this Section which provides that –

(*i*) "Body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(*ii*) "Reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(*iii*) "Sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.'

Penalty for failure to furnish information, return, etc.

As per section 44 of IT Act, 2000 as amended, If any person who is required under this Act or any rules or regulations made there under to –

(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues:

(c) Maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Residuary Penalty

Section 45 of IT Act, 2000 as amended provides that whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Tampering punishment for with computer source documents

This section provides for punishment upto three years or with a fine which may extend upto Rs. 2 lakhs or with both to a person who knowingly or intentionally tampers with the computer code source documents. *Computer Source Code* means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Punishment for sending message through communication service etc.

As per Section 66A of the IT Act,2000, Any person who sends, (*a*) any information that is grossly offensive or has menacing character; or (*b*) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device, (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the

addressee or recipient about the origin of such messages, by means of a computer resource or a communication device, s/he shall be punishable with imprisonment for a term which may extend to three years and with fine.

As per explanation given, for the purpose of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

Punishment for dishonestly receiving or retaining any stolen computer resource or communication device

As per section 66B of the IT Act, 2000 as amended, whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Punishment for Identity theft

As per section 66C of the IT Act, 2000 as amended, Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

Punishment for cheating by personation by using computer resource

As per section 66D of the IT Act, 2000 as amended, whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee.

Punishment for Violation of privacy

As per section 66E of the IT Act, 2000 as amended whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation. – For the purposes of this section –

(*a*) "Transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(*b*) "Capture", with respect to an image, means to videotape, photograph, film or record by any means;

(*c*) "Private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast:

(*d*) "Publishes" means reproduction in the printed or electronic form and making it available for public;

(*e*) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that –

(*i*) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(*ii*) any part of his or her private area would not be visible to the public regardless of whether that person is in a public or private place.

Punishment for Cyber terrorism

As per 66-F of the IT Act, 2000 as amended whoever, –

(*A*) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(*i*) denying or cause the denial of access to any person authorized to access computer resource; or

(*ii*) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(*iii*) introducing or causing to introduce any computer contaminant;

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(*B*) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Punishment for Publishing or transmitting of material obscene material in electronic form

As per 67 of the IT Act, 2000 as amended whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Punishment for Publishing or transmitting of material containing sexually explicit act, etc. in electronic form

As per 67A of the IT Act, whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Punishment for Publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

As per 67-B of the IT Act, whoever, –

(*a*) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(*b*) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(*c*) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(*d*) facilitates abusing children online, or

(*e*) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form –

(*i*) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(*ii*) which is kept or used for bonafide heritage or religious purposes.

Explanation- For the purposes of this section "children" means a person who has not completed the age of 18 years.

Punishment for publishing of information which is obscene in electronic form

Section 67 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to 3 years and with fine which may extend to Rs. 5 lakh on first conviction. In the event of second or subsequent conviction the imprisonment would be for a term which may extend to five years and fine which may extend to Rs. 10 lakhs.

Penalty for Misrepresentation

This section provides that any person found misrepresenting or suppressing any material fact from the Controller or the Certifying Authority shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.

Penalty for breach of confidentiality

Section 72 provides a punishment for breach of confidentiality and privacy of electronic records, books, information etc. by a person who has access to them without the consent of the person to whom they belong with imprisonment for a term which may extend to 2 years or with a fine which may extend to Rs. 1 lakh or with both.

Punishment for disclosure of information in breach of lawful contract

Section 72A of the Act provides. Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Penalty for publishing false electronic signature Certificate

This section provides punishment for publishing a **electronic signature** *Certificate* false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.

Penalty for fraudulent publication

This section provides for punishment with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both to a person whoever knowingly publishes for fraudulent purpose any electronic *Signature Certificate*.

LESSON ROUND-UP

- The Information Technology Act, 2000 was come into effect in year 2000 and it was further amended in Year 2008 by IT Amendment Act, 2008.
- This Act aims to provide the legal infrastructure for e-commerce in India. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.
- Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.
- Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference. The said chapter also details the legal recognition of Electronic Signatures.
- Chapter-VI of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Electronic Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Electronic Signature Certificates.
- Chapter-VII of the Act details about the scheme of things relating to Electronic Signature Certificates. The duties of subscribers are also enshrined in the said Act.
- Chapter-IX of the said Act talks about penalties, Compensation and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer for holding an inquiry in the manner prescribed by the Central Government. The adjudicating officer shall exercise jurisdiction to adjudicate matters in which the claim for inquiry or damage does not exceed Five Crore rupees.

– Chapter-X of the Act talks of the establishment of the Cyber Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

– Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Inspector of Police. These offences include tampering with computer source documents, Computer related offences, publishing of information, which is obscene in electronic form, cyber terrorism etc.

SELF-TEST QUESTIONS

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. Explain briefly the scope of the Information Technology Act 2000 as amended along with the relevant definitions that are used.
2. What are the conditions subject to which electronic record may be authenticated by means of affixing electronic signature?
3. Discuss the main provisions provided in Information Technology Act 2000 as amended to facilitate E-governance
4. What are the regulations relating to the appointment and powers of the certifying authorities under Chapter VI, Section 17 to 25 of Information Technology Act 2000 as amended?
5. What are the duties of a certifying authority under Section 30 of the Information Technology Act 2000 as amended?
6. What is a Digital Signature? How is it used? What are the duties of certifying authorities in regard to its usage?
7. Write short notes on the following:

   (a) Electronic Signature Certificate

   (b) Encryption.
8. Describe the composition and powers of Cyber appellate tribunal.
9. What are the major objectives of Information Technology Act 2000 as amended? Explain in brief.
10. Briefly explain the power of central government to make rules with respect to the Section 10 of Information Technology Act 2000 as amended.
11. Explain the power of Controller to make regulations under Section 89 of the Information Technology Act 2000 as amended.
12. What are the powers of a Police Officer under the Information Technology (Amendment) Act 2008 to enter and search etc?
13. Define ‘Electronic Signature’ and ‘Electronic Signature Certificate’ in the light of the Information Technology Act 2000 as amended.
14. Briefly explain the Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form as per Section 67 A of The Information technology Act, 2000 as amended.

Lesson 2
Information Systems

LESSON OUTLINE

- Systems – An Overview
- Information and Data: Definition and Distinctions
- Features and Qualities of Information
- Types of Information
- Process of Generating Information
- Value and Cost of Information
- Information as a Corporate Resource
- Information Needs at Various Levels of Management
- Factors Influencing Information Needs
- Information Systems: Definition and Elements
- Information System Activities
- Types of Information Systems
- Information Systems in Business Management
- Recent Trends in Information Systems

LEARNING OBJECTIVES

Information system is a term which is used for the framework that provides us information for decision making process. Information systems have a very important role to play in any business and successes of a business organization also depend on the timeliness, accuracy, and quality of information which is the output of an information system.

Information system is important at each level of business management. It supplies information from Strategic management team to middle management and it is very crucial for business successes. The importance of information system in a business management is for following reasons

- An aid in operational excellence
- Helpful in improved decision making
- Necessary for day to day survival
- Competitive Advantage
- Helpful in Cost Management

After going through this lesson the student should be able to:

- Understand the basics of information system
- Importance of Information systems in decision making process.

"What information consumes is rather obvious: it consumes the attention of its recipients. Hence, a wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it."

Herbert Simon

INTRODUCTION

Information system is a term use for the combination of networks of hardware and software, people, procedures, and organizations use to collect, filter, process, create, and distribute data, so that something meaningful can be extracted. It is playing a crucial role in everyone's life, as we all depend on information for better decision making. Information systems may be different for different types of people as the information need of different users are different; and it is difficult for a single information system to cater all users. Depending on the type of information requirement there are different information systems that exist. An information system which provides accurate, timely and reliable information is the key for an organization success. Here we will discuss

- Systems – An Overview
- Information and Data: Definition and Distinctions
- Information as a Corporate Resource
- Features and Qualities of Information
- Types of Information
- Process of Generating Information
- Value and Cost of Information
- Information Needs at Various Levels of Management
- Factors Influencing Information Needs
- Information Systems: Definition and Elements
- Information System Activities
- Types of Information Systems
- Information Systems in Business Management
- Recent Trends in Information Systems

SYSTEM OVERVIEW

A system is defined as multiple parts working together for a common purpose or goal. The term system is derived from the Greek word System, which means an organized relationship among functioning units or components. A system exists because it is designed to achieve one or more objectives. We come into daily contacts with the transportation system, the telephone system, the accounting system, the production system, and for over three decades, the computer system.

CHARACTERISTICS OF A SYSTEM

1. Organization of interrelated elements:

Organization implies structure and order. It is the arrangement of components that help to achieve objectives. For example, a computer system is designed around an input device, a central processing unit, an output device, and one or more storage units. When linked together they work as a whole system for producing information.

2. Interrelated components interaction:

Interaction refers to the manner in which each component functions with other component of the system. In a

computer system, for example, the central processing unit must interact with the input device to solve a problem. In turn, the main memory holds the program and data that the arithmetic unit uses for computation.

The interrelationship between these components enables the computer to perform smooth functions.

3. Interdependencies among system's parts

Interdependence means that parts of the system depend on one another. They are coordinated and linked together according to a plan. One subsystem depends on the input of another subsystem for proper functioning; i.e. the output of one subsystem is, the required input for another subsystem. This interdependence is crucial in systems work.

4. Common objectives

The last quality is central objective. Objectives may be real or stated. It is very common for an organization to state one objective and operates to achieve another. This important point is that users must know the central objective of a computer application early in the analysis for a successful design and conversion.

DIFFERENT TYPES OF SYSTEM

Systems are classified in different ways. Depending on their characteristics system can be classified in number of ways. The following classifications are worth mentioning.

1. Large and Small systems: This classification is based on the system size. Large complex systems can be the air traffic control system or our global telecommunication network. For small systems, small devices can also be considered as systems: such as a pocket calculator, alarm clock, or 10-speed bicycle.

2. Physical or Abstract systems: Systems can also be classified as physical and Abstract depending on whether they can be touched/seen or not. Examples are solar system and judicial system respectively.

Physical systems are tangible entities and may be static or dynamic in operation. For Example, the physical parts of the computer center are the offices, desks, and chairs that facilitate operation of the computer. They can be seen and counted, they are static. In contrast, programmed computer is a dynamic system. Data, programs, output and application changes as the user's demand or the priority of the information requested changes.

Abstract systems are conceptual or nonphysical entities. They may be models-the abstract conceptualization of physical situations such as traffic system. An abstract system can be a representation of a real or a planned system.

3. Open or Closed systems: Open systems refer to systems that interact with other systems or the outside environment. For example living organisms are considered open systems because they take in substances from their environment such as food and air and return other substances to their environment

Closed systems refer to systems having relatively little interaction with other systems or the outside environment. A watch is an example of a closed system in that it is a relatively self-contained, self-maintaining unit that has little interacts or exchange with its environment.

4. Natural or Manmade System: By virtue of their creation this classification applies. For example eco system, respiratory system in a human body are examples of natural systems, whereas computer system, electoral systems are examples of manmade system.

In the set of above classification, Information systems are large, manmade, open abstract system.

INFORMATION AND DATA: DEFINITION AND DISTINCTIONS

Meaning of Data and its characteristics

Data in Noun form means

- Facts and figures collected together for reference or analysis.
- The quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of Information.

Data is a collection of facts, such as values or measurements. It can be numbers, words, measurements, observations or even just descriptions of things.

Data characteristics

(a) Data means Facts, statistics used for reference or analysis.

(b) Data comprises Numbers, characters, symbols, images etc., which can be processed by a computer.

(c) Data must be interpreted, by a human or machine, to derive meaning.

(d) Data is a representation of information.

(e) Data is derived from Latin word 'datum' which means "that which is given".

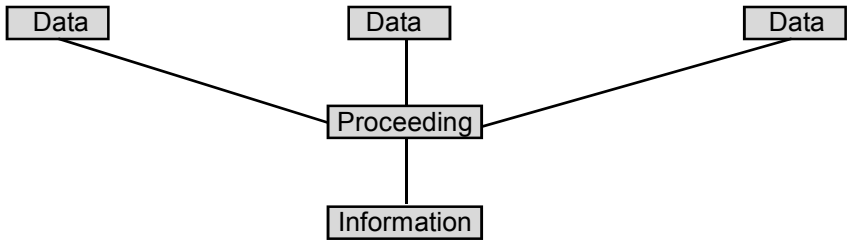
Meaning of Information and its characteristics

Information is Facts provided or learned about something or someone. It can be defined as data that:

- Has been verified to be accurate and timely
- Is specific and organized for a purpose
- Is presented within a context that gives it meaning and relevance, and
- That can lead to an increase in understanding and decrease in uncertainty.

In simple words it means processed data that has some meaning. Data alone are insufficient unless they are processed. Once converted in to information becomes directly applicable. The value of information lies solely in its ability to affect a behavior, decision, or outcome. A piece of information is considered valueless if, after receiving it, things remain unchanged

Information is created from data



Characteristics of Information

1. Information is the useful knowledge derived from the data
2. Information is knowledge derived from study, experience (by the senses), or instruction.
3. Information is any kind of knowledge that is exchangeable amongst people, about things, facts, concepts, etc.,

4. In some context “Information is interpreted data”.

Difference between Data and Information

	Data	Information
Definition	In Latin ‘datum’ means “that which is given”.	Information is interpreted data. Data was the plural form of datum singular
Meaning	Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized.	When data is processed, organized, structured or presented in a given context so as to make it useful, it is called Information.
Example	Each student’s test score is one piece of data	The class’ average score or the school’s average score is the information that can be concluded from the given data.

FEATURES AND QUALITIES OF INFORMATION

1. Relevancy: The information so generated should be relevant to the context for which it is collated. Too much irrelevant information may confuse the intended user so it is necessary o generate only relevant information. No information should be generated only because it can be generated by Information System. A good way of ensuring relevance is to closely define the objectives of any information reports. Another way to improve relevance is to produce information that focuses on “exceptions” - e.g. problems, high or low values, where limits have been exceeded.

2. Up-to-date: Information needs to be timely if it is to be actioned upon. For example, a professional need updated information about applicable laws so that he may give relevant advice to his clients. To improve the speed with which information is produced, businesses usually need to look at upgrading or replacing their information systems.

3. Accurate: As far as possible, information should be free from errors (e.g. the figures add up; data is allocated to the correct categories). The users of information should be informed whenever assumptions or estimates have been used.

4. Meet the needs of the User: Since different users have different information needs The managing director doesn’t have time to trawl through thick printouts of each week’s production or sales listings - he or she wants a summary of the key facts while the quality control supervisor will want detailed information about quality testing results rather than a brief one-line summary of how things are going. It is a good idea to encourage users to help develop the style and format of information reporting that they require.

5. Concise and User Friendly: Information should be clearly presented (e.g. use summaries, charts) and not too long. It also needs to be communicated using an appropriate medium (e.g. email, printed report, presentation. Businesses should also consider developing “templates” which are used consistently throughout the organization - so that users get used to seeing information in a similar style.

6. Worth the cost: Often forgotten. Information costs money. Data is costly to collect, analyze and report. Information takes time to read and assimilate. All users should question whether the information they receive/ have requested is worthwhile.

7. Reliable: Information should come from authoritative sources. It is good practice to quote the source used - whether it is internal or external sources. If estimates or assumptions have been applied, these should be clearly stated and explained.

TYPES OF INFORMATION

There may be different types of information classifications such as:

Factual vs. Analytical

Objective vs. Subjective

Primary vs. Secondary

1(A) Factual Information: These are just the facts. These information are very objective and real. Something that actually exists, reality, truth is a factual information. Examples of factual information are like; Temperature in a city, winner of academy award etc.

(B) Analytical Information: Interpretations, Analysis, Criticism constitute analytical information. To examine critically, so as to bring out the essential elements or give the essence of something, analysis is required. Examples include; Increase of drug use in the 2013, growth in crime rate etc.

2(A) Objective Information: Without Bias Non-judgmental "not influenced by personal feelings, interpretations, or prejudices; based on facts". It is to the point, clear cut without any personal projection. Examples of objective information needs: Chronology of the Feminist movement, the eight stages of development according to Erik Erikson

(B) Subjective Information: It includes **o**pinions, personal viewpoints, and evaluations existing in the mind. Examples of subjective information needs include; Criticism of O'Neill's play, Evaluation of a course based on class comments. Book review or movie reviews etc.

3(A) Primary Information: Information in its original form, not translated by anyone else, has not been published elsewhere, is termed as primary. Examples of primary information needs: Explanation or instructions from an employer or teacher, an eyewitness account of a house fire, etc.

(B) Secondary Information: It is repackaged examination, restatement or interpretation of primary information already collected by someone. Examples of secondary information needs: Notes borrowed from a classmate for a missed class, a bibliography on the letters of Ernest Hemingway and so on.

Based on it is meant for information may be Personal Information, or Business Information. There can be other classifications as well like, formal vs informal, confirmed vs tentative etc.

PROCESS OF GENERATING INFORMATION

The goal of information generation is to generating information which is reliable, timely, user friendly and meeting the intended user objectives. If it fails to meet the stated objectives it is considered poor in quality. Therefore information generation requires careful steps so that it serves it purpose. The process basically involves the following steps.

1. Understanding the user need in general
2. Create framework for generating intended information
3. Collecting the data.
4. Process or analyze data.
5. Collate the result from data, interpret, evaluate.
6. Communicate the result of interpretation, evaluation of data in form of Information to intended user.

VALUE AND COST OF INFORMATION

Information is of value to decision makers if it is accurate, timely, complete, and relevant. If it is poor on any o these criteria, it will be less useful hence may not have that value. These four criteria are used to distinguish valuable information from information that is of less value.

Accurate information provides a reliable and valid representation of reality. The cost of inaccurate or distorted information can be extremely high.

Consider the demise of the multimillion dollar Mars Climate Orbiter launched by NASA in 1998. The tragic outcome of this mission was blamed on the failure of one scientific team to recognize and correct an error in information from another team. Findings indicate that one team used English units (e.g., inches, feet and pounds) while the other used metric units for key spacecraft operations affecting navigation. This oversight caused the orbiter to burn up in Mars atmosphere before it could deploy to the surface. Oops.

Timely information is information that is available when it is needed. When information is needed almost always depends on the situation. In the fast-paced world of air travel, commercial airlines need virtually daily updates on what other commercial airlines are doing with their ticket prices. If one airline reduces its airfares from Mumbai Airport to New Delhi Airport, other airlines flying the same route would find out quickly about it and respond in a similar manner.

Complete information tends to be comprehensive in covering the issue or topic of interest. Complete information tells a complete story. Without complete information, a decision maker will get a distorted view of reality. Incomplete market information can lead businesses to introduce products and services that customers don't want.

Information is relevant if it has significance or can be applied to a specific situation, problem, or issue of interest. Here are some examples of relevant information. Human resource managers need information on hiring and employee turnover; operations managers need information on costs and productivity; marketing managers need information on sales projections and advertising rates; top executives need information on the strategic actions of their competitors. In contrast, product inventory information is not very relevant to a computer programmer.

INFORMATION AS A CORPORATE RESOURCE

Generally human, financial, physical and knowledge factors that provide a corporate the means to perform its business processes are considered as corporate resources.

Information can be considered as the raw material used in producing each and every decision taken in an organization. Organizations need to decide regularly on what objectives to be achieved, what actions to be taken to achieve these objectives, how and when these actions are to be taken, and the resources to be used for all these activities. These decisions are taken by all the people in the organization who work at different level of organizational hierarchy and handle different aspect of the organizational work.

The exact decision that in individual takes varies from person to person and from time to time, depending on nature of organizational tasks being performed. Also some people need to do more of decision making as compared to implementing the decisions. But everyone in the organization needs has to takes some decisions for which availability of adequate information is critical.

Information is also required to convey decisions taken to the people responsible for implementing the decisions taken, and for monitoring the actual results achieved as the work progresses. In want of information many decisions cannot be taken and in some cases it results into poor decisions. Therefore information is acting as a resource, which should be managed, so that needy people may get it in time when required. In this way information plays a role of corporate resource in every organization. Like any other resource it need to be formalized, must have some identified and systematize way of generation and dissemination.

INFORMATION NEEDS AT VARIOUS LEVELS OF MANAGEMENT

Information is needed for decision making at all levels of management. Managers at different organizational levels make different types of decisions, control different types of processes, and have different information needs.

Three classical levels of management include

1. Top Management or Strategic Management
2. Middle Management or tactical management
3. Low Level Management or Operational Management

Strategic Management includes directors/owner that make decisions which affect the entire organization, or large parts of it, and leave an impact in the long run. The decision making at this level is highly unstructured. By this we mean, there may not be a proper format for decision making. It requires lot of inputs in terms of information, but there is no fixed way of mixing those inputs.

Middle, or tactical, management receive strategic decisions from strategic management as general directives. Using those directives as guidelines, they develop tactics to meet those strategic directives. The decision making at this level is semi structured. Some pieces of information can be mixed to get some conclusion but some amount of ambiguity is always there.

Operational managers are responsible for daily operations. They make decisions concerning a narrow time span about the deployment of small groups of clerical and/or shop floor workers. Generally the decisions at this level are structured in nature.

People in different management levels have different information needs. Most of the information that managers require is used to make decisions. The decision making process of middle managers and above is less structured than that of operational managers; In general, strategic decisions have no proven methods for selecting a course of action that guarantees a predicted outcome.

Information needs of top or Strategic Management

Strategic management or TOP management of a company comprises the owners/managing director of a company. They are responsible for taking strategic decisions for a company which has long term bearing on company policies and perspectives. Strategic management is responsible for making strategic plan which is necessary to take the company on growth path. To prepare strategic Plan, Top management is not concerned about day to day information of company operations. They do the macro analysis and their decisions are based on macro analysis. Generally the Strategic Management information needs comprises

1. Information about market trend- Macro analysis.
2. Information about Government Policies.
3. Information about Competitors policies and tactics
4. Information about Major exceptions in implementing the company policy at tactical/operation level.
5. Analysis about major happening/event which may have a long term bearing on the strategic decisions of the company

The information need of TOP management is generally unstructured and it not easily defined.

Information needs of Middle Level Management/Tactical Management

Tactical management/Middle Management comprises those who are responsible for preparing annual business plan to achieve the strategic Plan objectives of a company. Tactical Managers prepare Annual

Business Plan on the basis of directs received from TOP management. The Information need of middle management comprises

1. Information about Strategic Decisions/Plan of the organization for which they have been working.
2. Information about Latest Technologies in the area they have been working.
3. Information about problems faced by operational management in getting the things implemented.
4. Information about best practices adopted by different organization in the same industries or different industries.

The information need of Middle level management is structured in comparison to TOP management and it can be developed in form of template in some cases.

Information needs of Low Level or Operational Management

Operation management is responsible for implementing the policies framed by tactical management to achieve the business plan of the organization. They are generally responsible for the operational part of the organization. The information need of Operational management is limited but very structured in nature. The information need of Operation management needs to be very accurate and it can be easily developed in the form of template.

FACTORS AFFECTING INFORMATION NEEDS

There are various factors which affected the information need of him. Some of them are explained as below

1. **Management Hierarchy:** Management Hierarchy plays an important role in deciding the information need of a user. Information need of TOP management will be entirely different from the information needs of Operational Management.
2. **Purpose of seeking information:** The information needs will be depend on the purpose of seeking information. If a person wants to investment in a company, he/she will be interested about the financial statement of the company. He/she will have no interest in knowing about the past directors of the company.
3. **Role in the Organization:** Information need of a person also depend on the role of the concerned user. The information needs of different stakeholder in the organization will be different. For example, an employee of the organization will be interested in knowing about the company wage policy. They will have no interest in knowing company policy on market segmentation.

INFORMATION SYSTEMS: DEFINITION AND ELEMENTS

An information system can be defined as:

All people, machines and activities aimed at the gathering and processing of data to supply the information need of people inside and outside the organization. In other words it can be defined as combination of people, hardware, software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose.

From the above definition we may observe following elements of an information system

- People
- Hardware
- Software
- Communication devices
- Network
- Data resources

INFORMATION SYSTEM ACTIVITIES

The major activities of an information system are:

1. **Input of data resource:** Input of data resources is prime and an important activity of an Information System. In this activity data about business transactions and other events is captured and prepared for processing. In this activity data entry activities such as recording and editing are covered.
2. **Processing of data into information:** Data is typically subjected to processing activities such as calculating, comparing, sorting, classifying, and summarizing. These activities organize, analyze and manipulate data, thus converting them into information for end users. The quality of any data stored in an information system must also be maintained by a continual process of correcting and updating activities.
3. **Output of information products:** Information in various forms is transmitted to end-users and made available to them in the output activity. The goal of information systems is the production of appropriate information products for end users. Common information products messages, reports, forms, and graphic images, which may be provided by video displays, audio responses, paper products, and multimedia.
4. **Storage of data resource:** Storage is a basic system component of information systems. Storage is the information system activity in which data and information are retained in an organized manner for later use. For example, just as written text material is organized into words, sentences, paragraphs, and documents; stored data is commonly organized into fields, records, files, and database. This facilitates its later use in processing or its retrieval as output when needed by users of a system.
5. **Control of system performance:** An important information system activity is the control of its performance. An information system should produce feedback about its input, processing, output, and the system is meeting established performance standards. Then appropriate system activities must be adjusted so that proper information products are produced for end users.

TYPES OF INFORMATION SYSTEM

Executive Support Systems (EIS)

An executive information system (EIS) is a type of management information system intended to facilitate and support the information and decision-making needs of senior executives by providing easy access to both internal and external information relevant to meeting the strategic goals of the organization. It is commonly considered as a specialized form of decision support system (DSS).

Management Information Systems (MIS)

An organized approach to the study of the information needs of an organization's management at every level in making operational, tactical, and strategic decisions. Its objective is to design and implement procedures, processes, and routines that provide suitably detailed reports in an accurate, consistent, and timely manner.

It is mainly concerned with internal sources of information. MIS usually take data from the transaction processing systems and summarize it into a series of management reports. MIS reports tend to be used by middle management and operational supervisors.

Decision-Support Systems (DSS)

Decision-support systems (DSS) are specifically designed to help management make decisions in situations where there is uncertainty about the possible outcomes of those decisions. DSS comprise tools and techniques to help gather relevant information and analyze the options and alternatives. DSS often involves use of complex spreadsheet and databases to create "what-if" models.

Knowledge Management Systems (KMS)

Knowledge Management Systems (KMS) exist to help businesses create and share information. These are typically used in a business where employees create new knowledge and expertise - which can then be shared by other people in the organization to create further commercial opportunities. Good examples include firms of lawyers, accountants and management consultants.

KMS are built around systems which allow efficient categorization and distribution of knowledge. For example, the knowledge itself might be contained in word processing documents, spreadsheets, PowerPoint presentations, Internet pages or whatever. To share the knowledge, a KMS would use group collaboration systems such as an intranet.

Transaction Processing Systems (TPS)

As the name implies, Transaction Processing Systems (TPS) are designed to process routine transactions efficiently and accurately. A business will have several (sometimes many) TPS; for example: Billing systems to send invoices to customers. Systems to calculate the weekly and monthly payroll and tax payments, Production and purchasing systems to calculate raw material requirements, Stock control systems to process all movements into, within and out of the business etc.

Office Automation Systems (OAS)

Office Automation Systems are systems that try to improve the productivity of employees who need to process data and information. Perhaps the best example is the wide range of software systems that exist to improve the productivity of employees working in an office (e.g. Microsoft Office XP) or systems that allow employees to work from home or whilst on the move.

INFORMATION SYSTEMS IN BUSINESS MANAGEMENT

Information system has been playing a pivotal role in Business Management nowadays. A good information system may be termed as the backbone of business management. In today scenario, it is imperative to say that an Information system is the key to success of a business. A good information system is essential for midsize business to large business. The massive data and increasing volumes of data needs organized storing and fast and effective processing for variety of purposes from decision making to risk management, from transaction processing to state-the art products. This is possible only with the help of an effective information system.

Now the business has become global and most of the businesses are global distributed across the world. These businesses require stable and reliable network infrastructure which can run and handle simultaneous and real time fast processing. Now with the advancement of information technology, simultaneous processing of data on 24x7 bases has got possible. This has increased the efficiency of business. Here we can say that the more businesses grow the more dependent they become of Information Systems

Information system is important at each level of business management. It supplies information from Strategic management team to middle management and it is very crucial for business successes. The importance of information system in a business management is for following reasons

(a) An aid in operational excellence

(b) Helpful in improved decision making

(c) Necessary for day to day survival

(d) Competitive Advantage

(e) Helpful in Cost Management

RECENT TRENDS IN INFORMATION SYSTEMS

It is generally accepted that information is a vital commodity for the successful operation of today's organizations. Nowadays modern business organizations are using computerized information systems in order to obtain desired information. However, as the technology advances rapidly the main issue is how can an organization should effectively use such an information system which its management sometimes can be unpredictable in order to effectively help the whole organization structure to improve and take the most out of it.

It seems fairly obvious that Information systems have played an important linking role even before the advent of the Internet. Thus, for example, the possibilities offered by Information systems have strongly influenced the way managers were able to exercise control and therefore constituted an important factor in the organization of large-scale enterprise and their geographic extension. The same is true for governments and their statistical apparatus. The recent integration of computer networks and electronic data exchange facilitated the creation of common databases and policies among governments, speeding up developments, which had started earlier. It also created new possibilities for business, for example enabling companies to develop new organizational practices (e.g. just-in-time).

However, the role of Information systems in the organization is shifting to support business processes rather than individual functions. The focus is outwards to customers, rather than inwards to procedures. Businesses are changing more and more rapidly.

This poses a challenge to existing Information systems, which are often inappropriately structured to meet these needs. It also poses a challenge to the people who design, work and use these systems, since they may hold outdated assumptions.

To ensure the services provided by Information systems whenever needed and their failure will not cause catastrophic disaster their reliability and efficiency become extremely important. Imagine what would happen when a banking system malfunctions due to some critical faults in the system or when a healthcare information system provides wrong advice for patients.

It is even not over-saying that our lives are already under control of computer systems but their reliability and efficiency has become extremely important

Here we would be discussing few of the information system which are evolving and getting widely used by the organizations.

Use of Cloud Computing

One of the most talked about concept in information system is the cloud computing. Clouding computing is defined as utilization of computing services, i.e. software as well as hardware as a service over a network. Typically, this network is the internet.

Some of the benefit of cloud computing is as follows:

1. Cloud computing reduces IT infrastructure cost of the company.
2. Cloud computing promotes the concept of virtualization, which enables server and storage device to be utilized across organization.
3. Cloud computing makes maintenance of software and hardware easier as installation is not required on each end user's computer.

Some issues concerning cloud computing are privacy, compliance, security, legal, abuse, IT governance, etc.

Use of Mobile Application

Another emerging trend within information system is use of mobile applications (software application on Smart phone, tablet, etc.) in designing information systems.

Mobile application or mobile app has become a success since its introduction. They are designed to run on Smartphone, tablets and other mobile devices. They are available as a download from various mobile operating systems like Apple, Blackberry, Nokia, etc. Some of the mobile app are available free where as some involve download cost. The revenue collected is shared between app distributor and app developer.

Use of User Interfaces

User interface has undergone a revolution since introduction of touch screen. The touch screen capability has revolutionized way end users interact with application. Touch screen enables the user to directly interact with what is displayed and also removes any intermediate hand-held device like the mouse.

Touch screen capability is utilized in smart phones, tablet, information kiosks and other information appliances.

Use of Analytics

The field of analytics has grown many folds in recent years. Analytics is a process which helps in discovering the informational patterns with data. The field of analytics is a combination of statistics, computer programming and operations research.

The field of analytics has shown growth in the field of data analytics, predictive analytics and social analytics. Data analytics is tool used to support decision-making process. It converts raw data into meaningful information. Predictive analytics is tool used to predict future events based on current and historical information. Social media analytics is tool used by companies to understand and accommodate customer needs. The every changing field of information technology has seen great advancement and changes in the last decade. And from the emerging trend, it can be concluded that its influence on business is ever growing, and it will help companies to serve customers better.

Use of Big Data Analytics

It is the process of examining large amounts of data of a variety of types (big data) to uncover hidden patterns, unknown correlations and other useful information. Such information can provide competitive advantages over rival organizations and result in business benefits, such as more effective marketing and increased revenue.

The primary goal of big data analytics is to help companies make better business decisions by enabling data scientists and other users to analyze huge volumes of transaction data as well as other data sources that may be left untapped by conventional business intelligence(BI) programs. These other data sources may include Web server logs and Internet click stream data, social media activity reports, mobile-phone call detail records and information captured by sensors. Some people exclusively associate big data and big data analytics with unstructured data of that sort, but consulting firms like Gartner Inc. and Forrester Research Inc. also consider transactions and other structured data to be valid forms of big data.

Use of Agile Technology: Agile software development

It is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development cycle. Agile technology is being widely used by the organization in developing information system now a days and it is resulting in various advantages.

Following are the major advantages of agile systems.

(1) Time & Money saving: The very first advantage that the company got to see with the Agile Methodology is the saving of time and money. There is less documentation required though documents help to a great deal in verifying and validating the requirements but considering the time frame of the project, this

approach leads to focus more on the application rather than documenting the things. Since it is iterative in its form, it tends to have a regular feedback from the end user so that the same can be implemented as soon as possible. And because all phases of SDLC need to be completed very quickly, there is a transparency to each individual working on the project with the status of each phase.

(2) Easy to incorporate changes: Another advantage that Agile Methodology offers to other approaches available is that in case there is any Change request or enhancements come in between any phase, it can be implemented without any budget constraint though there needs to be some adjustment in the already allotted time frame which will not be a difficult task for the projects following Agile tactics. Though it is useful for any Programming language or Technology around, it is advisable to make it employ for Web 2.0 or the projects which are new in media.

(3) Fast execution: Daily meetings and discussions for the project following agile approach can help to determine the issues well in advance and work on it accordingly. Quick coding and Testing makes the management aware of the gaps existing in either requirements or technology used and can try to find the workaround for the same.

(4) Short Project life cycle: Hence, with the quicker development, testing and constant feedbacks from the user, the Agile methodology becomes the appropriate approach for the projects to be delivered in a short span of time.

Here we have discussed few of the rapidly evolving trends in information systems but this list is growing and growing. Student are expect to keep them aware of latest trends in information system, development and applications

LESSON ROUND-UP

- System is a set of interrelated elements that collectively work together to achieve some common purpose or goal. Systems can be of different types and may be classified as Physical or Abstract systems, Open or Closed systems, 'Man-made' Information systems, Formal Information systems, Informal Information systems, Computer Based Information systems, Real Time System
- Data is a collection of facts, such as values or measurements. It can be numbers, words, measurements, observations or even just descriptions of things.
- Information is Facts provided or learned about something or someone. It can be defined as Data that (1) has been verified to be accurate and timely, (2) is specific and organized for a purpose, (3) is presented within a context that gives it meaning and relevance, and (4) that can lead to an increase in understanding and decrease in uncertainty
- There are various types of information such as Personal Information, Business Information, Statistical Information, Futuristic Information, Formal Information, Informal Information, Confirmed Information, Tentative Information, grapevine information, Technical Information, General Information, Secret Information, Strategic Information, Historical information, Current Information, Competitor Information.
- Process of generating information includes Understanding the user need in general, creating framework for generating intended information, collecting data, Processing and analyzing data, collating the result from data, interpret, evaluate and communicating the result of interpretation, evaluation of data in form of Information to intended user.
- Information is needed for decision making at all levels of management. Managers at different organizational levels make different types of decisions, control different types of processes, and have different information needs.
- Information needs of Top management is very unstructured and not defined as they require the information for strategic planning of institute while the information need of Middle level management is

structured in comparison to TOP management and it can be developed in form of template in some cases. The information need of Operation management needs to be very accurate and it can be easily developed in the form of template.

– An information system can be defined as all people, machines and activities aimed at the gathering and processing of data to supply the information need of people inside and outside the organization. In other words it can be defined as combination of people, hardware, software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose.

– Information system activities includes Input of data resource, Processing of data into information, Output of information products:, Storage of data resource:, Control of system performance:

– There are different types of information system being used which primarily includes Executive Support System, Management Information System, Decision-Support System, Knowledge Management System, Transaction Processing System, Office Automation System.

SELF-TEST QUESTIONS

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. What do you mean by System? Explain different types of systems in detail.
2. What is the difference between
   (a) Open system and Closed System
   (b) Physical system and abstract system
   (c) Formal information system and information system.
3. What do you mean by data and information? State the difference between data and information in detail.
4. All information may be categorized as data but all data item may not be categorized as information. Elucidate.
5. Explain about the information gathering process. Also explain the different characteristic of information.
6. Write a short note on information as a corporate resource
7. Explain the different levels of management and their information need in an organisation.
8. What are the factors which affects the information need?
9. What do you mean by information system? Explain any five types of information system which are being used by an organisation.
10. What are the different functions of an information system? Clearly explain
11. Write short note on use of
    (a) Cloud computing
    (b) Agile Technology
    (c) Big data technology
    (d) User Interface
    (e) Mobile application in information systems.

Lesson 3
Computer Hardware – An Overview

LESSON OUTLINE

- Introduction of the term Computers
- Types of Computers
- Classification of computers on the basis of size, functions and generations
- Newer technology in Computers
- Components of a Computer System
- Primary and Secondary Storage, Computer Storage Capacities
- Computer Peripherals – Inputs, Output and Storage Devices

LEARNING OBJECTIVES

The word 'Computer' is a part of almost everyone's life. Computer has become an essential of our life. Earlier when we were talking about computers, pictures of work place or office were coming out but now scenario has changed. Now computer is available even with most of the middle class people. Seeing this now everyone needs to know about computer and its applications.

A Company Secretary is professional who requires good knowledge of basics of computer and its application so in view of this, study of computers and its components becomes vital.

After reading one would be able to

- Understand the meaning of term computers
- Learn about different types of computers
- Understand the difference between Analog and digital computers
- Learn about the classification of computer on the basis of size, function and generation
- Know about the newer types of computers
- Understand about different components of computers and their functions.
- Learn about different computer peripherals i.e. Input, Output and Storage devices

What a computer is to me is the most remarkable tool that we have ever come up with. It's the equivalent of a bicycle for our minds"

Steve Jobs

COMPUTERS: AN INTRODUCTION

"What is computer" this question that today sounds absurd, as everyone seems to know the answer to this redundant question. The fact actually is, everyone has their own interpretation of what A Computer is as they see it. The word computer has been expanded by different person in different perspective. 4 different expanded form of the word computer are as

COMPUTER Common Operating Machine Particularly Used for Trade, Education, and Research

COMPUTER Common Operating Machine Particularly Used for Training, Education, and Reporting

COMPUTER Commonly Operated Machine Particularly Used for Technological Engineering Research

COMPUTER Complicated Office Machine Put Under Tremendous Effort to Reduce manpower

Thus from the above table we may observe that

(a) Computer is a Machine

(b) Computer is used in Trade, Education, Research, Training and Technological Research.

(c) Computer helps in reducing man efforts.

(d) Computer is used in office for business reporting.

The field of computers has seen such unprecedented growth that it has become an integrated and important part of everyone's life. Today, a computer would is viewed as a youngster's toy which they use to surf the internet, listen songs, see videos, see pictures and more popularly - be connected using social networking. A computer has been reduced to a device that no longer needs any prior experience or learning to operate it, quite in contrast to the past days.

COMPUTER SYSTEM – CONCEPT

A computer system in contemporary usage refers to a desktop system including the computer along with any software and peripheral devices that are necessary to make the computer function.

A Computer system is made up of two parts: The hardware and the software.

1. Hardware: The physical equipment required to create, use, manipulate and store electronic data.

2. Software: The computerized instructions that operate a computer manipulate the data and execute particular functions or tasks.

In this chapter we will confine our discussion to the Hardware of the computer

TYPES OF COMPUTERS

Analog Computers

Analog computers are used to process continuous data. Analog computers represent variables by physical quantities. Thus any computer which solve problem by translating physical conditions such as flow, temperature, pressure, angular position or voltage into related mechanical or electrical related circuits as an analog for the physical phenomenon being investigated in general it is a computer which uses an analog quantity and produces analog values as output. Thus an analog computer measures continuously. Analog computers are very much speedy. They produce their results very fast. But their results are approximately correct. All the analog computers are special purpose computers.

Digital Computers

Digital computer represents physical quantities with the help of digits or numbers. These numbers are used to perform Arithmetic calculations and also make logical decision to reach a conclusion, depending on, the data they receive from the user.

Hybrid Computers

Various specifically designed computers are with both digital and analog characteristics combining the advantages of analog and digital computers when working as a system. Hybrid computers are being used extensively in process control system where it is necessary to have a close representation with the physical world.

The hybrid system provides the good precision that can be attained with analog computers and the greater control that is possible with digital computers, plus the ability to accept the input data in either form.

Difference between Analog and Digital Computers

Analog Computers	***Digital Computers***
Analog computers process measured data. A speedometer in your car is a common type of analog device.	A digital computer processed discrete data (digits). In this case 0 and 1
Analog Computers Work on continuous values.	Digital computers Work on discrete values
Analog Computers have low memory.	Digital computers have a very large memory
Analog computers have Slow speed.	Digital computers have fast speed.
Analog computers are less reliable.	Digital computers are more reliable.
Analog computers are used in engineering, science and medical fields.	Digital computers are used in all fields of life.
Analog computers are used to calculate / measure analog quantities like speed and temperature.	Digital computers are used to calculate mathematical and logical operations. It can solve addition, subtraction, division, multiplication and other mathematical and statistical operations.
Analog computers provide less accurate results.	Digital computers provide 100% accurate results.
Normally Analog Computers are specific purpose	Digital Computers are general purpose
Analog computers are difficult to use	Digital computers are easy to use
Examples of Analog computers are: thermometer, analog clock, speedometer etc.	Examples of digital computers are:Personal Computer, laptops, smart phones etc.

CLASSIFICATION OF COMPUTER

Classification by Size

1. Supercomputer

Supercomputers are highly sophisticated computers used for very special tasks like scientific research etc. Supercomputers are very expensive and are employed for specialized applications that require immense amounts of mathematical calculations (number crunching). For example, weather forecasting requires a supercomputer. Other uses of supercomputers scientific simulations, (animated) graphics, fluid dynamic calculations, nuclear energy research, electronic design, and analysis of geological data (e.g. in petrochemical prospecting).

Supercomputers are the most powerful computers made till now. The main feature of super computer is multiprocessing which enables the computer to perform number of operation simultaneously.

The 1st Supercomputer was built in 1960 in US for US department of defense. India has also made its own Super computer named PARAM in 1991.

2. Mainframe Computer

Mainframe computers are large-sized, powerful multi-user computers that can support concurrent programs. That means, they can perform different actions or 'processes' at the same time. Mainframe computers can be used by as many as hundreds or thousands of users at the same time. Large organisations may use a mainframe computer to execute large-scale processes such as processing the organization's payroll.

The chief difference between a supercomputer and a mainframe is that a supercomputer channels all its power into executing a few programs as fast as possible, whereas a mainframe uses its power to execute many programs concurrently. In some ways, mainframes are more powerful than supercomputers because they support more simultaneous programs. But supercomputers can execute a single program faster than a mainframe.

3. Minicomputer

Mini-computers are mid-sized multi-processing computers. Again, they can perform several actions at the same time and can support from 4 to 200 users simultaneously. In recent years the distinction between mini-computers and small mainframes has become blurred. Often the distinction depends upon how the manufacturer wants to market its machines. Organizations may use a mini-computer for such tasks as managing the information in a small financial system or maintaining a small database of information about registrations or applications.

4. Workstation

Workstations are powerful, single-user computers. They have the capacity to store and process large quantities of data, but they are only used by one person at a time. However, workstations are typically linked together to form a computer network called a local area network, which means that several people, such as staff in an office, can communicate with each other and share electronic files and data.

A workstation is similar to a personal computer but is more powerful and often comes with a higher-quality monitor. In terms of computing power, workstations lie in between personal computers and mini-computers. Workstations commonly support applications that require relatively high-quality graphics capabilities and a lot of memory, such as desktop publishing, software development and engineering applications.

5. Personal computers

Personal computers (PCs), also called microcomputers, are the most popular type of computer in use today. The PC is a small-sized, relatively inexpensive computer designed for an individual user. Today, the world of PCs is basically divided between IBM-compatible and Macintosh-compatible machines, named after the two computer manufacturers. Computers may be called 'desktop' computers, which stay on the desk, or 'laptop' computers, which are lightweight and portable. Organizations and individuals use PCs for a wide range of tasks, including word processing, accounting, desktop publishing, preparation and delivery of presentations, organization of spreadsheets and database management. Entry-level PCs are much more powerful than a few years ago, and today there is little distinction between PCs and workstations.

Classification by function

1. Servers

Server usually refers to a computer that is dedicated to providing a service. For example, a computer dedicated to a database may be called a "database server". "File servers" manage a large collection of computer files. "Web servers" process web pages and web applications. Many smaller servers are actually personal computers that have been dedicated to providing services for other computers.

2. Workstations

Workstations are computers that are intended to serve one user and may contain special hardware enhancements not found on a personal computer.

3. Information appliances

Information appliances are computers specially designed to perform a specific user-friendly function —such as playing music, photography, or editing text. The term is most commonly applied to mobile devices, though there are also portable and desktop devices of this class.

4. Embedded computers

Embedded computers are computers that are a part of a machine or device. Embedded computers generally execute a program that is stored in non-volatile memory and is only intended to operate a specific machine or device. Embedded computers are very common. Embedded computers are typically required to operate continuously without being reset or rebooted, and once employed in their task the software usually cannot be modified. An automobile may.

Classification by Generations

The history of computer development is often referred to in reference to the different generations of computing devices. Each generation of computer is characterized by a major technological development that fundamentally changed the way computers operate, resulting in increasingly smaller, cheaper, more powerful and more efficient and reliable devices.

1. First Generation (1940-1956) Vacuum Tubes

The first computers used vacuum tubes for circuitry and magnetic drums for memory, and were often enormous, taking up entire rooms. They were very expensive to operate and in addition to using a great deal of electricity, generated a lot of heat, which was often the cause of malfunctions.

First generation computers relied on machine language, the lowest-level programming language understood by computers, to perform operations, and they could only solve one problem at a time. Input was based on punched cards and paper tape, and output was displayed on printouts.

The UNIVAC and ENIAC computers are examples of first-generation computing devices. The UNIVAC was the first commercial computer delivered to a business client, the U.S. Census Bureau in 1951.

2. Second Generation (1956-1963) Transistors

Transistors replaced vacuum tubes and ushered in the second generation of computers. The transistor was invented in 1947 but did not see widespread use in computers until the late 1950s. The transistor was far superior to the vacuum tube, allowing computers to become smaller, faster, cheaper, more energy-efficient and more reliable than their first-generation predecessors. Though the transistor still generated a great deal of heat that subjected the computer to damage, it was a vast improvement over the vacuum tube. Second-generation computers still relied on punched cards for input and printouts for output.

Second-generation computers moved from cryptic binary machine language to symbolic, or assembly, languages, which allowed programmers to specify instructions in words. High-level programming languages were also being developed at this time, such as early versions of COBOL and FORTRAN. These were also the first computers that stored their instructions in their memory, which moved from a magnetic drum to magnetic core technology.

The first computers of this generation were developed for the atomic energy industry.

3. Third Generation (1964-1971) Integrated Circuits

The development of the integrated circuit was the hallmark of the third generation of computers. Transistors

were miniaturized and placed on silicon chips, called semiconductors, which drastically increased the speed and efficiency of computers.

Instead of punched cards and printouts, users interacted with third generation computers through keyboards and monitors and interfaced with an operating system, which allowed the device to run many different applications at one time with a central program that monitored the memory. Computers for the first time became accessible to a mass audience because they were smaller and cheaper than their predecessors.

4. Fourth Generation (1971-Present) Microprocessors

The microprocessor brought the fourth generation of computers, as thousands of integrated circuits were built onto a single silicon chip. What in the first generation filled an entire room could now fit in the palm of the hand. The Intel 4004 chip, developed in 1971, located all the components of the computer—from the central processing unit and memory to input/output controls—on a single chip.

In 1981 IBM introduced its first computer for the home user, and in 1984 Apple introduced the Macintosh. Microprocessors also moved out of the realm of desktop computers and into many areas of life as more and more everyday products began to use microprocessors.

As these small computers became more powerful, they could be linked together to form networks, which eventually led to the development of the Internet. Fourth generation computers also saw the development of GUIs, the mouse and handheld devices.

5. Fifth Generation (Present and Beyond) Artificial Intelligence

Fifth generation computing devices, based on artificial intelligence, are still in development, though there are some applications, such as voice recognition, that are being used today. The use of parallel processing and superconductors is helping to make artificial intelligence a reality. Quantum computation and molecular and nanotechnology will radically change the face of computers in years to come. The goal of fifth-generation computing is to develop devices that respond to natural language input and are capable of learning and self-organization.

NEWER DEVELOPMENT IN COMPUTERS

Laptop Computers

Laptop computers are usually lightweight mobile PCs with an LCD display thin screen. They are sometimes called notebook computers because they can be used instead of a notebook with paper. Laptops can also operate on batteries, so you can take them anywhere you need to work. Unlike desktops, laptops are completely self-contained. The laptop folds and closes like a book. Hence making it easy for you to learn how to use computer faster any where you go.

Handheld Computers

Handheld computers, also called personal digital assistants (PDAs), are battery-powered computers like Blackberry's. Handheld computers are not as fast as desktops or laptops, handhelds are handy for making appointments, keeping track of addresses and phone numbers, and playing games.

Some handhelds have more advanced features, like making telephone calls or getting on the Internet. Instead of a keyboard, handheld computers or PDA's have touch screens that you use with your finger or a stylus, which looks a lot like a pen without ink.

Tablet Computers

Tablet Personal Computers are mobile PCs that combine features of laptops and handhelds. Like laptop computers, Tablet computers are very powerful, fast and have a screen like a tablet. Like handhelds, Tablets can allow you to make notes or draw pictures directly on the screen, usually with a tablet pen instead of a

stylus. Tablets can also transform your handwriting into typed text? Some Tablet PCs have a screen that swivels and unfolds to reveal a keyboard under the computer.

Palmtop

A small computer that literally fits in your palm. Compared to full-size computers, palmtops are severely limited, but they are practical for certain functions such as phone books and calendars. Palmtops that use a pen rather than a keyboard for input are often called hand-held computers or PDAs. Because of their small size, most palmtop computers do not include disk drives. However, many contain PCMCIA slots in which you can insert disk drives, modems, memory, and other devices. Palmtops are also called PDAs, hand-held computers and pocket computers

COMPUTER HARDWARE

The hardware are the parts of the computer itself including the Central Processing Unit (CPU) and related microchips and micro-circuitry, keyboards, monitors, case and drives (hard, CD, DVD, floppy, optical, tape, etc...). Other extra parts called peripheral components or devices include mouse, printers, modems, scanners, digital cameras and cards (sound, colour, and video) etc... Together they are often referred to as a personal computer. The different Hardware components of a computer are explained below.

Central Processing Unit

Pronounced as separate letters, CPU is the abbreviation for ***c**entral **p**rocessing **u**nit*. Sometimes referred to simply as the *central processor*, but more commonly called *processor,* the CPU is the brains of the computer where most calculations take place. In terms of computing power, the CPU is the most important element of a computer system.

On large machines, the CPU requires one or more printed circuit boards. On personal computers and small workstations, the CPU is housed in a single chip called a *microprocessor*. Since the 1970's the microprocessor class of CPUs has almost completely overtaken all other CPU implementations.

The CPU itself is an internal component of the computer. Modern CPUs are small and square and contain multiple metallic connectors or pins on the underside. The CPU is inserted directly into a CPU socket, pin side down, on the motherboard.

Each motherboard will support only a specific type (or range) of CPU, so you must check the motherboard manufacturer's specifications before attempting to replace or upgrade a CPU in your computer. Modern CPUs also have an attached heat sink and small fan that go directly on top of the CPU to help dissipate heat.

Two typical components of a CPU are the following:

- The *arithmetic logic unit (ALU)*, which performs arithmetic and logical operations.
- The *control unit (CU)*, which extracts instructions from memory and decodes and executes them, calling on the ALU when necessary.

Functions of Central Processing unit

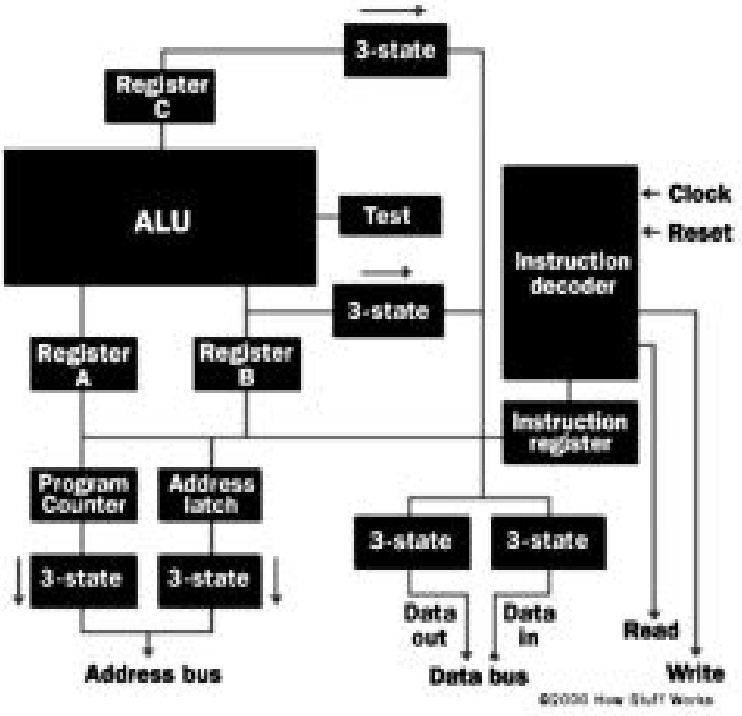
A CPU has four primary functions: **fetch**, **decode**, **execute**, and **write back**.

A. Fetch

In the first step, the CPU retrieves the instruction that it needs to run from program memory. Each instruction in a program (which contains millions of instructions) is stored at a specific address. The CPU has a *program counter*, which keeps track of the CPU's position in the program ""more specifically, the address of the instruction that the CPU is accessing.

B. Decode

For this step, it's important to know that no matter what code a program is written in, the compiler for that specific language breaks the code down to Assembly Language. Assembly language is a language that the CPU understands, but may vary between different CPUs. From there on, an "˜assembler' translates Assembly Language into binary code, which the CPU can manipulate to execute the instructions it is given.



C. Execute

Based on the instructions it is given, the CPU can then do one of three things:

(1) Using its Arithmetic Logic Unit (ALU), the CPU can calculate extremely complicated mathematical functions;

(2) Move data from one memory location to another;

(3) Jump to different addresses in the program based on decisions made by the CPU itself.

The diagram above shows the setup of an extremely simple microprocessor capable of performing these actions.

D. Write back

Typically, each of the actions taken by the CPU produces some sort of output. The CPU takes this output and writes it into the computer's memory. For example, if a program wanted to execute the first item of the list above

on two operands, 3 and 5, the output, 8, would be written back into a specific address. However, for the 3rd bullet, the program counter (which, as stated above, is used to keep track of the CPU's progress through a program) simply changes to reflect the start of the next set of instructions.

When these four steps have been completed, the Program Counter moves onto the next instruction and repeats the entire process again, until the termination of the program.

Another important component of a CPU is called the "clock." The clock produces a signal that acts to synchronize the logic units within the CPU as they execute the instructions given in a program. In the diagram above, the purple line represents the signal of a clock as it is being inputted into a logic unit. For every time the line goes from low to high, and back to low (one cycle), an instruction is carried out.

Thus, the CPU Clock speed refers to the number of times that a CPU's clock cycles per second. Typical computers have a clock speed around 2.8 GHz (Gigahertz), which means that the clock cycles 2.8 billion times a second, and execute an equivalent number of instructions!

INPUT DEVICES

Keyboard

The Keyboard is an Input device of a computer. It is mechanical in nature. The keyboard is used to type information into the computer. On the basis of input made through Keyboard computer executes its function. There are many different keyboard layouts and sizes with the most common for Latin based languages being the QWERTY layout (named for the first 6 keys). It is available in 101 and 104 keys. The standard keyboard has 101 keys. It has following basic types of keys-alphanumeric keys, modified keys (shift, Cntrl, Alt), special character keys, function keys (F1 toF12), Cursor movement keys (Arrow, PgUp, PgDn, Home, End), and special purpose keys (Insert, Delete, Escape, Print, Scroll, Scroll lock and Pause}.

Mouse

Mouse is also a popular input device. Most modern computers today mainly desktop are run using a mouse controlled pointer. Earlier mouse was mechanical in nature but now optical mouse are also used extensively. Mouse is generally available in 2 button and 3 buttons models. Generally if the mouse has two buttons the left one is used to select objects and text and the right one is used to access menus.

Now with the popularization of Laptop, use of mouse has declined. Laptop computers use touch pads, buttons and other devices to control the pointer. Handhelds computers use a combination of devices to control the pointer, including touch screens.

Trackball

A trackball is a pointing device consisting of a ball held by a socket containing sensors to detect a rotation of the ball about two axes – like an upside-down mouse with an exposed protruding ball. It is mechanical in nature and available in two and three button models. The user rolls the ball with the thumb, fingers, or the palm of the hand to move a pointer. Compared with a mouse, a trackball has no limits on effective travel; at times, a mouse can

reach an edge of its working area while the operator still wishes to move the screen pointer farther. With a trackball, the operator just continues rolling. Some trackballs, such as Logitech's optical-pickoff types, have notably low friction, as well as being dense (glass), so they can be spun to make them coast.

Image Scanner

Image Scanner often abbreviated as scanner is an input device which scans text or graphics on a printed paper and digitize the same into a form that computer can use. It is photo electric in nature an available in hand held or flat bed model.

Bar Code Reader

A Bar Code reader is an input device which reads the bar code printed and converts the barcode into a machine readable form. Bar Code reader has found wide acceptance in industry and widely used in retail trade. It is also photo electric in nature.

Optical Character Recognition (OCR)

Optical character recognition, usually abbreviated to OCR, is the mechanical or electronic conversion of scanned images of handwritten, typewritten or printed text into machine-encoded text. It is widely used as a form of data entry from some sort of original paper data source, whether documents, sales receipts, mail, or any number of printed records. It is crucial to the computerization of printed texts so that they can be electronically searched, stored more compactly, displayed on-line, and used in machine processes such as machine translation, text-to-speech and text mining. OCR is a field of research in pattern recognition, artificial intelligence and computer vision.

Other Input Devices

A. Web Cameras: Often known as webcam is a video camera that feeds its images in real time to a computer or computer network, often via USB, Ethernet, or Wi-Fi.

B. Digital Cameras: A digital camera (or digicam) is a camera that takes video or still photographs, or both, digitally by recording images via an electronic image sensor. It is the main device used in the field of digital photography.

C. Camcorders: A camcorder (formally a *video camera recorder*) is an electronic device that combines a video camera and a video recorder into one unit; typically for out-of-studio consumer video recording.

D. Microphone: A microphone informally called a mic or mike; is an acoustic-to-electric transducer or sensor that converts sound into an electrical signal. Microphones are used in many applications such as telephones, tape recorders, karaoke systems, hearing aids, motion picture production, live and recorded audio engineering, FRS radios, megaphones, in radio and television broadcasting and in computers for recording voice, speech recognition, VoIP, and for non-acoustic purposes such as ultrasonic checking or knock sensors.

E. Joystick: A **joystick** is an input device consisting of a stick that pivots on a base and reports its angle or direction to the device it is controlling. Joysticks are often used to control video games, and usually have one or more push-buttons whose state can also be read by the computer.

F. Optical Mark Reader: It is a special scanning device that can read carefully placed pencil marks on specially designed documents. OMR is frequently used in forms, questionnaires, answer-sheets.

G. Touch Pen: A stylus for touch screens on mobile devices, such as iPhones and Androids, that requires the body's electricity. The touch pen, which has a rubber tip with high carbon content, allows current to transfer between the user and capacitive screens.

H. Touch pad: A touchpad (or track pad) is a pointing device featuring a tactile sensor, a specialized surface that can translate the motion and position of a user's fingers to a relative position on screen. Touchpads are commonly used in Laptop as a substitute of a mouse.

I. Touch Screen: A touch screen is an electronic visual display that can detect the presence and location of a touch within the display area. The term generally refers to touching the display of the device with a finger or hand. Touch screens can also sense other passive objects, such as a stylus. Touch screens are common in devices such as game consoles, all-in-one computers, tablet computers, and smartphones.

J. Light pen: A light pen is a computer input device in the form of a light-sensitive rod used in conjunction with a computer's CRT display. It allows the user to point to displayed objects or draw on the screen in a similar way to a touch screen but with greater positional accuracy.

K. Graphic digitizer: Graphic Digitizer also known as graphics tablet is an input device which is used to convert hand-drawn images into a format suitable for computer processing. Images are usually drawn onto a flat surface with a stylus and then appear on a computer monitor or screen.

OUTPUT DEVICES

Monitors

It is an output device used for observing, checking, or keeping a continuous record of a process or quantity: A monitor is also known as display/Screen/Visual Display Unit. It is electronic in nature. The monitor comprises the display device, circuitry, and an enclosure. The display device in modern monitors is typically a thin film transistor liquid crystal display (TFT-LCD) thin panel, while older monitors use a cathode ray tube about as deep as the screen size.

Monitors come in many types and sizes. The resolution of the monitor determines the sharpness of the screen. The resolution can be adjusted to control the screen's display.

Printer

Printer is an output device which produces a text or graphics of documents stored in electronic form, usually on physical print media such as paper or transparencies. These are often classified as impact printer or non impact printer. Dot matrix printer, daisy wheel printer, thermal printer and Line printer are known as Impact printer while Inkjet Printer, Laser printer are known as non impact printer.

Many printers are primarily used as local peripherals, and are attached by a printer cable or, in most new printers, a USB cable to a computer which serves as a document source. Some printers, commonly known as *network printers*, have built-in network interfaces, typically wireless or Ethernet based, and can serve as a hard copy device for any user on the network.

Plotter

The plotter is a computer output device which produces drawing on paper based on commands from a computer. Plotter .differ from printer as it draws lines using a pen. It can produce continuous lines. It is mainly used in engineering application and expensive in nature.

Sound Card and Speakers

Sound card and speakers are output devices which facilitates the audio output from computer. Sound card helps in converting digital signal into audio output which is then heard through the speakers. Today with the advent of Multimedia systems, sound cards and speaker have become integral parts of the computer system.

OTHER COMPUTER PERIPHERALS

Modem

Modem is the abbreviated form of Modulator Demodulator. A modem is a device or program that enables a computer to transmit data over, for example, telephone or cable lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem

converts between these two forms. It modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used over any means of transmitting analog signals, from light emitting diodes to radio. The most familiar example is a voice band modem that turns the digital data of a personal computer into modulated electrical signals in the voice frequency range of a telephone channel. These signals can be transmitted over telephone lines and demodulated by another modem at the receiver side to recover the digital data

Video Cards

A video card, display card, graphics card, or graphics adapter is an expansion card which generates a feed of output images to a display. Most video cards offer various functions such as accelerated rendering of 3D scenes and 2D graphics, MPEG-2/MPEG-4 decoding, TV output, or the ability to connect multiple monitors (multi-monitor).

Video hardware can be integrated into the motherboard but recently it has been integrated into the CPU, however all modern motherboards, and even motherboards from the 90's provide expansion ports to which a video card can be attached.

Network Card

A network card is a piece of hardware that allows a computer to connect to a computer network. Sometimes the network card is integrated on the motherboard. Each network card has a unique number; this is used for addressing. It is called the MAC address.

Computer Data Storage

Computer data storage is often called storage or memory, refers to computer components and recording media that retain digital data. Data storage is a core function and fundamental component of computers.

In contemporary usage, 'memory' usually refers to semiconductor storage read-write random-access memory, typically DRAM (Dynamic-RAM). *Memory* can refer to other forms of fast but temporary storage. *Storage* refers to storage devices and their media not directly accessible by the CPU, (secondary or tertiary storage), typically hard disk drives, optical disc drives, and other devices slower than RAM but are non-volatile (retaining contents when powered down).

Historically, *memory* has been called *core*, *main memory*, *real storage* or *internal memory* while storage devices have been referred to as *secondary storage*, *external memory* or *auxiliary/peripheral storage*.

The distinctions are fundamental to the architecture of computers. The distinctions also reflect an important and significant technical difference between memory and mass storage devices, which has been blurred by the historical usage of the term *storage*. Nevertheless, this article uses the traditional nomenclature.

Many different forms of storage, based on various natural phenomena, have been invented. So far, no practical universal storage medium exists, and all forms of storage have some drawbacks. Therefore a computer system usually contains several kinds of storage, each with an individual purpose.

Measurement of Computer Data Storage

Computer storage is measured in bytes, kilobytes (KB), megabytes (MB), gigabytes (GB) and increasingly terabytes (TB). One byte is one character of information, and is comprised of eight bits (or eight digital 1's or 0's). Technically a kilobyte is 1024 bytes, a megabyte 1024 kilobytes, a gigabyte 1024 megabytes, and a terabyte 1024 gigabytes. This said, whilst this remains true when it comes to a computer's internal RAM and solid state storage devices (like USB memory sticks and flash memory cards), measures of hard disk capacity often take 1MB to be 1,000,000 bytes (not 1,024,768 bytes) and so on. This means that the storage capacity of two devices labelled as the same size can be different, and which remains an ongoing source of debate within the computer industry.

TYPES OF COMPUTER MEMORY

Primary Storage

Primary storage (or *main memory* or *internal memory*), often referred to simply as *memory*, is the only one directly accessible to the CPU. The CPU continuously reads instructions stored there and executes them as required. Any data actively operated on is also stored there in uniform manner. Main memory is a combination of both RAM and ROM.

Random Access Memory or RAM is a form of data storage that can be accessed randomly at any time, in any order and from any physical location in contrast to other storage devices, such as hard drives, where the physical location of the data determines the time taken to retrieve it. RAM is read write memory i.e. information can be read as well as write on this type of memory. RAM is referred to as volatile memory and is lost when the power is turned off

Read-only memory or ROM is a form of data storage in computers and other electronic devices that can not be easily altered or reprogrammed. ROM in non-volatile and the contents are retained even after the power is switched off.

Difference between Random Access Memory (RAM) and Read-only memory (ROM)

Stands for:	Random Access Memory	Read-only memory
Volatility:	RAM is volatile i.e. its contents are lost when the device is powered off.	It is non-volatile i.e. its contents are retained even when the device is powered off.
Types:	The two main types of RAM are static RAM and dynamic RAM.	The types of ROM include PROM, EPROM and EEPROM.
Use:	RAM allows the computer to read data quickly to run applications. It allows reading and writing.	ROM stores the program required to initially boot the computer. It only allows reading.
Definition:	Random Access Memory or RAM is a form of data storage that can be accessed randomly at any time, in any order and from any physical location.	Read Only Memory is a form of memory which is used for storing program. As the name suggest it can only read but not altered.

Cache Memory

Cache (pronounced cash) is a block of high speed memory where data is copied when it is retrieved from the RAM. This storage of key instructions enables a performance improvement in the processor. Intel processors incorporate level 1 (L1) and level 2 (L2) caches.

There are two groups of extremely fast memory chips that allow the computer to operate faster:

(1) Internal cache (L1) is built into the CPU, and

(2) External cache (L2) resides on the motherboard. The L2 cache is an area of high-speed memory that improves performance by reducing the average memory access time. L2 cache is also called SRAM.

Both L1 and L2 store data recently used by the CPU. When the CPU needs data, it first checks the fastest source — L1. If the data is not there, the CPU checks the next-fastest source — L2. If the data still cannot be found, a time-consuming search of the slower RAM is required.

Secondary Storage/Secondary Memory

The auxiliary storage memory, also known as the secondary storage memory is an external (to the CPU) memory. This memory is also known as auxiliary storage/secondary storage. A secondary storage device is a storage

medium that holds information until it is deleted or overwritten. For example, a floppy disk drive or a hard disk drive is an example of a secondary storage device. Secondary memory is permanent in nature i.e. the information stored in this memory is not lost unless specifically deleted. Secondary storage as permanent in nature is also used for transportation of data from one computer to another.

Secondary storage is actually any storage not currently in use. Even the hard drive in your computer is secondary storage, as programs such as Word or PowerPoint, are stored there when not in use as well as all of your files. Ssecondary memory is much slower and also less costly. Secondary memories may also be considered as input output devices as they provide the information as input and store the final result as output .

Difference between Primary Memory and Secondary Memory

Primary Memory	Secondary Memory
These are semiconductor memories.	These are magnetic and optical memories.
They are characterized as volatile random access memories (RAM) or non-volatile memories (ROM).	They are non-volatile.
They contain program and data that is currently being used by micro processor.	These are used to for bulk storage.
These memories are fast enough to interact with the microprocessor.	Slower than primary memories.
Also known as Main Memory	Also known as Backup Memory or Auxiliary Memory. E.g. Tapes, Floppies, Hard Discs, CD ROMs, DVDs

Computer Storage Capacities

Storage capacity refers to how much disk space one or more storage devices provides. It measures how much data a computer system may contain. For an example, a computer with a 500GB hard drive has a storage capacity of 500 gigabytes. A network server with four 1TB drives has a storage capacity of 4 terabytes.

As of 2011, the most commonly used data storage technologies are semiconductor, magnetic, and optical, while paper still sees some limited usage. *Media* is a common name for what actually holds the data in the storage device. Some other fundamental storage technologies have also been used in the past or are proposed for development.

COMPUTER STORAGE TECHNOLOGY

Semiconductor Storage Technology

Semiconductor memory is an electronic data storage device, often used as computer memory, implemented on a semiconductor-based integrated circuit. Examples of semiconductor memory include non-volatile memory such as read-only memory (ROM), magneto resistive random-access memory (MRAM), and flash memory. It also includes volatile memory such as static random-access memory (SRAM), which relies on several transistors forming a digital flip-flop to store each bit, and dynamic random-access memory (DRAM), which uses one capacitor and one transistor to store each bit. Shift registers, processor registers, data buffers and other small digital registers that have no memory address decoding mechanism are not considered as memory.

Magnetic Storage Technology

Magnetic storage and **magnetic recording** are terms from engineering referring to the storage of data on a

magnetized medium. Magnetic storage uses different patterns of magnetization in a magnetizable material to store data and is a form of non-volatile memory. The information is accessed using one or more read/write heads. As of 2011, magnetic storage media, primarily hard disks, are widely used to store computer data as well as audio and video signals. In the field of computing, the term *magnetic storage* is preferred and in the field of audio and video production, the term *magnetic recording* is more commonly used. The distinction is less technical and more a matter of preference. Other examples of magnetic storage media include floppy disks, magnetic recording tape, and magnetic stripes on credit cards.

Optical Storage Technology

Optical storage is any storage method in which data is written and read with a laser for archival or backup purposes. Typically, data is written to optical media, such as CDs and DVDs. For several years, proponents have spoken of optical storage as a near-future replacement for both hard drives in personal computers and tape backup in mass storage.

Optical media is more durable than tape and less vulnerable to environmental conditions. On the other hand, it tends to be slower than typical hard drive speeds, and to offer lower storage capacities.

Magneto-optical disc storage is optical disc storage where the magnetic state on a ferromagnetic surface stores information. The information is read optically and written by combining magnetic and optical methods. Magneto-optical disc storage is *non-volatile*, *sequential access*, slow write, fast read storage used for tertiary and off-line storage.

Paper Based Storage Technology

Paper data storage, typically in the form of paper tape or punched cards, has long been used to store information for automatic processing, particularly before general-purpose computers existed. Information was recorded by punching holes into the paper or cardboard medium and was read mechanically (or later optically) to determine whether a particular location on the medium was solid or contained a hole. A few technologies allow people to make marks on paper that are easily read by machine – these are widely used for tabulating votes and grading standardized tests. Barcodes made it possible for any object that was to be sold or transported to have some computer readable information securely attached to it.

DATA STORAGE DEVICES

USB Flash Drive

A **USB flash drive** is a small device that stores information and files from a computer. Flash drives are an easy way of moving data between different computers or devices to be read or edited. Flash drives are connected to

a computer using a USB port, which can be found on many devices. Flash drives take their name from the **flash** memory used to hold files. Flash memory is a type of memory that does not need any moving parts, unlike a CD or Floppy disk.

The capacity of flash drives starts at few megabytes. In April 2010, the ones that could hold most data could hold about 256 gigabytes.

Other common names for a flash drive include: **memory stick**, **keydrive**, **pendrive**, **thumbdrive** and **jumpdrive** or simply **USB**.

USB flash drives have some advantages over other portable storage devices. They are much smaller than floppy disks, and can hold much more data. They do not have moving parts, so they should be more reliable.

Hard Disk

Top and bottom views of a Western Digital WD400 3.5" hard disk

A **hard disk drive** (HDD) , **hard disk** (sometimes 'disk' is also spelled *disc*) or **hard drive**, is something used by computers to store information. Hard disks use magnetic recording (similar to the way recording is done on magnetic tapes) to store information on rotating circular platters. The capacity of a hard drive is usually measured in gigabytes (GB). A gigabyte is one thousand megabytes and a megabyte is one million bytes, which means that a gigabyte is one billion bytes. Some hard drives are so large that their capacity is measured in terabytes, (TB) where one terabyte is a thousand gigabytes (1 TB = 1000 GB). Very early Consumer Grade hard drives were measured in Megabytes

Compact Disc

The read side of a **Compact Disc**

A **Compact Disc** (**CD**) is a type of optical disc. It is flat and round, and is used to store digital data. It was first used to store music and other sounds (and is sometimes called an "audio CD"). The sound on a CD is played using a compact disc player. It was developed by Phillips and Sony.

Later, Compact Discs were made that could be used to store computer files in the same way as audio compact discs. These are called CD-ROMs (Compact Disc Read-Only Memory). The computer reads the disc using a CD-ROM drive. Another use is to store MPEG videos cheaply; these CDs are called VCDs (Video CDs) and are especially popular in Asia. For example, in Indonesia they are used instead of the more expensive DVD.

The diameter of a normal CD is 120 mm. The middle hole in a CD is about the size of a five cent coin (about 1.5 cm). The person who decided the size was Dutch and used the size of an old Dutch coin (old because the Dutch now have switched to the Euro), called a "dubbeltje", or dime. A CD usually holds a maximum of 74-80 minutes of sound or 650-700 megabytes of data.

DVD

Two kinds of DVD: Single layer (left) and dual layer (right).

A **DVD** (which means **Digital Versatile Disc** or a **Digital Video Disc**) is an optical disc capable of storing up to 4.7 GB of data, more than six times what a CD can hold. DVDs are often used to store movies at better quality than a VHS. DVDs can also have interactive menus and bonus features such as deleted scenes and commentaries. Like CDs, DVDs are read with a laser.

The disc can have one or two sides, and one or two layers of data per side; the number of sides and layers determines how much it can hold. A 12 cm diameter disc may have one of the following storage capacities:

The capacity of a DVD-ROM can be visually determined by noting the number of data sides, and looking at the data side(s) of the disc. Double-layered sides are usually gold-colored, while single-layered sides are usually silver-colored, like a CD. One additional way to tell if a DVD contains one or two layers is to look at the center ring on the underside of the disc. If there are two barcodes, it is a dual layer disc. If there is one barcode, there is only one layer.

DVD Data Storing

Both **CD** and **DVD** discs have equal sizes (diameter, thickness etc.). However, the amount of information they can store is different. These discs are made of the same materials and have the same methods of production.

CDs and DVDs use the same way of keeping information. Both CDs and DVDs have pits and bumps on the data track (the data track represents a path which has certain information). The information is read by a laser.

A DVD disk has several layers, which are made of plastic. All layers have a thickness of 1.2 millimeters. An injection used on a polycarbonate plastic leads to the creation of microscopic bumps. Today's production uses this type of plastic to create different things because it can resist very high and low temperatures.

When layers are made, the bumps appear. Many bumps form one continuous spiral that can include information. After that a spray of a special reflective layer covers the bumps.

Aluminum is applied behind inner layers and semi-reflective gold covers the outer layers. This helps the laser to concentrate through the outer layers onto the inner ones. Then, after applying a protective liquid (lacquer) and pressing the layers, they are treated with infrared light.

LESSON ROUND-UP

- A computer system in contemporary usage refers to a desktop system including the computer along with any software and peripheral devices that are necessary to make the computer function.
- Hardware and software are the two basic parts of a computer system Hardware - any part of a computer system you can touch Software - a set of electronic instructions that tell a compute what to do.
- Computers are of various types as Analog Computers which are used to process continuous data such as flow, temperature, pressure, angular position or voltage and Digital Computers which are used to perform Arithmetic calculations and also make logical decision to reach a conclusion, depending on, the data they receive from the user. Hybrid Computers refers to various specifically designed computers with both digital and analog characteristics combining the advantages of analog and digital computers when working as a system. Hybrid computers are being used extensively in process control system where it is necessary to have a close representation with the physical world.
- Computers can be classified on the basis of size, generations, and functions.
- There are many news technologies being introduced in computers. Now computer has moved from office to home. Tablets, Laptop, Palmtop are some of the newer technologies computers which are used extensively by people.
- A computer collects processes, stores and outputs information Input Device are the peripherals which lets us to communicate with a computer. A keyboard, mouse, and joystick are input devices. Storage Devices are used to place information on a storage media. A floppy drive, recordable CD-ROM, tape drives and DVD-ROM are considered storage devices
- CPU is the abbreviation for ***c**entral **p**rocessing **u**nit*. Sometimes referred to simply as the *central processor*, but more commonly called *processor,* the CPU is the brains of the computer where most calculations take place. In terms of computing power, the CPU is the most important element of a computer system.
- Processor / CPU - Central Processing Unit is the main chip in a computer. The CPU processes instructions, manages the flow of information through a computer system. The CPU communicates with input, output and storage devices to perform tasks.
- Output device lets a computer communicate with us. These devices displays information on a screen, printed copies, or generate sound. Examples of output devices are printer, scanner, plotters, monitors etc.
- Byte refers to one character; a character can be a number, a letter or symbol. Consists of eight bits. Bit - The smallest unit of information a computer can process. Kilobyte (K)- One kilobyte = 1024 characters. This is approximately equal to one page of double spaced text. Megabyte (MB) - One Megabyte = 1,048,576 character. This is approximately equal to one book. Gigabyte (GB) - One Gigabyte = 1,073,741,824 characters. This is approximately equal to a shelf of books in a library. Terabyte (TB) - One terabyte = 1,099,511,627,776 character. This is equal to an entire library of books.

- Hard Drive is the primary device that a computer uses to store information. RAM Temporarily stores information inside a computer. This information is lost when you turn off the computer.
- Motherboard/System board - The main circuit board of a computer. All electrical components plug into the mother board.
- Port – It is a connector at the back of a computer where you plug in an external device such as printer or modem. This allows instructions and data to flow between the computer and the device. Parallel Port - has 25 holes. This type of port is known as a female connector. A parallel port connects a printer or tape drive. Serial Port - has either 9 or 25 pins. This type of port is known as a male connector. A serial port connects a mouse or modem. USB Port - Universal Serial Bus - allows you connect up to 127 devices using on one port.
- MONITOR and VIDEO CARD A monitor and video card work together to display text and images on the screen. Video card - a circuit board that plugs into and expansion slot inside the computer. The video card translates instructions from the computer to a form the monitor can understand. Also called the video adaptor, graphics board or graphics card.

SELF-TEST QUESTIONS

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. What do you mean by a computer system? Explain the basic functions of a computer system.
2. What are the difference types of computers? Explain the difference between Analog and Digital computers?
3. Classify the computers on the basis of generations
4. Classify the computers on the basis of size
5. What do you mean by Super computers? Explain the difference between Super computer and main frame computers.
6. What is the difference between a work station and person computers? Explain.
7. What do you mean by Central Processing unit (C.P.U)? Explain the functions of C.P.U in details.
8. Explain about four input devices of a computer.
9. Explain about four output devices of a computers
10. What are the storage devices being used in a computers?
11. What do you mean by “Cache Memory”? Explain its basic functions.
12. What do you mean by RAM and ROM? Explain the difference between RAM and ROM.

SHORT QUESTIONS AND MCQS

1. The TV type of screen is called a _____.
2. Which of the following best characterizes the first generation of computing?
   (a) Emphasis on marketing computers to business
   (b) Computers used for mainly scientific calculations.
   (c) Speeds in microseconds (millionth/sec)
   (d) Software is an emphasis

3. Which of the following is not a printer?
   (a) Laser (c) scanner
   (b) Dot matrix (d) Ink-Jet
4. The component of the computer that would best be characterized as a traffic cop is
   (a) Central processing unit (c) Motherboard
   (b) Data Bus (d) RAM
5. The component of the computer that is responsible for temporary storage of information is known as
   (a) Central processing unit (c) Motherboard
   (b) Data Bus (d) RAM
6. What is the basic unit of composition of an image on a screen called?
   (a) Resolution (c) Video Card
   (b) Pixel (d) Bit
7. Which of the following has the least capability to computers?
   (a) Floppy Disk (c) CD-WR
   (b) Hard Disk (d) Zip Disk
8. All the following are input devices except:
   (a) Keyboard (c) Mouse
   (b) Voice Activated Devices (d) Printer
9. PC stands for _____ _____.
10. What was the first name of the two co-founders of Apple?
    (a) Bill (c) Steve
    (b) Paul (d) Heraldo

Lesson 4
Computer Software – An Overview

LESSON OUTLINE

- Computer Software: An Introduction,
- System Software
- Application Software
- Firmware
- Software Trends
- Multi-Programming,
- Multi-Processing,
- Time Sharing,
- Batch Processing
- On-Line and Real Time Processing
- Systems Securities
- Lesson Round Up
- Self Test Questions

LEARNING OBJECTIVES

Computers have become an important part of each of our's life. Basically a computer system is a combination of two parts. Hardware and Software. Hardware constitutes the physical part of a computer which one can see but the software is something which is intangible in nature. It is the set of instruction which carries out the whole processing by a computer system. In other words we may say that hardware is the body of a computer system while software is the soul of the computer. System. After going through this lesson, student would be able to –

- Understand about software and its classification
- Understand the functions of different types of software
- Understand the meaning of Multiprogramming and Multiprocessing
- Understand about time sharing, batch processing, online processing and real-time processing
- Understand about requirement of system security and different aspects relating to system security.

Computers themselves, and software yet to be developed, will revolutionize the way we learn.

Steve Jobs

COMPUTER SOFTWARE: AN INTRODUCTION

Computer cannot do anything on its own. It is the user who instructs computer; what to do, how to do and when to do. In order to perform any task, you have to give a set of instructions in a particular sequence to the computer. These sets of instructions are called Programs. ***Software refers to a set of programs that makes the hardware perform a particular set of tasks in particular order***. The process of writing (or *coding*) programs is called *programming*, and individuals who perform this task are called *programmers*.

Qualities of good Software

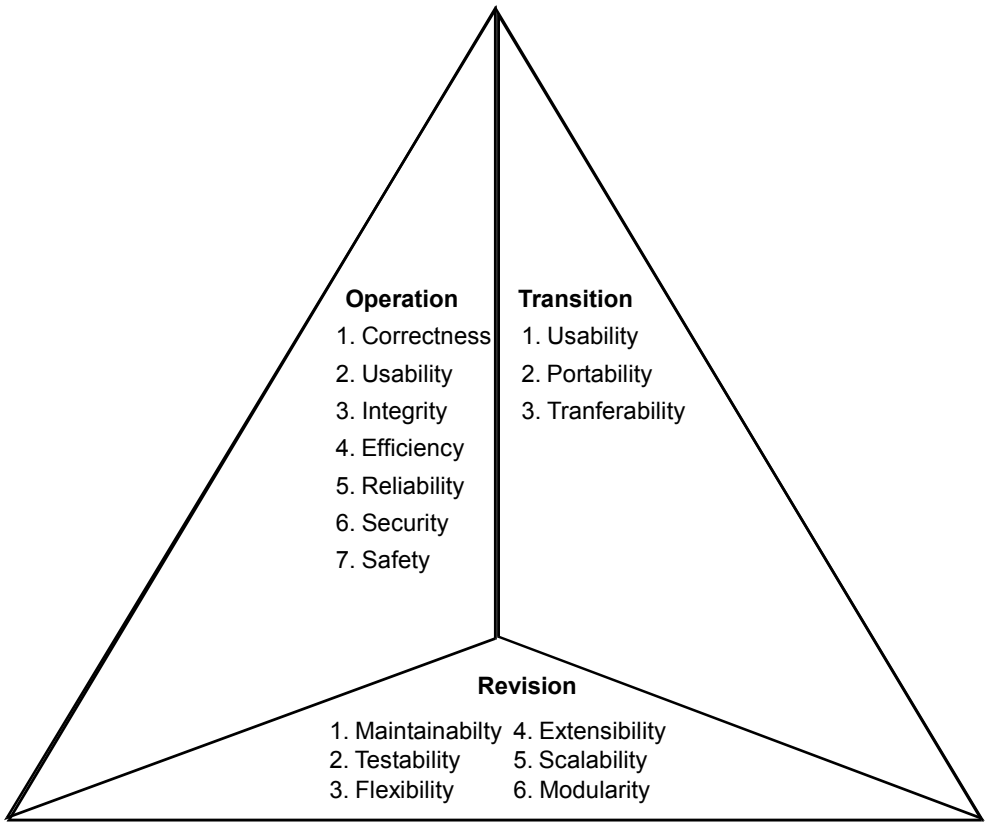
The three characteristics of good software are :-

(1) Operational Characteristics

(2) Transition Characteristics

(3) Revision Characteristics

Software Quality Triangle



Software Quality Triangle with characteristics

What Operational Characteristics should software have?

These are functionality based factors and related to 'exterior quality' of software. Various Operational Characteristics of software are:

1. **Correctness:** The software should meet all the specifications stated by the customer.

2. **Usability/Learnability:** The amount of efforts or time required to learn how to use the software should be less. This makes the software user-friendly even for IT-illiterate people.
3. **Integrity:** Software should be integrated with other applications and it should not affect the working of another application.
4. **Reliability:** The software should not have any defects. Not only this, it shouldn't fail while execution.
5. **Efficiency:** The software should make effective use of the storage space and execute command as per desired timing requirements.
6. **Security:** The software shouldn't have ill effects on data / hardware. Proper measures should be taken to keep data secure from external threats.
7. **Safety:** The software should not be hazardous to the environment/life.

Revision Characteristics of software

Various Revision Characteristics of software are:-

1. **Maintainability :** Maintenance of the software should be easy for any kind of user.
2. **Flexibility:** Changes in the software should be easy to make.
3. **Extensibility:** It should be easy to increase the functions performed by it.
4. **Scalability:** It should be very easy to upgrade it for more work (or for more number of users).
5. **Testability:** Testing the software should be easy.

Transition Characteristics of the software

1. **Interoperability:** Interoperability is the ability of software to exchange information with other applications and make use of information transparently.
2. **Reusability:** If we are able to use the software code with some modifications for different purpose then we call software to be reusable.
3. **Portability:** The ability of software to perform same functions across all environments and platforms, demonstrate its portability.

Importance of any of these factors varies from application to application.

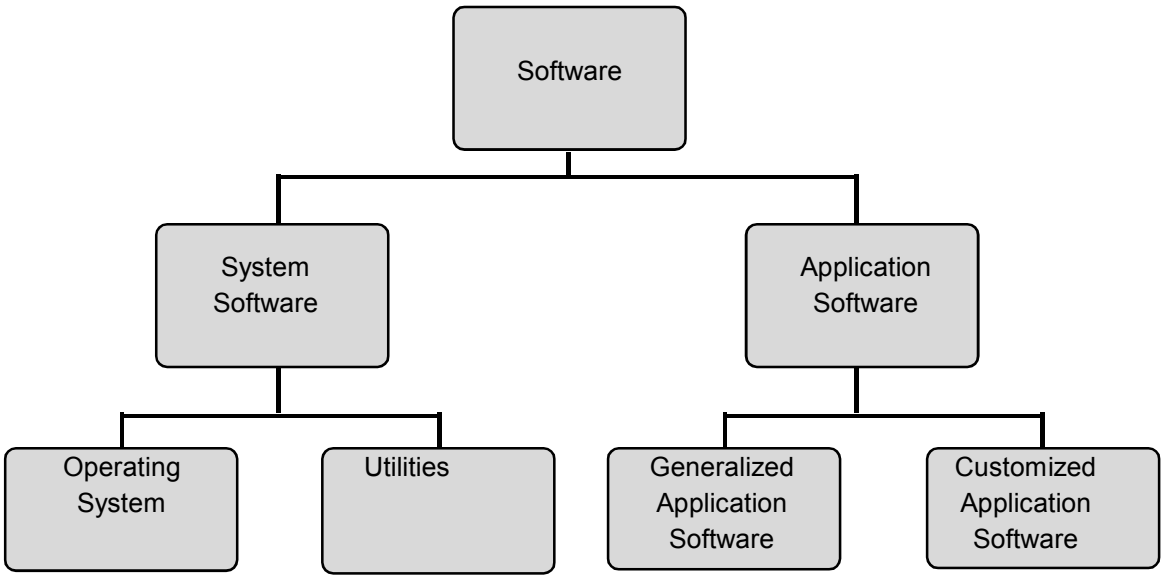
DIFFERENCE BETWEEN HARDWARE AND SOFTWARE

Basis of Difference	Hardware	Software
Examples:	CD-ROM, monitor, printer, video card, scanners, label makers, routers, and modems.	QuickBooks, Adobe Acrobat, Internet Explorer, Microsoft Word , Microsoft Excel
Types:	Input, storage, processing, control, and output devices.	System software, Programming software, and Application software.
Interdependency:	Hardware starts functioning once software is loaded.	To deliver its set of instructions, Software is installed on hardware.
Function:	Hardware serves as the delivery system for software solutions. The hardware of a computer is infrequently changed, in comparison with software	To perform the specific task you need to complete. Software is generally not needed to for the hardware to perform its basic level tasks such as turning on and responding to input.

	and data, which are "soft" in the sense that they are readily created, modified, or erased on the computer	
Reliability:	Hardware stays at steady reliability level in useful life.	Software needs constant testing after upgrades.
Failure:	Hardware failure is random. Hardware does have increasing failure at the last stage.	Software failure is systematic. Software does not have an increasing failure rate.
Fault:	Hardware faults are physical.	Software faults are not.
Lifetime:	Hardware wears out over time.	Software does not wear out over time.
Nature:	It is physical in nature	It is logical in nature
Definition:	Devices required to store and execute (or run) the software.	Collection of instructions that enables a user to interact with the computer. Software is a program that enables a computer to perform a specific task, as opposed to the physical components of the system (hardware).
Simple small definition:	Anything which we can see when the computer is off is hardware.	Anything which we can see on the screen when the computer is on is software.

CLASSIFICATION OF SOFTWARE

Software can be classified mainly into following categories



SYSTEM SOFTWARE

System software is a program that manages and supports the computer resources and operations of a computer system while it executes various tasks such as processing data and information, controlling hardware components, and allowing users to use application software. That is, systems software functions as a *bridge* between computer system hardware and the application software. System software is made up of many control programs, including the operating system, communications software and database manager.

Three Kinds of Programs

Systems software consists of three kind of programs –

(a) The system management programs,

(b) system support programs,

(c) system development programs.

(a) System Management Programs

These are programs that manage the application software, computer hardware, and data resources of the computer system. These programs include operating systems, operating environment programs, database management programs, and telecommunications monitor programs. Among these, the most important system management programs are operating systems. The operating systems are needed to study more details. There are two reasons. First, users need to know their functions first. For the second, there are many kinds of operating systems available today.

Telecommunications monitor programs are additions of the operating systems of microcomputers. These programs provide the extra logic for the computer system to control a class of communications devices.

(b) System Support Programs

These are the programs that help the operations and management of a computer system. They provide a variety of support services to let the computer hardware and other system programs run efficiently. The major system support programs are system utility programs, system performance monitor programs, and system security monitor programs (virus checking programs).

(c) System Development Programs

These are programs that help users develop information system programs and prepare user programs for computer processing. These programs may analyze and design systems and program itself. The main system development programs are programming language translators, programming environment programs, computer-aided software engineering packages.

TYPES OF SYSTEM SOFWARE

1. OPERATING SYSTEMS

An operating system is a collection of integrated computer programs that provide recurring services to other programs or to the user of a computer. These services consist of process management, disk and file management, memory management, error handling, system accounting and device management. In other words, it manages CPU operations, input/output activities, storage resources, diverse support services, and controls various devices.

Operating system is the most important program for computer system. Without an operating system, every computer program would have to contain instructions telling the hardware each step the hardware should take to do its job, such as storing a file on a disk. Because the operating system contains these instructions, any program can call on the operating system when a service is needed. Operating system acts as an interface between user and handware.

Need to Study Operating System?

There are many different computer systems and several available operating systems. Thus, users must know what each operating system can do and cannot do to meet their necessity. Today, many operating systems are used for general use or sometimes for specific use. Then, which one is best for a specific purpose? This is the main reason that users need to study Operating system.

The predominant microcomputer operating system for IBM and IBM-compatibles so far was DOS (Disk Operating System). It has different versions including MS-DOS, PC-DOS and others. DOS is very popular and wide spread, but it has some limitations. Users need to learn DOS although it may fade out in a few years and has some weakness, because it will be used for the next several years. The other popular operating system was the Apple Macintosh operating system.

As more powerful microcomputers become common place, more advanced operating systems are needed. Microcomputer users are beginning to demand more powerful operating system that can run powerful microcomputers more efficiently. Today's very powerful microcomputers are demanding more complex and refined operating system that can do multifunction. They also ask an easier user interface than old operating systems did. Now, there are more than six popular operating systems, leading to the lack of a standard. The other reason that operating system should be learned is here.

Operating System Functions

An operating system executes many functions to operate computer system efficiently. Among them, four essential functions are the followings.

- **Resource Management:** An operating system manages a collection of computer hardware resources by using a variety of programs. It manages computer system resources, including its CPU, primary memory, *virtual memory*, secondary storage devices, input/output peripherals, and other devices.
- **Task Management:** The function of the operating system that controls the running of many tasks. It manages one program or many programs within a computer system simultaneously. That is, this function of operating system manages the completion of users' tasks. A task management program in an operating system provides each task and interrupts the CPU operations to manage tasks efficiently. Task management may involve a *multitasking* capability.
- **Memory Management:** through this operating system keeps track of all the memory locations whether they are free or allocated. It also determines how and how much memory needs to be allocated to a process so that it can be executed smoothly. It also manages the allocation and deallocation of memory when operating system is handling multiple processes at a time.
- **File management:** This is a function that manages data files. An operating system contains file management programs that provide the ability to create, delete, enter, change, ask, and access of files of data. They also produce reports on a file.
- **User Interface:** It is a function of an operating system that allows users to interact with a computer. A user interface program may include a combination of menus, screen design, keyboard commands. A well-designed user interface is essential for an operating system to be popular. Because of the function, users can load programs, access files, and accomplish other tasks.

Examples of Operating Systems

The most popular operating systems are DOS, Windows, Macintosh System, Linux, Android and UNIX.

- Windows XP Professional Edition - A version used by many businesses on workstations. It has the ability to become a member of a corporate domain.
- Windows XP Home Edition - A lower cost version of Windows XP which is for home use only and should not be used at a business.
- Windows 2000 - A better version of the Windows NT operating system which works well both at home and as a workstation at a business. It includes technologies which allow hardware to be automatically detected and other enhancements over Windows NT.
- Windows ME - A upgraded version from windows 98 but it has been historically plagued with programming errors which may be frustrating for home users.

- Windows 98 - This was produced in two main versions. The first Windows 98 version was plagued with programming errors but the Windows 98 Second Edition which came out later was much better with many errors resolved.
- Windows NT - A version of Windows made specifically for businesses offering better control over workstation capabilities to help network administrators.
- Windows 95 - The first version of Windows after the older Windows 3.x versions offering a better interface and better library functions for programs.

Android

Android is a Linux-based operating system designed primarily for touch screen mobile devices such as smart phones and tablet computers. Android was unveiled in 2007 along with the founding of the Open Handset Alliance: a consortium of hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices. The first Android-powered phone was sold in October 2008.

Android is open source and Google releases the code under the Apache License This open source code and permissive licensing allows the software to be freely modified and distributed by device manufacturers, wireless carriers and enthusiast developers. Additionally, Android has a large community of developers writing applications ("apps") that extend the functionality of devices, written primarily in a customized version of the Java programming language.

Unix

Unix is a multiuser and time sharing operating system, which offers best resource utilization and sharing.

2. UTILITY SOFTWARE

Utility software is system software designed to help analyze, configure, optimize or maintain a computer. Utility software usually focuses on *how* the computer infrastructure (including the computer hardware, operating system, application software and data storage) operates. Due to this focus, utilities are often rather technical and targeted at people with an advanced level of computer knowledge - in contrast to application software, which allows users to do things like creating text documents, playing video games, listening to music or viewing websites.

Utility software categories

1. Antivirus

A computer virus is malicious code that has the ability to duplicate and send copies of itself to other computers throughout the internet. Viruses can alter, corrupt and delete files, freeze your computer and interfere with computer operation. Antivirus software protects your computer from virus threats, including worms, trojans, spyware, adware, phishing, pharming and greyware.

Antivirus software is a computer program which detects, prevents and takes action to disarm or remove malicious software, such as viruses and worms, from a computer.

A quality antivirus program such as Kaspersky Anti-Virus 2011, gives your computer virus protection and shields your PC from other malware by automatically scanning suspicious files, websites and e-mails

2. Data Clean up

Disk Cleanup is a system utility which allows scanning the entire hard drive to search for extra room by deleting any unnecessary files such as temporary files from the Internet and cookies. It also allows for deleting Restore Points, uninstalling programs, removing Windows components, and compressing old files all in the click of a mouse.

3. Disk Defragmenter

The Disk Defragmenter is another system utility which is used to reassemble fragmented files. Whenever a

file is modified in any way, the computer stores the file in broken pieces across the hard drive rather than putting the whole file in one spot. This can lead to system malfunction and poor performance because the computer must search for all the pieces of a specific file before it can display it. The Disk Defragmenter searches for all pieces of every file on your hard drive and reassembles the files into a specific location. This increases the speed at which files are displayed and results in less delay when opening files or programs.

4. System Restore

System Restore is a system utility that allows returning the computer to an earlier time in which it had not encountered an error. System Restore is great for fixing problems that a virus has caused after using antivirus software to rid the computer of the malware. System Restore allows to manually setting Restore Points on a calendar and also automatically creates Restore Points on a regular basis as well as right before the computer goes through any major change such as installing a new program.

5. Disk Compression and Archivers

Disk compression is a system utility that allows for a program to search the hard drive and compress files, particularly old or unused files. This greatly improves the computer's functionality and performance because it does not have to keep track of so many files at once. It also serves to free up space, which is the main function of disk compression software. Archivers, another form of file compression software, allow compressing a file or folder and then decompressing the file whenever you decide to. The most popular archiver to date is Winrar, which is named after Winzip but has no affiliation. Both Winrar and a plethora of disk compression programs are available on the Internet at no charge.

6. Registry Cleaners

Registry cleaners are programs that allow scanning the computer for any errors in the registry, which is a collection of the core computer files that are essential to performance and functionality, and repairs them if needed. Registry cleaners are widely available on the Internet and give a significant upper hand when cleaning up the mess that a virus or other malware has left on the computer. Likewise, some otherwise safe programs can cause errors in the registry without intending to. Registry files can also be corrupted if the user unknowingly deletes or modifies a file in the registry. This usually occurs when an inexperienced user tries to fix their computer and inevitably causes more damage than before.

7. File Splitters

File splitters are programs that allow to break a file into smaller pieces in order to store or send files. File splitters often come in handy because many online storage services, including email attachments, limit you to a specific file size that can be transferred at one time even though files often exceed these limits. File splitters allow to break the file into two or more pieces, send them simultaneously, and then piece them back together when you are ready to use the file again. A good file splitter is File Splitz. It allows for to break a file of any size into multiple pieces and then rejoin the files together just as easily.

8. Archivers output a stream or a single file when provided with a directory or a set of files. Archive utilities, unlike archive suites, usually do not include compression or encryption capabilities. Some archive utilities may even have a separate un-archive utility for the reverse operation.

9. Backup software are the system utilities that make copies of all information stored on a disk and restore either the entire disk (e.g. in an event of disk failure) or selected files (e.g. in an event of accidental deletion).

10. A clipboard manager expands the clipboard functionality of an operating system and adds functionality to an operating system's clipboard. Many clipboards provide only one buffer, overwritten by each new "copy"

operation. The main task of a clipboard manager is to store data copied to the clipboard in a way that permits richer use of the data. Clipboard managers enhance the basic functions of cut, copy, and paste operations with one or more of the following features:

1. Multiple buffers and the ability to merge, split, and edit their contents
2. Selecting which buffer "cut" or "copy" operations should store data in
3. Selecting which buffer(s) "paste" operations should take data from
4. Handling formatted text, tabular data, data objects, media content, and URLs
5. Saving copied data to long term storage
6. Indexing or tagging of clipped data
7. Searching of saved data

11. Cryptographic utilities provide command-line tools for code signing, signature verification, and other cryptography tasks.

12. Data compression utilities output a shorter stream or a smaller file when provided with a stream or file.

13. Data synchronization utilities establish consistency among data from a source to target data storage and vice versa. There are several branches of this type of utility:

(a) File synchronization utilities maintain consistency between two sources. They may be used to create redundancy or backup copies but are also used to help users carry their digital music, photos and video in their mobile devices.

(**b) Revision control** utilities are intended to deal with situations where more than one user attempts to simultaneously modify the same file.

14. Disk partitions can divide an individual drive into multiple logical drives, each with its own file system which can be mounted by the operating system and treated as an individual drive.

15. Disk space analyzers for the visualization of disk space usage by getting the size for each folder (including sub folders) & files in folder or drive. showing the distribution of the used space.

16. File managers provide a convenient method of performing routine data management tasks, such as deleting, renaming, cataloging, uncataloging, moving, copying, merging, generating and modifying data sets.

17. Hex editors directly modify the text or data of a file. These files could be data or an actual program.

18. Network utilities analyze the computer's network connectivity, configure network settings, check data transfer or log events.

19. Screensavers were desired to prevent phosphor burn-in on CRT and plasma computer monitors by blanking the screen or filling it with moving images or patterns when the computer is not in use. Contemporary screensavers are used primarily for entertainment or security.

20. System monitors for monitoring resources and performance in a computer system.

21. System profilers provide detailed information about the software installed and hardware attached to the computer.

APPLICATION SOFTWARE

Application software consists of Programs that direct computers to perform specific information processing activities for end users. These programs are called application packages because they direct the processing required for a particular use, or application, which users want to accomplish.

KINDS OF APPLICATION SOFTWARE

Application software includes a variety of programs that can be subdivided into general-purpose and application-specific categories.

General-Purpose Application Programs

General-purpose applications packages are programs that perform common information processing hobs for end users. For example, word processing programs, electronic spreadsheet programs, database management programs, graphics programs, communications programs, and integrated packages are popular with microcomputer users for home, education, business, scientific, and many other general purposes.

Application-Specific Software

Many application programs are available to support specific applications of end users. *Business Application Programs*: Programs that accomplish the information processing tasks of important business functions or industry requirements.

Scientific Application Programs: Programs that perform information processing tasks for the natural, physical, social, and behavioral sciences, engineering and all other areas involved in scientific research, experimentation, and development. There are so many other application areas such as education, music, art, medicine, etc.

APPLICATION SOFTWARE TRENDS

The trend in computer application software is toward multipurpose, expert-assisted packages with natural language and graphical user interfaces. There are two major trends:

Off-The-Shelf Software Packages

There is a trend away from custom-designed one-of- a-kind programs developed by the professional programmers or end users of an organization.

Instead, the trend is toward the use of the "*off-the-self*" software package acquired by end users from software vendors. "*off-the-self*" software refers to the software package developed by the software companies for the end users. This software is inexpensive in nature and is ready to use. This trend accelerated with the development of *inexpensive* and *easy-to-use* productivity software packages for microcomputers, and it continues to grow.

Nonprocedural, Natural Languages

There is a major trend away from technical, machine-specific programming languages using binary-based or symbolic codes and from procedural languages, which use English-like statements and mathematical expressions to specify the sequence of instructions a computer must perform.

Instead, the trend is toward nonprocedural, natural languages that are closer to human conversation. This trend has accelerated with the creation of easy-to-use, nonprocedural *fourth- generation languages* (4GL). It continues to grow as developments in graphics and artificial intelligence produce natural language and *graphical interfaces* that make software packages easier to use.

EXAMPLES OF SOME APPLICATION SOFTWARE

1. Word Processing Software: Allows users to create, edit a document. Example: MS Word, Word Pad etc.

2. Spreadsheet Software: Allows users to create document and perform calculation. Example: Excel, Lotus1-2-3 etc.

3. Database Software: Allows users to store and retrieve vast amount of data. Example: MS Access, MySQL, Oracle etc.

4. Presentation Graphic Software: Allows users to create visual presentation. Example: MS Power Point

5. Multimedia Software: Allows users to create image, audio, video etc. Example: Real Player, Media Player etc.

6. Accounting Software: Allows users to do the accounting of the transaction entered into. Examples Tally, busy, etc

7. Mobile software: Allows users to carry out various applications through mobile. Examples opera mini, ebuddy etc.

Difference between System Software and Application Software

1. System software gets installed when the operating system is installed on the computer while application software is installed according to the requirements of the user.

2. System software includes programs such as compilers, debuggers, drivers, assemblers while application software includes media players, word processors, and spreadsheet programs.

3. Generally, users do not interact with system software as it works in the background whereas users interact with application software while doing different activities.

4. A computer may not require more than one type of system software while there may be a number of application software programs installed on the computer at the same time.

5. System software can run independently of the application software while application software cannot run without the presence of the system software.

SPECIAL SYSTEM SOFTWARE

Firmware

Firmware is a combination of software and hardware. Computer chips that have data or programs recorded on them are firmware. These chips commonly include the following:

- ROMs (read-only memory)
- PROMs (programmable read-only memory)
- EPROMs (erasable programmable read-only memory)

In electronic systems and computing, **firmware** is the combination of persistent memory and program code and data stored in it. The data which is stored in chip is used to boot the computer after power on and load the operating system from hard disk to main memory. This process is called as *booting* and sometime firmware is called as *bootstrap loader.* Typical examples of devices containing firmware are embedded systems (such as traffic lights, consumer appliances, and digital watches), computers, computer peripherals, mobile phones, and digital cameras. The firmware contained in these devices provides the control program for the device. Firmware is held in non-volatile memory devices such as ROM, EPROM, or flash memory. Changing the firmware of a device may rarely or never be done during its economic lifetime; some firmware memory devices are permanently installed and cannot be changed after manufacture. Common reasons for updating firmware include fixing bugs or adding features to the device. This may require physically changing ROM integrated circuits or reprogramming flash memory with a special procedure. Firmware such as the ROM BIOS of a personal computer may contain only elementary basic functions of a device and may only provide services to higher-level software. Firmware such as the program of an embedded system may be the only program that will run on the system and provide all of its functions.

SOFTWARE TRENDS

In the era of change, software technology has also been seeing changes. Recently following changes have emerged in software technologies.

Agile Software development

Systems are becoming increasingly reliant on software due to needs for rapid fielding of interoperability, net-centricity, and rapid adaptation to change. The need for rapid adaptation and releases led to increased interest in agile methods of software development.

Agile methods break tasks into small increments with minimal planning and do not directly involve long-term planning. Iterations are short time frames (time boxes) that typically last from one to four weeks. Each iteration involves a team working through a full software development cycle, including planning, requirements analysis, design, coding, unit testing, and acceptance testing when a working product is demonstrated to stakeholders. This minimizes overall risk and allows the project to adapt to changes quickly. Stakeholders produce documentation as required. Iteration might not add enough functionality to warrant a market release, but the goal is to have an available release (with minimal bugs) at the end of iteration. Multiple iterations might be required to release a product or new features.

Team is usually cross-functional and self-organizing and members take responsibility for tasks that deliver the functionality iteration requires. They decide individually how to meet iteration's requirements.

Agile methods emphasize face-to-face communication over written documents when the team is all in the same location. Team size is typically small (5-9 people) to simplify team communication and team collaboration. Larger development efforts can be delivered by multiple teams working toward a common goal or on different parts of an effort. This might require a coordination of priorities across teams.

In team meetings team members report to each other what they did the previous day, what they intend to do today, and what their roadblocks are. This face-to-face communication exposes problems as they arise. Agile development emphasizes working software as the primary measure of progress. This, combined with the preference for face-to-face communication, produces less written documentation than other methods. The agile method encourages stakeholders to prioritize "wants" with other iteration outcomes, based exclusively on business value perceived at the beginning of the iteration

Real Analytics

Many organizations began to see information automation outweigh business process automation as their highest priority area. Analytics offer improved visibility to drive operational efficiencies, as well as a platform for growth by addressing heart-of the-business questions that could guide decisions, yield new insights and help predict the future of business. Leading organizations are launching broad initiatives with executive-level sponsorship, ready and eager to achieve their vision via real analytics. Due to exploding data volumes and regulators demands deeper insight into risks, exposure and public responsiveness are much needed.

By investing in a balance of information management, performance management and advanced analytics, organizations can make small steps, smartly made to capture measurable results. Real analytics can provide knowledge, fact-based predictions and business prescriptions if applied to the right problems, and if the suggestions based on results are pushed into action.

Applied Mobility

In today's age of technology what really matter is harnessing available networks, form factor, user interface and raw device computing power to create rich yet simple and intuitive apps to solve real business problems. These solutions can be as simple as placing a mobile layer over existing offerings and business processes which conducts business as usual, but through channels independent of physical locations. These new mobile solutions serve the full spectrum of transactional, analytical and social computing capabilities that are having different design and deployment concepts which is more focused in scope and simple in execution from user perspective compared to multipurpose feature-rich enterprise applications.

The Mobile applications are essentially powerful that they are elegant solutions to well-defined problems, and designed for operations on-the-go. Companies are rethinking business processes and enabling new business models that would not have been possible without mobile technology. Evolutions in location-based services, social networks, mobile payment processing, low-cost device add-ons and integration with enterprise systems has led to the potential for employees, customers and suppliers to consume and produce sophisticated information, goods and services from anywhere. And with the extension of mobile solutions to sensors and actuators in physical goods and equipment, otherwise known as asset intelligence there is the potential for almost anything to become part of the mobile solution footprint.

Capability Clouds

Capability clouds move beyond the building blocks of capacity to deliver finished services that directly address business objectives and enterprise goals. Instead of dealing with machine images or database instances, the discussion shifts to the analytics cloud, the testing cloud or the sales cloud and help to focus on a more important set of values. Also with the advent of capability clouds helps focusing on accelerating time-to-results, adding new functionality or changing business processes and business models rather than cost of ownership and efficiency issues. It is relatively easy for a business unit leader to buy a software-as-a-service tool for point solutions such as workforce planning or compensation management; the main requirement is simply a corporate credit card.

There have been three main drivers of cloud adoption thus far: a preference for operating expense over capital expense; speed to solution; and flexible, scalable access to specialized resources – be they technology, software or people. The capability cloud can add opportunities for agility and innovation in how business processes even business models are acquired composed and revised. For an example the analytics cloud may go beyond just delivering analytics databases, models and tools and offer PHD-level statisticians applying the art of the science where you only pay for the level of service that is needed.

Social Computing

Everyone has started going online for their daily needs and hence we are leaving the trails our opinion, behavior and choices. The data of traces created when mined would provide business with a good source of insight on

market positioning, consumer sentiment and employee productivity. By performing analytical operation on the data organizations can better understand their customer needs, preferences, their employee's experiences and problems that require immediate co-corporate attention. With the help of Social computing Businesses are able to take a results oriented and business-led approach, focusing on specific issues and communities, soliciting membership and creating platforms for content, collaboration and transactional support. Now the companies are on the job to develop software for social computing.

TYPES OF PROCESSING

Multiprogramming and Multiprocessing

Multiprogramming is a 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.

Several jobs are placed in the main memory and the processor is switched from job to job as needed to keep several jobs advancing while keeping the peripheral devices in use. Thus It improves the CPU efficiency by increasing the CPU utilization. It keeps more than one program in the memory and when a program needs to do I/O, it starts executing another program. Thus no time is wasted and the CPU doesn't need to wait for the I/O to get completed

Multiprocessing is the coordinated 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). With the advent of parallel processing, multiprocessing is divided into symmetric multiprocessing (SMP) and massively parallel processing (MPP).

In symmetric (or "tightly coupled") multiprocessing, the processors share memory and the I/O bus or data path. A single copy of the operating system is in charge of all the processors. SMP, also known as a "shared everything" system, does not usually exceed 16 processors. In massively parallel (or "loosely coupled") processing, up to 200 or more processors can work on the same application. Each processor has its own operating system and memory, but an "interconnect" arrangement of data paths allows messages to be sent between processors. Typically, the setup for MPP is more complicated, requiring thought about how to partition a common database among processors and how to assign work among the processors. An MPP system is also known as a "shared nothing" system.

TIME SHARING

In data processing, method of operation in which multiple users with different programs interact nearly simultaneously with the central processing unit of a large-scale digital computer is termed as Time sharing. Because the central processor operates substantially faster than does most peripheral equipment, it has sufficient time to solve several discrete problems during the input/output process. Even though the central processor addresses the problem of each user in sequence, access to and retrieval from the time-sharing system seems instantaneous from the standpoint of remote terminals since the solutions are available to them the moment the problem is completely entered. Time-sharing was developed during the late 1950s and early '60s to make more efficient use of expensive processor time. Commonly used time-sharing techniques include multiprocessing, parallel operation, and multiprogramming. Also, many computer networks organized for the purpose of exchanging data and resources are centered on time-sharing systems.

BATCH PROCESSING

Batch processing is execution of a series of programs ("jobs") on a computer without manual intervention. Jobs

are set up so they can be run to completion without manual intervention. So, all input data are preselected through scripts, command-line parameters, or job control language. This is in contrast to "online" or interactive programs which prompt the user for such input. A program takes a set of data files as input, processes the data, and produces a set of output data files. This operating environment is termed as "batch processing" because the input data are collected into batches of files and are processed in batches by the program.

ONLINE PROCESSING

Online processing means users directly enter information online (usually, online, in this case, means online to a central processor, rather than its modern connotation of the Internet, but it could mean both!), it is validated and updated directly onto the master file. No new file is created in this case. Therefore, there is near immediate input process, and output. Imagine a cash dispenser transaction or booking a holiday at travel agents or over the Internet. Compared with batch processing the number of transactions will be few.

Online comes in many different flavours such as centralised, distributed, time-share etc and the choice of architecture will depend on cost, speed needed, number of users, number of transactions and time needed for a response.

REAL-TIME PROCESSING

Real time processing is usually found in systems that use computer control. This processing method is used when it is essential that the input request is dealt with quickly enough so as to be able to control an output properly. For example, the computer inside the Engine Control Unit in a car has to manage the engine at every moment based on what the driver wants to do.

Real time processing has to be programmed very carefully to ensure that no input events are missed. For example, a traffic light system is a real-time system but it only needs to process data relatively slowly. On the other hand, controlling a car engine has to deal with input events happening every thousandth of a second so a very fast computer is needed to do this -but both the traffic-light and the car engine computers are carrying out 'real-time' processing.

Examples:

- Traffic lights
- Heart rate monitoring
- Aircraft control
- Computer games
- Controlling robots

The user interface of a real-time system may use specialist input devices to provide data input.. For example, a car driver will be providing input data to the onboard computer with throttle and brake pedals. A gamer may be using a joystick or hand held control to interact with the real-time game. A traffic light system may sense the car at the lights using a buried inductive loop.

SYSTEM SECURITY

In general, the term system security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. System Security is a mechanism through which it is ensured that the organisation data and information is secured from unauthorized access

Traditionally, computer facilities have been physically protected for three reasons:

1. To prevent theft of or damage to the hardware
2. To prevent theft of or damage to the information

3. To prevent disruption of service

Strict procedures for access to the machine room are used by most organizations, and these procedures are often an organization's only obvious computer security measures. Today, however, with pervasive remote terminal access, communications, and networking, physical measures rarely provide meaningful protection for either the information or the service; only the hardware is secure. Nonetheless, most computer facilities continue to protect their physical machine far better than they do their data, even when the value of the data is several times greater than the value of the hardware.

SYSTEM SECURITY MEASURES

System security measures can be bifurcated as given below

Basic system Security measures

These *Basic System Security Measures* apply to all systems regardless of the level of their *System Classification* (see "Definitions," below). It is a baseline, which all systems must meet

1. **Password Protection:** All accounts and resources must be protected by passwords which meet the following requirements, which must be automatically enforced by the system:
   (a) Must be at least eight characters long.
   (b) Must NOT be dictionary or common slang words in any language, or be readily guessable.
   (c) Must include at least three of the following four characteristics, in any order: upper case letters, lower case letters, numbers, and special characters, such as *!@#$%^&*.
   (d) Must be changed at least once per year.
2. **Software Updates:** Systems must be configured to automatically update operating system software, server applications (webserver, mailserver, database server, etc.), client software (web browsers, mail clients, office suites, etc.), and malware protection software (antivirus, anti-spyware, etc). For *Medium* or *High Availability* systems, a plan to manually apply new updates within a documented time period is an acceptable alternative.
3. **Firewall:** Systems must be protected by a firewall that allows only those incoming connections necessary to fulfill the business need of that system. Client systems which have no business need to provide network services must deny all incoming connections. Systems that provide network services must limit access to those services to the smallest reasonably manageable group of hosts that need to reach them.
4. **Malware Protection:** Systems running Microsoft or Apple operating systems must have antivirus and anti-spyware software installed and it must be configured to automatically scan and update.

Intermediate System Security Measures

These *Intermediate System Security Measures* define the security measures that must be applied to *Medium Criticality* and *High Criticality* systems. Note that except under special circumstances, they do not apply to desktop and laptop computers. The requirements are:

1. Authentication and Authorization

(a) Remove or disable accounts upon loss of eligibility: Accounts which are no longer needed must be disabled in a timely fashion using an automated or documented procedure.

(b) Separate user and administrator accounts: Administrator accounts must not be used for non-administrative purposes. System administrators must be provisioned with non-administrator accounts

for end-user activities, and a separate administrator account that is used only for system-administration purposes.

(c) Use unique passwords for administrator accounts: Privileged accounts must use unique passwords that are not shared among multiple systems. Credentials which are managed centrally, such as the NetID/password combination, are considered a single account, regardless of how many systems they provide access to.

(d) Throttle repeated unsuccessful login-attempts: A maximum rate for unsuccessful login attempts must be enforced. Account lockout is not required, but the rate of unsuccessful logins must be limited.

(e) Enable session timeout: Sessions must be locked or closed after some reasonable period.

(f) Enforce least privilege: Non-administrative accounts must be used whenever possible. User accounts and server processes must be granted the least-possible level of privilege that allows them to perform their function.

2. Audit and Accountability

(a) Synchronize system clock: The system clock must be synchronized to an authoritative time server run by NYU (currently tick.nyu.edu and tock.nyu.edu) at least once per day.

(b) Enable system logging and auditing: The facilities required to automatically generate, retain, and expire system logs must be enabled.

(c) Follow an appropriate log retention schedule: System logs must be retained for 30-90 days and then destroyed unless further retention is necessary due to legal, regulatory, or contractual requirements.

(d) Audit successful logins: Generate a log message whenever a user successfully logs in.

(e) Audit failed login attempts: Generate a log message whenever a user attempts to log in without success.

(f) Audit when a system service is started or stopped: Generate a log message when a system service is started or stopped.

(g) Audit serious or unusual errors: Generate a log message when a serious or unusual error occurs, such as crashes.

(h) Audit resource exhaustion errors: Generate a log message when a resource exhaustion error occurs, such as an out-of-memory error or an out-of-disk error.

(i) Audit failed access attempts: Generate a log message when an attempt to access a file or resource is denied due to insufficient privilege.

(j) Audit permissions changes: Generate a log message when the permissions of a user or group are changed.

(k) Include appropriate correlation data in audit events: For each audit event logged be sure to include sufficient information to investigate the event, including related IP address, timestamp, hostname, username, application name, and/or other details as appropriate.

3. Configuration and Maintenance

(a) Security partitioning: Systems may share hardware and resources only with other systems that have similar security requirements, regardless of their *Criticality* classification. Systems which share similar security requirements have user communities of similar size and character, similar firewall profiles, and similar technical requirements. For example:

(i) Multiple systems of the same *Criticality* may be aggregated together to share hardware and resources provided they have similar security requirements.

(ii) *Medium Criticality* systems may share hardware and resources with *Low Criticality* systems provided that all systems meet these *Intermediate Systems Security Measures*, and share similar security requirements.

(b) Follow vendor hardening guidelines: This document cannot be comprehensive for all systems available. Follow basic vendor recommendations to harden and secure systems.

(c) Disable vendor default accounts and passwords: Many systems come with default accounts which are publicly known. These accounts should be disabled.

(d) Disable all unnecessary network services: Processes and services which are not necessary to complete the function of a system must be disabled.

4. Additional Requirements

(a) Report potential security incidents: Potential security incidents must be reported to ITS Technology Security Services: security@nyu.edu.

(b) Security review: During the design of the technical architecture, a review of the system must be requested from ITS Technology Security Services.

(c) Vulnerability assessment: Before system deployment, a vulnerability assessment must be requested from ITS Technology Security Services.

(d) Physical access: The system must reside in a locked facility, to which only authorized personnel have access.

(e) Documentation: Create and maintain documentation summarizing the business process, major system components, and network communications associated with a system.

Advanced System Security Measures

These *Advanced System Security Measures* define the security measures that must be applied to *High Criticality* systems. The requirements are:

I. Audit and Accountability

(a) Enable process auditing or accounting: Enable process auditing or accounting, which generates log information about the creation of new processes and their system activity.

(b) Audit privilege escalation or change in privilege: Generate a log message whenever a user changes their level of privilege.

(c) Audit firewall denial: Generate a log message when the host-based firewall denies a network connection.

(d) Audit all significant application events: Log all significant application events.

(e) Write audit events to a separate system: System logs must be written to a remote system in such a way that they cannot be altered by any user on the system being logged.

II. Configuration and Maintenance

(a) Follow advanced vendor security recommendations: This document cannot be comprehensive for all systems and applications available. Conform to best practices and recommendations outlined in vendor security whitepapers and documentation.

(b) Host-based and network-based firewalls: Systems must be protected by both a host-based and a network-based firewall that allows only those incoming connections necessary to fulfill the business need of that system.

(c) Configuration management process: Configuration changes must be regulated by a documented configuration and change management process.

(d) Partitioning: Systems may share hardware and resources only with other systems that have similar security requirements, regardless of their *Criticality* classification. Systems which share similar security requirements have user communities of similar size and character, similar firewall profiles, and similar technical requirements. For example:

(i) Multiple systems of the same *Criticality* may be aggregated together to share hardware and resources provided they have similar security requirements.

(ii) *High Criticality* systems may share hardware and resources with *Medium* and *Low Criticality* systems provided that all systems meet these *Advanced Systems Security Measures*, and share similar security requirements.

III. Additional Requirements

Physical access: The system must reside in a secured, managed data center.

DATA HANDLING SECURITY MEASURES

1. Requirements for Handling Confidential Data

(a) Access control: Access to confidential data must be provided on a least-privilege basis. No person or system should be given access to the data unless required by business process. In such cases where access is required, permission to use the data must be granted by the *Data Steward* (see "Definitions," below).

(b) Sharing: Confidential data may be shared among the NYU community. It may be released publicly only according to well-defined business processes, and with the permission of the data steward.

(c) Retention: Confidential data should only be stored for as long as is necessary to accomplish the documented business process.

2. Requirements for Handling Protected Data

(a) Access control: Access to *protected data* must be provided on a least-privilege basis. No person or system should be given access to the data unless required by business process. In such cases where access is required, permission to use the data must be granted by the Data Steward.

(a) Sharing: Protected data may be shared among the among University employees according to well-defined business process approved by the Data Steward. It may be released publicly only according to well-defined business processes, and with the permission of the Data Steward.

(c) Retention: Protected data should only be stored for as long as is necessary to accomplish the documented business process.

(d) Incident Notification: If there is a potential security incident that may place protected data at risk of unauthorized access, ITS Technology Security Services must be notified:

3. Requirements for Handling Restricted Data

(a) Collection: Restricted data should only be collected when all of the following conditions are met:

(i) The data is not available from another authoritative source;

(ii) The data is required by business process; and

(iii) You have permission to collect the data from the appropriate Data Steward.

(b) Access control: Individuals must be granted access to restricted data on a least-privilege basis. No person or system may access the data unless required by a documented business process. In such cases where access is required, permission to use the data must be granted by the Data Steward.

(c) Access auditing: Enable file access auditing to log access to files containing restricted data.

(d) Labeling: Portable media containing restricted data should be clearly marked.

(e) Sharing: Access to restricted data can be granted only by a Data Steward. No individual may share restricted data with another individual who has not been granted access by a Data Steward.

(f) Idle access: Devices which can be used to access *restricted data* must automatically lock after some period of inactivity, through the use of screensaver passwords, automatic logout, or similar controls.

(g) Transit encryption: Restricted data must be encrypted during transmission with a method that meets the following requirements.

(i) Cryptographic algorithm(s) are listed in FIPS 140-2 Annex A, the list of approved security functions.

(ii) Cryptographic key lengths meet best practices for length, given current computer processing capabilities.

(iii) Both the source and destination of the transmission must be verified.

(h) Storage encryption: Restricted data must be encrypted using strong, public cryptographic algorithms and reasonable key lengths given current computer processing capabilities. Keys must be stored securely, and access to them provided on a least-privilege basis (see ISO 11568 for recommendations on securing keys). If one-way hashing is used in lieu of reversible encryption, salted hashes must be used. Possible encryption scenarios are:

(i) Encrypt files containing restricted data using different keys or passwords than those used for system login.

(ii) Encrypt data stored in databases at the column-level.

(iii) In addition to file and/or database encryption, implement full-disk encryption on portable devices containing restricted data.

(i) Retention: Restricted data should only be stored for as long as is necessary to accomplish the documented business process.

(j) Destruction: When restricted data is no longer needed it should be destroyed using methods that are resistant to data recovery attempts such as cryptographic data destruction utilities, on-site physical device destruction, or NAID certified data destruction service.

(k) Incident notification: If there is a potential security incident which may place restricted data at risk of unauthorized access, ITS Technology Security Services must be notified

LESSON ROUND-UP

– Software refers to a set of programs that makes the hardware perform a particular set of tasks in particular order. The process of writing (or *coding*) programs is called *programming*, and individuals who perform this task are called *programmers*.

– Software can be classified mainly into following categories. 1. System Software 2. Application Software.

– An operating system is a collection of integrated computer programs that provide recurring services to other programs or to the user of a computer. These services consist of disk and file management, memory management, and device management. In other words, it manages CPU operations, input/output activities, storage resources, diverse support services, and controls various devices.

- Android is a Linux-based operating system designed primarily for touch screen mobile devices such as smart phones and tablet computers.
- Utility software is system software designed to help analyze, configure, optimize or maintain a computer. Utility software usually focuses on how the computer infrastructure (including the computer hardware, operating system, application software and data storage) operates
- Application software consists of Programs that direct computers to perform specific information processing activities for end users. These programs are called application packages because they direct the processing required for a particular use, or application, which users want to accomplish.
- Firmware is a combination of software and hardware. Computer chips that have data or programs recorded on them are firmware
- Multiprogramming is a 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 is the coordinated 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)
- In data processing, method of operation in which multiple users with different programs interact nearly simultaneously with the central processing unit of a large-scale digital computer is termed as Time sharing
- Batch processing is execution of a series of programs (“jobs”) on a computer without manual intervention. Jobs are set up so they can be run to completion without manual intervention. So, all input data are preselected through scripts, command-line parameters, or job control language
- Online processing means users directly enter information online (usually, online, in this case, means online to a central processor, rather than its modern connotation of the Internet, but it could mean both!), it is validated and updated directly onto the master file. No new file is created in this case. Therefore, there is near immediate input process, and output. Imagine a cash dispenser transaction or booking a holiday at travel agents or over the Internet
- Real time processing is usually found in systems that use computer control. This processing method is used when it is essential that the input request is dealt with quickly enough so as to be able to control an output properly.
- System security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. System Security is a mechanism through which it is ensured that the organisation data and information is secured from unauthorized access

SELF-TEST QUESTIONS

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. What do you mean by the term Software? Differentiate between the hardware and software of a system.
2. What are the different characteristics of software? Explain in detail.
3. What are the different types of Computer software? Explain each one in detail.

4. What do you mean by operating system? Explain about different types of operating system.
5. What are the different Functions of operating systems?
6. What do you mean by utility software? Explain about 5 popular utility software in detail.
7. What do you mean by Application software? Explain about different Application software.
8. What is the difference between Application Software and system software? Explain
9. What do you mean by multiprogramming and multiprocessing? State the difference between multiprogramming and multiprocessing.
10. What do you mean by batch processing, online processing and real-time processing? Explain the difference between online processing and real-time processing.
11. What do you mean by system security? Explain basic system securities measures.
12. Write short note on
    (a) Time sharing
    (b) Android operating system
    (c) Linux
    (d) Characteristic of strong password
    (e) Firewall
    (f) Social Computing
    (g) Agile software development technology
    (h) Firmware

Lesson 5
Database Management

LESSON OUTLINE

- Data Base Concepts
- Data Structure
- Data Base Management System
- Data Base Files
- Data Mining and Warehousing

LEARNING OBJECTIVES

A database is a collection of related files that are usually integrated, linked or cross-referenced to one another. The advantage of a database is that data and records contained in different files can be easily organized and retrieved using specialized database management software called a database management system (DBMS) or database manager.

Data base and database management system are extensively used in all fields i.e. business, research, education, governance, audit etc. Now the day is not far when database will be far ahead from software. Seeing the importance of database and DBMS, it becomes necessary for professionals like Company Secretaries to know basics concepts of data base and DBMS.

After reading this lesson, you should be able to:

- Understand the meaning of Data base, its types, advantages and disadvantages· Know about basics of data structure
- Define the term database management system (DBMS), its objectives and functions
- Understand the meaning of Data Mining and data warehouse and their uses.

The weaker the data available upon which to base one's conclusion, the greater the precision which should be quoted in order to give the data authenticity.

Norman Ralph Augustine

DATABASE MANAGEMENT

Meaning of Database

Database is a collection of information organized in such a way that a computer program can quickly select desired pieces of data. One form of Database can be an electronic filing system.

Traditional databases are organized by *fields*, *records*, and *files*. A field is a single piece of information; a record is one complete set of fields; and a file is a collection of records. For example, a telephone book is analogous to a file. It contains a list of records, each of which consists of three fields: name, address, and telephone number.

To access information from a database, you need a *database management system (DBMS)*. This is a collection of programs that enables you to enter, organize, and select data in a database.

Database is a collection of information that is organized so that it can easily be accessed, managed, and updated. In one view, databases can be classified according to types of content: bibliographic, full-text, numeric, and images.

In computing, databases are sometimes classified according to their organizational approach. The most prevalent approach is the relational database, a tabular database in which data is defined so that it can be reorganized and accessed in a number of different ways. A distributed database is one that can be dispersed or replicated among different points in a network. An object-oriented programming database is one that is congruent with the data defined in object classes and subclasses.

Computer databases typically contain aggregations of data records or files, such as sales transactions, product catalogs and inventories, and customer profiles. Typically, a database manager provides users the capabilities of controlling read/write access, specifying report generation, and analyzing usage. Databases and database managers are prevalent in large mainframe systems, but are also present in smaller distributed workstation and mid-range systems such as the AS/400 and on personal computers. SQL (Structured Query Language) is a standard language for making interactive queries from and updating a database such as IBM's DB2, Microsoft's SQL Server, and database products from Oracle, Sybase, and Computer Associates.

Characteristics of Data Base system (Differential features of database system w.r.t. file system)

There are a number of characteristics that distinguish the database approach with the file-based approach.

1. Self-Describing Nature of a Database System

A Database System contains not only the database itself but also the descriptions of data structure and constraints (meta-data). This information is used by the DBMS software or database users if needed. This separation makes a database system totally different from the traditional file-based system in which the data definition is a part of application programs.

2. Insulation between Program and Data

In the file based system; the structure of the data files is defined in the application programs so if a user wants to change the structure of a file, all the programs that access that file might need to be changed as well. On the other hand, in the database approach, the data structure is stored in the system catalog not in the programs. Therefore, one change is all that's needed.

3. Support multiple views of data

A view is a subset of the database which is defined and dedicated for particular users of the system. Multiple users in the system might have different views of the system. Each view might contain only the data of interest to a user or a group of users.

4. Sharing of data and Multiuser system

A multiuser database system must allow multiple users access to the database at the same time. As a result, the multiuser DBMS must have concurrency control strategies to ensure several users access to the same data item at the same time, and to do so in a manner that the data will always be correct – data integrity.

5. Control Data Redundancy

In the Database approach, ideally each data item is stored in only one place in the database. In some cases redundancy still exists so as to improve system performance, but such redundancy is controlled and kept to minimum.

6. Data Sharing

The integration of the whole data in an organization leads to the ability to produce more information from a given amount of data.

7. Enforcing Integrity Constraints

DBMSs should provide capabilities to define and enforce certain constraints such as data type, data uniqueness, etc.

8. Restricting Unauthorized Access

Not all users of the system have the same accessing privileges. DBMSs should provide a security subsystem to create and control the user accounts.

9. Data Independence

System data (Meta Data) descriptions are separated from the application programs. Changes to the data structure is handled by the DBMS and not embedded in the program.

10. Transaction Processing

The DBMS must include concurrency control subsystems to ensure that several users trying to update the same data do so in a controlled manner. The results of any updates to the database must maintain consistency and validity.

11. Providing multiple views of data

A view may be a subset of the database. Various users may have different views of the database itself. Users may not need to be aware of how and where the data they refer to is stored.

12. Providing backup and recovery facilities

If the computer system fails in the middle of a complex update process, the recovery subsystem is responsible for making sure that the database is restored to the stage it was in before the process started executing.

13. Managing information

Managing information means taking care of it so that it works for us, and is useful for the work we are doing. The information we collect is no longer subject to “accidental disorganization” and becomes more easily accessible and integrated with the rest of our work. Managing information using a database allows us to become strategic users of the data we have.

Examples of Database

Student

Student Name	No. of Studnet	Class	Department
Ram	17	1	CS
Shyam	8	2	CS

Course

Course Name	Course No.	Credits	Department
Introduction to CS	CS 1310	4	CS
Data Structures	CS3320	4	CS
Discrete Mathematics	MA 2410	3	MA
Database Manage itient	CS3380	3	CS

Prerequisite

Course No.	Prereq No.
CS3380	C53320
CS3380	MA2410
CS3320	CS131A

Session

Session Identity	Course No.	Semester	Year	Professor
85	MA 2410	Fall	96	A
132	CS 1310	Fall	96	B
102	CS3320	Spring	97	C
112	MA2410	Fall	97	D
119	CS1310	Fall	97	E

Grade Report

Student No.	Session Identity	Grade
17	112	14
17	119	12
8	85	16
8	92	16
8	102	14

TYPES OF DATABASES

Flat-File "Databases"

Flat-file databases are so simplest These are very common, both for basic programming storage tasks as well as highly-scalable massively multi-user Internet megasites.

Here's an example of a flat-file database for some company:

Customer	Address	Order	Shipper	Ship Date
Rubble, Barney	93 Pebble Lane, Bedrock	120459	Fedex	2006-08-21
Leela, Taronga	1 Planet Express Plaza, NNY	120788	Fedex	2006-08-23
Griffin, Stewie	31 Spooner Street, Quohog	120791-A	UPS	2006-08-23
Griffin, Stewie	31 Spooner Street, Quohog	120791-B	Fedex	2006-08-23
Leela, Taronga	1 Planet Express Plaza, NNY	120844	UPS	2006-08-24

It's pretty easy to make sense of: one order was sent to Barney, one to Stewie (but split into two for some unknown reason), and two to Leela on different days. But the main disadvantage is flat databases donot provide automatic query environment and possibility of redundancy is more.

Analytic Databases

Analytic databases (a.k.a. OLAP- On Line Analytical Processing) are primarily static, read-only databases which store archived, historical data used for analysis. For example, a company might store sales records over the last

ten years in an analytic database and use that database to analyze marketing strategies in relationship to demographics.

Operational Databases

Operational databases (a.k.a. OLTP On Line Transaction Processing), on the other hand, are used to manage more dynamic bits of data. These types of databases allow you to do more than simply view archived data. Operational databases allow you to modify that data (add, change or delete data).

These types of databases are usually used to track real-time information. For example, a company might have an operational database used to track warehouse/stock quantities. As customers order products from an online web store, an operational database can be used to keep track of how many items have been sold and when the company will need to reorder stock.

DATABASE MODELS

Besides differentiating databases according to function, databases can also be differentiated according to how they model the data.

What is a data model?

Well, essentially a data model is a "description" of both a container for data and a methodology for storing and retrieving data from that container. Actually, there isn't really a data model "thing". Data models are abstractions, oftentimes mathematical algorithms and concepts. You cannot really touch a data model. But nevertheless, they are very useful. The analysis and design of data models has been the cornerstone of the evolution of databases. As models have advanced so has database efficiency.

Types of data base models

1. *Flat model*: This may not strictly qualify as a data model. The flat (or table) model consists of a single, two-dimensional array of data elements, where all members of a given column are assumed to be similar values, and all members of a row are assumed to be related to one another.

2. A distributed database is a database in which storage devices are not all attached to a common processing unit such as the CPU, controlled by a distributed database management system (together sometimes called a distributed database system). It may be stored in multiple computers, located in the same physical location; or may be dispersed over a network of interconnected computers. Unlike parallel systems, in which the processors are tightly coupled and constitute a single database system, a distributed database system consists of loosely coupled sites that share no physical components

3. *Hierarchical model*: In this model data is organized into a tree-like structure, implying a single upward link in each record to describe the nesting, and a sort field to keep the records in a particular order in each same-level list.

4. *Network model*: This model organizes data using two fundamental constructs, called records and sets. Records contain fields, and sets define one-to-many relationships between records: one owner, many members.

5. *Relational model*: is a database model based on first-order predicate logic. Its core idea is to describe a database as a collection of predicates over a finite set of predicate variables, describing constraints on the possible values and combinations of values

6. *Object-relational model*: Similar to a relational database model, but objects, classes and inheritance are directly supported in database schemas and in the query language.

7. Star schema is the simplest style of data warehouse schema. The star schema consists of a few "fact tables" (possibly only one, justifying the name) referencing any number of "dimension tables". The star schema is considered an important special case of the snowflake schema.

Components of Database Systems

The term database system refers to an organization of components that define and regulate the collection, storage, management and use of the data within a database environment.

The database system is composed of the five major parts:

1. Hardware
2. Software
3. People
4. Procedures
5. Data

Hardware

Hardware refers to all of the system's physical devices; for example, computers microcomputers, workstations, servers and supercomputers), storage devices, printers, network devices(hubs, switches, routers, fiber optics) and other devices(automated teller machines, ID readers).

Software

Three types of software are required in data based system :

(a) *Operating System Software*: It manages all hardware components and makes it possible for other software to run on the computers. Examples of operating system software include Microsoft Windows, Linux, Mac OS and UNIX.

(b) *DBMS Software*: It manages the database within the database system. Some examples of DBMS software include Microsoft SQL Server, Oracle,MySQL and IBM DB2.

(c) *Application programs and utility software*: They are used to access and manipulate data in the DBMS and to manage the computer environment in which data access and manipulation take place. Application programs are most commonly used to access data found within the database to generate reports, tabulations and other information to facilitate decision making. Utilities are the software tools used to help manage the database system's computer components. For example, all major DBMS vendors now provide GUI to help create database structures, control database access and monitor database operations.

People

This component includes all users of the database system. On the basis of primary job functions, five types of users can be identified in a database system.

(a) *System Administrators*: They oversee the database system's general operations.

(b) *Database Administrators*: also known as DBA, manage the DBMS and ensure that the database is Functioning properly. The DBA role is sufficiently important in Database Administration and Security.

(c) *Database Designers*: They design the database structure. They are, in effect, the database architects. If the database design is poor, even the best application programmers and the most dedicated DBA cannot produce a useful database environment.

(d) *System Analysts and Programmers*: They design and implement the application programs. They design and create the data entry screens, reports and procedures through which end users access and manipulate the database's data.

(e) *End Users*: They are the people who use the application programs to run the organization's daily operations. For example, clerks, supervisors, managers, etc.

Procedures

Procedures are the instructions and rules that govern the design and use of the database system. Procedures pay an important role in a company because they enforce the standards by which business is conducted within the organization and with customers. Procedures are also used to ensure that there is an organized way to monitor and audit both the data and the information that is generated through the use of the data

Data

The word data covers the collection of facts stored in the database. Because data are the raw material from which information is generated, the determination of what data are to be entered into the database and how that data are to organized is a vital part of the database designer's job.

Elements of Databases

1. The database schema – is a structure defined by the database administrator of a Database system that refers to the organization of data. It is also called as blueprint of database system.

2. Schema objects -A schema is a collection of database objects. A schema is owned by a database user and has the same name as that user. Schema objects are logical structures created by users. Objects such as tables or indexes hold data, or can consist of a definition only, such as a view.

3. Indexes -A database index is a data structure that improves the speed of data retrieval operations on a database table at the cost of slower writes and the use of more storage space.

4. Tables- a data table is a set of data elements (values) that is organized using a model of vertical columns (which are identified by their name) and horizontal rows, the cell being the unit where a row and column intersect.

5. Fields and columns- a column is a set of data values of a particular simple type, one for each row of the table. The columns provide the structure according to which the rows are composed. Columns are also called as fields.

6. Records and rows- it is a set of fields is called as record or tuple or row.

7. Keys - a key part of a relational database and a vital part of the structure of a table. They ensure each record within a table can be uniquely identified by one or a combination of fields within the table. There are various type of keys we used like super key, candidate key, primary key etc.

8. Relationships- we create different type of entities or tables in the database but these entities should have a kind of relationship between them For instance, customers make orders, and orders contain items. There are various kind of relationships like one to one, one to many etc.

9. Data types – this is the characteristics assign to a particular field that which kind of value will it contain. Like character, integer, float etc.

DATA STRUCTURE

What is Data Structure?

In computer science, a data structure is a particular way of storing and organizing data in a computer so that it can be used efficiently. Different kinds of data structures are suited to different kinds of applications, and some are highly specialized to specific tasks. For example, B-trees are particularly well-suited for implementation of databases, while compiler implementations usually use hash tables to look up identifiers.

Data structures provide a means to manage large amounts of data efficiently, such as large databases and internet indexing services. Usually, efficient data structures are a key to designing efficient algorithms. Some formal design methods and programming languages emphasize data structures, rather than algorithms, as the key organizing factor in software design. Storing and retrieving can be carried out on data stored in both main memory and in secondary memory.

In simple words, The term *data structure* refers to a scheme for organizing related pieces of information. The basic types of data structures include:

1. files
2. lists
3. arrays
4. records
5. trees
6. tables

Each of these basic structures has many variations and allows different operations to be performed on the data.

Characteristics of data structures

1. It contains data items that can be elementary item, group item or another data structure. 2. It has a set of operations that can be performed on data items. Such as searching, insertion etc. 3. It describes the rules of how the data items are related to each other.

DATA BASE MANAGEMENT SYSTEM

DBMS Fundamentals

A database management system is a set of software programs that allows users to create, edit and update data in database files, and store and retrieve data from those database files. Data in a database can be added, deleted, changed, sorted or searched all using a DBMS. If you were an employee in a large organization, the information about you would likely be stored in different files that are linked together. One file about you would pertain to your skills and abilities, another file to your income tax status, another to your home and office address and telephone number, and another to your annual performance ratings. By cross-referencing these files, someone could change a person's address in one file and it would automatically be reflected in all the other files. DBMSs are commonly used to manage:

- Membership and subscription mailing lists
- Accounting and bookkeeping information
- The data obtained from scientific research
- Customer information
- Inventory information
- Personal records
- Library information

Types of data base management system

1. Hierarchical DBMS

A DBMS is said to be hierarchical if the relationships among data in the database are established in such a way that one data item is present as the subordinate of another one or a sub unit. Here subordinate means that items have "parent-child" relationships among them. Direct relationships exist between any two records that are stored consecutively. The data structure "tree" is followed by the DBMS to structure the database. No backward movement is possible/allowed in the hierarchical database.

2. Network DBMS

A DBMS is said to be a Network DBMS if the relationships among data in the database are of type many-to-

many. The relationships among many-to-many appear in the form of a network. Thus the structure of a network database is extremely complicated because of these many-to-many relationships in which one record can be used as a key of the entire database. A network database is structured in the form of a graph that is also a data structure. Though the structure of such a DBMS is highly complicated however it has two basic elements i.e. records and sets to designate many-to-many relationships. Mainly high-level languages such as Pascal, COBOL and FORTRAN etc. were used to implement the records and set structures.

3. Relational DBMS

A DBMS is said to be a Relational DBMS or RDBMS if the database relationships are treated in the form of a table. there are three keys on relational DBMS 1)relation 2)domain 3)attributes. *A network means it contains a fundamental constructs sets or records. sets contains one to many relationship ,records contains fields statical table that is composed of rows and columns is used to organize the database and its structure and is actually a two dimension array in the computer memory. A number of RDBMSs are available; some popular examples are Oracle, Sybase, Ingress, Informix, Microsoft SQL Server, and Microsoft Access.*

4. Object-Oriented DBMS

Able to handle many new data types, including graphics, photographs, audio, and video, object-oriented databases represent a significant advance over their other database cousins. Hierarchical and network databases are all designed to handle structured data; that is, data that fits nicely into fields, rows, and columns. They are useful for handling small snippets of information such as names, addresses, zip codes, product numbers, and any kind of statistic or number you can think of. On the other hand, an object-oriented database can be used to store data from a variety of media sources, such as photographs and text, and produce work, as output, in a multimedia format.

The Advantages of a DBMS

***1. Improved availability*:** One of the principle advantages of a DBMS is that the same information can be made available to different users.

***2. Minimized redundancy*:** The data in a DBMS is more concise because, as a general rule, the information in it appears just once. This reduces data redundancy, or in other words, the need to repeat the same data over and over again. Minimizing redundancy can therefore significantly reduce the cost of storing information on hard drives and other storage devices. In contrast, data fields are commonly repeated in multiple files when a file management system is used.

***2. Accuracy*:** Accurate, consistent, and up-to-date data is a sign of data integrity. DBMSs foster data integrity because updates and changes to the data only have to be made in one place. The chances of making a mistake are higher if you are required to change the same data in several different places than if you only have to make the change in one place.

***3. Program and file consistency*:** Using a database management system, file formats and system programs are standardized. This makes the data files easier to maintain because the same rules and guidelines apply across all types of data. The level of consistency across files and programs also makes it easier to manage data when multiple programmers are involved.

***4. User-friendly*:** Data is easier to access and manipulate with a DBMS than without it. In most cases, DBMSs also reduce the reliance of individual users on computer specialists to meet their data needs.

***5. Improved security*:** As stated earlier, DBMSs allow multiple users to access the same data resources. This capability is generally viewed as a benefit, but there are potential risks for the organization. Some sources of information should be protected or secured and only viewed by select individuals. Through the use of passwords, database management systems can be used to restrict data access to only those who should see it.

Disadvantages of DBMS

The disadvantages of the database approach are summarized as follows:

1. Complexity: The provision of the functionality that is expected of a good DBMS makes the DBMS an extremely complex piece of software. Database designers, developers, database administrators and end-users must understand this functionality to take full advantage of it. Failure to understand the system can lead to bad design decisions, which can have serious consequences for an organization.

2. Size: The complexity and breadth of functionality makes the DBMS an extremely large piece of software, occupying many megabytes of disk space and requiring substantial amounts of memory to run efficiently.

3. Performance: Typically, a File Based system is written for a specific application, such as invoicing. As result, performance is generally very good. However, the DBMS is written to be more general, to cater for many applications rather than just one. The effect is that some applications may not run as fast as they used to.

4. Higher impact of a failure: The centralization of resources increases the vulnerability of the system. Since all users and applications rely on the vailability of the DBMS, the failure of any component can bring operations to a halt.

5. Cost of DBMS: The cost of DBMS varies significantly, depending on the environment and functionality provided. There is also the recurrent annual maintenance cost.

6. Additional Hardware costs: The disk storage requirements for the DBMS and the database may necessitate the purchase of additional storage space. Furthermore, to achieve the required performance it may be necessary to purchase a larger machine, perhaps even a machine dedicated to running the DBMS. The procurement of additional hardware results in further expenditure.

7. Cost of Conversion: In some situations, the cost of the DBMS and extra hardware may be insignificant compared with the cost of converting existing applications to run on the new DBMS and hardware. This cost also includes the cost of training staff to use these new systems and possibly the employment of specialist staff to help with conversion and running of the system. This cost is one of the main reasons why some organizations feel tied to their current systems and cannot switch to modern database technology.

Senarios when DBMS should not be used

In spite of the advantages of using a DBMS, there are a few situations in which such a system may involve unnecessary overhead costs, as that would not be incurred in traditional file processing.

The overhead costs of using a DBMS are due to the following:

1. High initial investment in hardware, software, and training
2. Generality that a DBMS provides for defining and processing data
3. Overhead for providing security, concurrency control, recovery, and integrity functions.

Additional problems may arise, if the database designers and DBA do not properly design the database or if the database systems applications are not implemented properly.

Hence, it may be more desirable to use regular files under the following circumstances:

1. The database and applications are simple, well defined and not expected to change.
2. There are tight real-time requirements for some programs that may not be met because of DBMS overhead.

3. Multiple user access to data is not required.
4. An application may need to manipulate the data in a way not supported by the query language.

Requirements for a DBMS

The software responsible for the management data in computers i.e. DBMS (like Oracle, FoxPro, SQL Server etc.) should meet the following requirements:

1. Provide data definition facilities: It should support Data Definition Language (DDL) and provides user accessible catalog Known as Data Dictionary.

2. Provide facilities for storing, retrieving and updating data: It should support Data Manipulation Language (DML), so that required data can be inserted, updated, deleted and retrieved.

3. Supports multiple view of data: The end user should have the facility of flexible query language so that required information can be accessed easily.

4. Provides facilities for specifying Integrity constraints: It should support the constraints like Primary key, foreign key during creation of tables so that only the valid information is stored in the database. As soon as, we try to insert any incorrect information it should display the error message.

5. Provide security of data : It should have the facilities for controlling access to data and prevent unauthorized access and update.

6. Provide concurrency control mechanism: It should allow simultaneous access and update of data by multiple users

7. Support Transactions: It should support all the properties of transaction known as ACID properties. It means a sequence of operations to be performed as a whole. In other words all operations are performed or none.

8. Provide facilities for database recovery: It should bring database back to consistent state after a failure such as disk failure, faulty program etc.

9. Provide facilities for database maintenance: It should support maintenance operations like unload, reload, mass insertion, deletion and validation of data.

10. Master and transaction file: A master file stores relatively static data. It changes occasionally and stores all the details of the object. For example, in case of banking software the customer file which contains the data about the customer like customer id, account no, account type, name, address; phone number etc. is a master file, because it contains the static data and whole information about the customer.

The other file, which contains the data about the customer transactions, is called as a Transaction file. The customer transaction file contains the data about the account no,\ transaction_)d, date, transaction type (e.g. deposit or withdrawal), amount, balance etc. It is dynamic file and updated each time for any withdrawal and deposit on a given account number.

DATABASE ADMINISTRATOR & HIS FUNCTIONS

Database administrators (DBAs) are primarily responsible for specific databases in the subsystem. the primary responsibilities of database administrator are installation, configuration, monitoring, upgradation etc. Many tools are available to help DBAs perform their tasks.

– The DBA creates the hierarchy of data objects, beginning with the database, then table spaces, tables, and any indexes or views that are required. This person also sets up the referential integrity definitions and any necessary constraints.

- The DBA essentially implements the physical database design. Part of this involves having to do space calculations and determining how large to make the physical data sets for the table spaces and index spaces, and assigning storage groups (also called stogroups).
- The DBA can be responsible for granting authorizations to the database objects, although sometimes there is a special security administration group that does this.
- The centralization of data and control of access to this data is inherent to a database management system. One of the advantages of this centralization is the availability of consistent data to more than one application. As a consequence, this dictates tighter control of that data and its usage.
- Responsibility for an accurate implementation of control lies with the DBA. Indeed, to gain the full benefits of using a centralized database, you must have a central point of control for it. Because the actual implementation of the DBA function is dependent on a company's organization, we limit ourselves to a discussion of the roles and responsibilities of a DBA. The group fulfilling the DBA role will need experience in both application and systems programming.
- In a typical installation, the DBA is responsible for:
  - Providing the standards for, and the administration of, databases and their use
  - Guiding, reviewing, and approving the design of new databases
  - Determining the rules of access to the data and monitoring its security
  - Ensuring database integrity and availability, and monitoring the necessary activities for reorganization backup and recovery
  - Approving the operation of new programs with existing production databases, based on results of testing with test data.
- In general, the DBA is responsible for the maintenance of current information about the data in the database. Initially, this responsibility might be carried out using a manual approach. But it can be expected to grow to a scope and complexity sufficient to justify, or necessitate, the use of a data dictionary program.

The DBA is not responsible for the actual content of databases. This is the responsibility of the user. Rather, the DBA enforces procedures for accurate, complete, and timely update of the database

Database design and its importance

Database design refers to the activities that focus on the design of the database structure that will be used to store and manage end-user data. A database that meets all user requirements does not just happen; its structure must be designed carefully. Even a good DBMS will perform poorly with a badly designed database. Proper database design requires the designer to identify precisely the database expected use.

Designing a transactional database recognizes accurate and consistent data and operational speed. The design of a data warehouse database recognizes the use of historical and aggregated data. Designing a database to be in a centralized, single-user environment requires a different approach from that used in the design of a distributed, multi-user environment. A well-designed database facilities data management and generates accurate and valuable information. A poorly designed database is likely to become a breeding ground for difficult-to-trace errors that may lead to bad decision making and bad decision making can lead to the failure of an organization.

Functions of Database Management System

A DBMS performs several functions that guarantee the integrity and consistency of the data in the database. Most of these functions are transparent to the users and most can be achieved only through the use of a DBMS.

***1. Data Dictionary Management*:** The DBMS stores definitions of the data elements and their relationships

(metadata) in a data dictionary. In turn, all programs that access the data in the database work through the DBMS. The DBMS uses the data dictionary to look up the required data component structures and relationships, thus relieving the programmer from having to code such complex relationships n each program. Additionally, any changes made in a database structure are automatically recorded in the data dictionary. In other words, the DBMS provides data abstraction and it removes structural and data dependency from the system.

***2. Data Storage Management*:** The DBMS creates and manages the complex structures required for data storage, thus relieving programmer from the difficult task of defining and programming the physical data characteristics. A modern DBMS provides storage not only for the data, but also for related data entry forms or screen definitions, report definitions, data validation rules, procedural code, structures to handle video and picture formats, etc. Data storage management is also important for database performance tuning. Performance tuning relates to the activities that make the database perform more efficiently in terms of storage and access speed. Although the user sees the database as a single data storage unit, the DBMS actually stores the database in multiple physical files. Such data files may even be stored on difficult storage media. Therefore, the DBMS doesn't have to wait for one dist request to finish before the next one starts. In other words, the DBMS can fulfill the database requests concurrently.

***3. Data Transformation and Presentation*:** The DBMS transforms entered data to conform to required data structures. The DBMS formats the physically retrieved data to make it conform to the user's logical expectations. An end user in India would expect to enter data such as June 15, 2010 as 15/06/10 whereas the same date is entered in US as 06/15/10.

***4. Security Management*:** The DBMS creates a security system that enforces user security and data privacy. Security rules determine which users can access the database which data items each user can access and which data operations (read, add, delete or modify) the user can perform. This is especially important in multi-user database system. All database users may be authenticated to the DBMS through a username and password or through biometric authentication such as fingerprint scan. The DBMS uses this information to assign privileges to various database components such as queries and reports.

***5. Multi-user Access Control*:** To provide data integrity and data inconsistency, the DBMS uses sophisticated algorithms to ensure that multiple users can access the database concurrently without compromising the integrity of the database.

***6. Backup and Recovery Management*:** The DBMS provides backup and data recovery to ensure data safety and integrity. Current DBMS systems provide special utilities that allow the DBA to perform routine and special backup and restore procedures. Recovery management deals with the recovery of the database after a failure such as a bad sector in the disk or a power failure. Such capability is critical to preserving the database's integrity.

***7. Data Integrity Management*:** The DBMS promotes and enforces integrity rules, thus inimizing data redundancy and maximizing data inconsistency. The data relationships stored in the data dictionary are used to enforce data integrity. Ensuring data integrity is especially important in transaction-oriented database systems.

***8. Database Access Languages and API*:** The DBMS provides data access through a query language. A query language is a non-procedural language – one that lets the user specify what must be done without having to specify how is to be done. SQL is the query language and data access standard supported by majority of DBMS vendors. The DBMS also provides application programming interfaces to procedural languages such as COBOL, C. Java, etc. In addition, the DBMS provides administrative utilities used by the DBA and the database designer to create, implement, monitor and maintain the database.

***9. Database Communication Interface*:** Current generation DBMSs accept end-user requests via multiple, different network environments. For example, the DBMS might provide access to the database via the Internet through the use of Web browsers such as Internet Explorer, Firefox.

DATABASE LANGUAGES

A DBMS is a software package that carries out many different tasks including the provision of facilities to enable the user to access and modify information in the database. The database is an intermediate link between the physical database, computer and the operating system and the users. To provide the various facilities to different types of users, a DBMS normally provides one or more specialized programming languages called database languages.

Database languages come in different forms. They are: -

1. Data Description Language (DDL)
2. Data Manipulation Language (DML)

Data Description Language (DDL)

As the name suggests, this language is used to define the various types of data in the database and their relationship with each other.

The basic functions performed by DDL are:-

- Create tables, files, databases and data dictionaries.
- Specify the storage structure of each table on disk.
- Integrity constraints on various tables.
- Security and authorization information of each table.
- Specify the structure of each table.
- Overall design of the Database.

Data Manipulation Language (DML)

A language that enables users to access or manipulate data (retrieve, insert, update, delete) as organized by a certain Data Model is called the Data Manipulation Language (DML). It can be of two types: -

1. *Procedural DML* - It describes what data is needed and how to get it. For example: - Rela-tional Algebra.
2. *Non-Procedural DML* - It describes what data is needed without specifying how to get it. For example: - Relational calculus.

DATABASE FILE

A database file is defined as a collection of related records. A database file is sometimes called a table. A file may be composed of a complete list of individuals on a mailing list, including their addresses and telephone numbers. Files are frequently categorized by the purpose or application for which they are intended. Some common examples include mailing lists, quality control files, inventory files, or document files. Files may also be classified by the degree of permanence they have. Transition files are only temporary, while master files are much more long-lived.

At a minimum, every SQL Server database has two operating system files: a data file and a log file. Data files contain data and objects such as tables, indexes, stored procedures, and views. Log files contain the information that is required to recover all transactions in the database. Data files can be grouped together in file groups for allocation and administration purposes.

SQL Server databases have three types of files, as shown in the following table.

File	Description
Primary	The primary data file contains the startup information for the database and points to the other files in the database. User data and objects can be stored in this file or in secondary data files. Every database has one primary data file.
Secondary	Secondary data files are optional, are user-defined, and store user data. Secondary files can be used to spread data across multiple disks by putting each file on a different disk drive. Additionally, if a database exceeds the maximum size for a single Windows file, you can use secondary data files so the database can continue to grow.
Transaction Log	The transaction log files hold the log information that is used to recover the database. There must be at least one log file for each database.

For example, a simple database named Sales can be created that includes one primary file that contains all data and objects and a log file that contains the transaction log information. Alternatively, a more complex database named Orders can be created that includes one primary file and five secondary files. The data and objects within the database spread across all six files, and the four log files contain the transaction log information.

DATA WAREHOUSE AND DATA MINING

Today in organizations, the developments in the transaction processing technology requires that, amount and rate of data capture should match the speed of processing of the data into information which can be utilized for decision making. A data warehouse is a subject-oriented, integrated, time-variant and non-volatile collection of data that is required for decision making process whereas Data mining involves the use of various data analysis tools to discover new facts, valid patterns and relationships in large data sets. Data mining also includes analysis and prediction for the data. Data mining helps in extracting meaningful new patterns that cannot be found just by querying or processing data or metadata in the data warehouse.

DATA WAREHOUSING

Large amount of operational data are routinely collected and stored away in the archives of many organizations. To take a simple example, the railway reservation system has been operational for over a decade and large amount of data is generated each day on train bookings. Much of this data is probably archived for audit purposes. This archived operational data can be effectively used for tactical strategic management of the railways. For example, by analyzing the reservation data it would be possible to find out traffic patterns in various sectors and use it to add or remove bogies in certain trains, to decide on the mix of various classes of accommodation, etc. For this analysis building a data warehouse is an effective solution.

Data warehouse is a storage area for processed and integrated data across different sources which will be both operational data and external data. Data warehouses offer organizations the ability to gather and store enterprise information in a single conceptual enterprise repository. It allows its users to extract required data for business analysis and strategic decision making. One can also define a warehouse as a copy of transaction data specifically structured for query and analysis. It is a repository of information, integrated from several operational databases. Data warehouses store large amount of data which can be frequently used by decision support system. It is maintained separately from the organizations operational database. They are relatively static with only infrequent updates. The most effective advantages of data warehousing is high speed of data processing and summarized data.

Characteristics of data warehouse

– *Subject oriented*: A data warehouse is organized around major subjects such as customer, products, sales; etc. Data is organized according to subject instead of application. For example, an insurance company using a data warehouse would organize their data by customer, premium and claim instead of

by different product like auto, life; etc. The data organized by subject obtains only the information necessary for the decision support processing.

– *Integrated*: A data warehouse is usually constructed by integrating multiple, heterogeneous sources such as relational databases, flat files, and OLTP file. When data resides in many separate applications in the operational environment, the encoding of data is often inconsistent. When data is moved from operational environment into the data warehouse, they assume a consistent coding convention. Data cleaning and data integration techniques are applied to maintain consistency in naming convention, measures of variables, encoding structure and physical attributes.

– *Nonvolatile*: A data warehouse is always a physically separate store of data, which is transformed from the application data found in the appropriate environment. Due to this separation, data warehouses do not require transaction processing, recovery, concurrency control, etc. The data is not updated or changed in any way once they enter the data warehouse, but are only loaded, refreshed and accessed for queries

– *Time variant*: Data is stored in data warehouse to provide a historical perspective. Every key structure in the data warehouse contains, implicitly or explicitly, an element of time. The data warehouse contains a place for sorting data that are 5 to 10 years old, or older, to be used for comparisons, trends and forecasting.

Database vs. data warehouse

Database is a collection of related information stored in a structured form in terms of table so that it makes easier insertion, deletion and manipulation of data. Database consists of tables that contain attributes. Whereas a data warehouse is a database system optimized for reporting and analysis. It generally refers to the combination of many different databases across entire enterprise. Once the data entered in the data warehouse, it can be then only loaded, refreshed and accessed for queries.

DATA MINING

It is a process of extracting hidden predictive information from large databases. It is a powerful new technology to help companies focus on the most important information in their data warehouses. Data mining tools predict future trends and behaviors, allowing businesses to make proactive, knowledge-driven decisions. For a commercial business, the discovery of previously unknown statistical patterns or trends can provide valuable insight into the function and environment of their organization. Data-mining techniques can generally be grouped into two categories: predictive method and descriptive method.

***1. Descriptive method*:** It a method of finding human interpretable patterns that describe the data. Data mining in this case is useful to group together similar documents returned by search engine according to their context.

***2. Predictive method*:** In this method, we can use some variables to predict unknown or future values of other variable. It is used to predict whether a newly arrived customer will spend more than Rs. 1000 at a department store.

In its simplest form, data mining automates the detection of relevant patterns in a database, using defined approaches and algorithms to look into current and historical data that can then be analyzed to predict future trends. Because data mining tools predict future trends and behaviors by reading through databases for hidden patterns, they allow organizations to make proactive, knowledge-driven decisions and answer questions that were previously too time-consuming to resolve.

Data mining is not particularly new — statisticians have used similar manual approaches to review data and provide business projections for many years. Changes in data mining techniques, however, have enabled organizations to collect, analyze, and access data in new ways. The first change occurred in the area of basic

data collection. Before companies made the transition from ledgers and other paper-based records to computer-based systems, managers had to wait for staff to put the pieces together to know how well the business was performing or how current performance periods compared with previous periods. As companies started collecting and saving basic data in computers, they were able to start answering detailed questions quicker and with more ease.

LESSON ROUND-UP

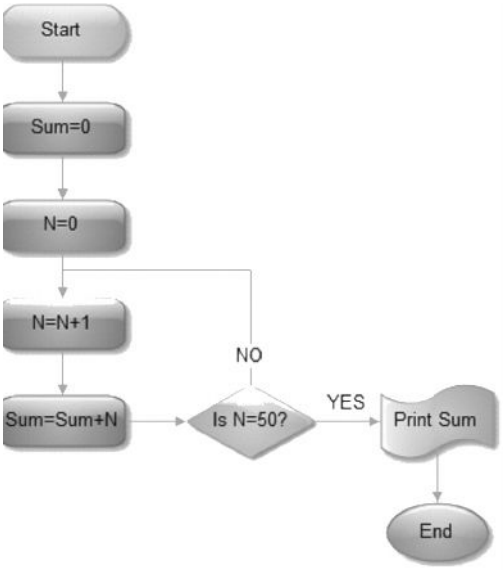
- Database is a collection of related files that are usually integrated, linked or cross-referenced to one another. The advantage of a database is that data and records contained in different files can be easily organized and retrieved using specialized database management software called a database management system (DBMS) or database manager.
- The term database system refers to an organization of components that define and regulate the collection, storage, management and use of the data within a database environment. The database system is composed of: 1. Hardware, 2. Software, 3. People, 4. Procedures, 5. Data
- A database management system is a set of software programs that allows users to create, edit and update data in database files, and store and retrieve data from those database files. Data in a database can be added, deleted, changed, sorted or searched all using a DBMS.
- DBMSs are commonly used to manage, Membership and subscription mailing lists, Accounting and bookkeeping information, The data obtained from scientific research, Customer information, Inventory information, Personal records, Library information
- The Advantages of a DBMS includes improved data availability, Minimized data redundancy, data Accuracy, Program and file consistency, User-friendliness, Improved security. DBMS have certain disadvantages which includes high cost, security issues etc.
- Data Model can be defined as an integrated collection of concepts for describing and manipulating data, relationships between data, and constraints on the data in an organization. The purpose of a data model is to represent data and to make the data understandable.
- Data structure is a particular way of storing and organizing data in a computer so that it can be used efficiently. Data structures provide a means to manage large amounts of data efficiently, such as large databases and internet indexing services. Usually, efficient data structures are a key to designing efficient algorithms.
- Database administrators (DBAs) are primarily responsible for specific databases in the subsystem. In some companies, DBAs are given the special group authorization, SYSADM, which gives them the ability to do almost everything in the DB's subsystem, and gives them jurisdiction over all the databases in the subsystem. The DBA can be responsible for granting authorizations to the database objects, although sometimes there is a special security administration group that does this.
- Data Definition Languages is used to define the various types of data in the database and their relationships with each other while Data Manipulation Language (DML) enables users to access or manipulate data (retrieve, insert, update, delete).
- A database file is defined as a collection of related records. A database file is sometimes called a table. A file may be composed of a complete list of individuals on a mailing list, including their addresses and telephone numbers.
- A data warehouse is a subject-oriented, integrated, time-variant and non-volatile collection of data that is required for decision making process whereas Data mining involves the use of various data analysis

tools to discover new facts, valid patterns and relationships in large data sets. Data mining also includes analysis and prediction for the data. Data mining helps in extracting meaningful new patterns that cannot be found just by querying or processing data or metadata in the data warehouse

SELF-TEST QUESTIONS

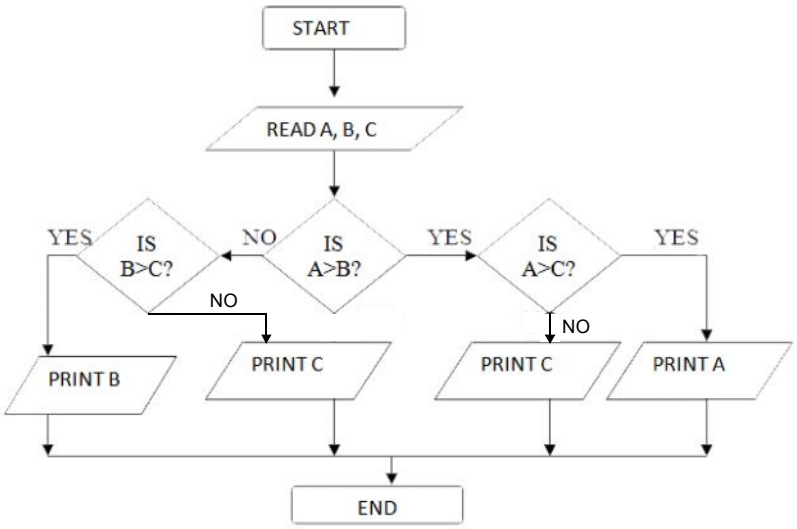
(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. What is database or database management systems (DBMS)? What's the difference between file and database? Can files qualify as a database?
2. Write the difference between DBMS and RDBMS?
3. Define data models. What are the different data models are available?
4. What do you mean by Data Definition Languages (DDL) and Data Manipulation Languages (DML)?
5. What is Data Warehousing? Explain its characteristics?
6. What is Data mining? Compare Data mining and Data Warehousing?
7. What is database? What are the characteristics of database system?
8. What are the functions of a database administrator?
9. What are the scenarios where we donot require database system? Explain any one.

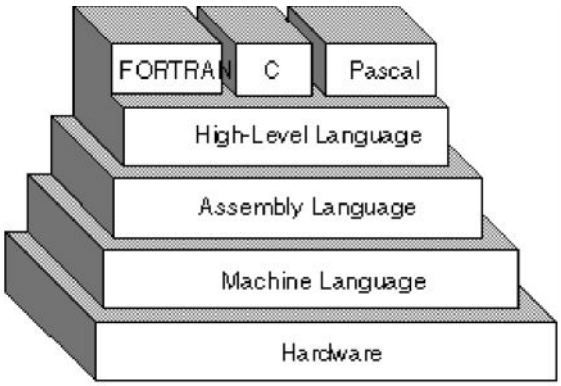


***Example No.* 2**: Draw a flowchart to find the largest of three numbers A,B, and C.

Answer: The required flowchart is shown as below



PROGRAMMING LANGUAGE



Lesson 7
Internet and Other Technologies

LESSON OUTLINE

- Systems- An Overview
- Internet
- World-Wide Web
- Intranets
- Extranets
- Applications of Internet
- Internet Protocols
- E-Commerce
- Supply Chain Management
- Customer relationship Management (CRM)
- Electronic Data Interchange (EDI)
- Electronic Fund Transfers (EFT)
- Mobile Commerce
- Bluetooth
- WI-FI

LEARNING OBJECTIVES

Internet and internet driven technologies i.e. Bluetooth, wi-fi and so has become an integral part of our life. It has affected each of us life in one or other way. It is internet only which enables us to do various tedious tasks in minutes. All Government agencies and regulatory bodies are promoting use of internet and its applications. After reading this lesson students will be able to:

- Understand Internet and a variety of its applications and other related technologies.
- Understand various aspects related to Internet Protocols, E-commerce security.
- Get an idea about e-commerce and its various variants.
- Understand the mechanism of internet driven technologies i.e. electronic fund transfer system, EDI etc.

The Internet is becoming the town square for the global village of tomorrow.

Bill Gates

INTERNET

The Internet is a global system of interconnected computer networks. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies.

The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support email. It uses the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide.

The Internet has enabled and accelerated new forms of human interactions through instant messaging, Internet forums, and social networking. Online shopping has boomed both for major retail outlets and small artisans and traders. Business-to-business and financial services on the Internet affect supply chains across entire industries. Most traditional communications media including telephone, music, film, and television are being reshaped or redefined by the Internet, giving birth to new services such as Voice over Internet Protocol (VoIP) and Internet Protocol Television (IPTV). Newspaper, book and other print publishing are adapting to web site technology, or are reshaped into blogging and web feeds.

Origin of Internet

The origin of the Internet reach back to research commissioned by the United States government in the 1960s to build robust, fault-tolerant communication via computer networks. The funding of a new U.S. backbone by the National Science Foundation in the 1980s, as well as private funding for other commercial backbones, led to worldwide participation in the development of new networking technologies, and the merger of many networks. The commercialization of what was by the 1990s an international network resulted in its popularization and incorporation into virtually every aspect of modern human life. As of June 2012, more than 2.4 billion people – over a third of the world's human population – have used the services of the Internet; approximately 100 times more people than were using it in 1995, when it was mostly used by tech-savvy middle and upper class people in the United States and several other countries

WORLD WIDE WEB

The World Wide Web (abbreviated as www commonly known as the web), is a system of interlinked hypertext documents (these are standard document format for internet, written using Hyper Text Mark up Language, HTML), accessed via the Internet. With a web browser (browser is a piece of software that acts as interface between the user and inner workings of the internet), one can view web pages that may contain text, images, videos, and other multimedia, and navigate between them via hyperlinks.

British Engineer Sir Tim Berners-Lee in March, 1989, wrote a proposal that referenced his database and software project 'ENQUIRE', and described a more elaborate information management system. In Year 1990, he published a more formal proposal to build a "Hypertext project" called "Worldwide Web" to be viewed by "browsers" using client–server architecture.

This project has only give birth to World Wide Web.

Features of World Wide Web

1. Medium of Publishing Information: The 'world wide web' or 'web' for short is a medium for publishing information on the internet in an easy to use form. If we take the analogy of television then internet would be equivalent to the broadcasting equipment such as mast and transmitter and World Wide Web to the content of different T.V. programmes. The medium is based on standard document format known as HTML (Hyper Text Mark up Language).

2. Easy retrieval of Information: The amount of information available on the Internet has become so large that it is difficult to search for specific information. The World Wide Web (WWW) makes retrieval easy and quick.

3. Easy Navigation of Documents: The WWW is a search tool that helps you find and retrieve information from a Web site using links to other sites and documents. The WWW was built on the technology called Hypertext. This technology increases accessibility to linked documents on the Internet and helps user to navigate between documents very easily.

4. Linking of Documents: Hypertext is identified by underlined text and a different color usually. Some places will refer these types of technique as Jump-Off Points. Hypertext can make links within the same document or to other documents.

5. Helpful in sharing information: The WWW is intended to help people share information resources, and services with the widest possible community of users. Thus a user can access the WWW on Apple, UNIX, Macintosh, DOS, Windows, and other operating systems.

6. Easy search, transverse and other use of information: WWW lets you search, traverse, and use many types of information at numerous sites and in multiple forms. This interface is called a browser. Some people refer to a browser as a 'web browser' often these terms are used interchangeably

7. Use of Protocol: Just like the Internet, the www has a protocol, which is known as HyperText Transfer Protocol (HTTP). HTTP acts as an interface between a Web Client Software, such Netscape Navigator.

Web Browsers

A browser is a piece of software that acts as interface between the user and inner workings of the internet specifically the World Wide Web. Browsers are also referred to as web clients, or universal clients, because in the client/server model, the browser functions as the client program. The browser acts on the behalf of user. The browser -

- Contacts a web server and sends a request for information.
- Receives the information and then display it on the user's computer.

Text and graphical information can be displayed in browser. The www incorporate hypertext, photographs, sounds, video etc. that can be fully experienced through graphical browser.

Popular browser includes

1. Netscope Navigator.
2. Microsoft Internet Explorer
3. Mosaic
4. Opera
5. Lynx
6. Hot java
7. Mozilla Navigator
8. Safari
9. Mozilla Firefox
10. Google Chrome

Features of web browsers:

Regardless of which browser one use, web browser may support some or all of these features.

- Book mark for favourite websites
- Multiple browsing windows
- Frames or multiple views with in a window
- Secure data transmission
- Java and other Language support
- Web interface to FTP and Gopher internet Sites.

Web addresses:

Web addresses refers to particular pages on a web server which are hosted by company or organisation. The technical name for these is uniform resource location. They are usually prefixed by http://www to denote the web protocol and then broken down as follows:

http://www.domain-name.extension/file name

Domain Name: It refers to the name of server and usually selected to be the same as the name of the company, the extension indicates its type. A domain name always contains two or more components separated by period called dot.

The top-level portion of a domain describes the type of organisation holding the name. An important category for top level domains covers the following:

1. com : Commercial Organisation
2. edu : Educational Institutions
3. net : Organisation involved in internet operations
4. org : Miscellaneous Organisations
5. in : It is the country code for India. Two letter abbreviations are used for it.
6. gov : Government entities.

INTRANET

It refers to a private network which is designed to meet the internal information needs of the employees. It is accessible only by authorised employees, contractors and customers. It is basically used to communicate non-sensitive but broadly useful information such as Recent Corporate News:

(a) General product information

(b) Details of health insurance

(c) Travel expense forms

(d) Product pricing

(e) In-house training programmes.

The need for intranet is the result of many factors such as:

(a) cost effectiveness

(b) Prompt availability of information to company and users

(c) Less expensive means of communication to remain in touch with employees located in scattered offices

(d) Custom support

Advantages of Intranet

Important advantages of Intranet include the following:

- Easy, economic and fast system of communication within enterprise
- Based on internet protocol which expands accessibility
- Serves information automatically
- Replaces Grapevine and permit inter-employee communication with more transparency
- Improves productivity of executives by devoting more time in analysing information than waiting for information
- Ready to access the information globally
- Makes the flow of Information need driven
- Handles multimedia data effortlessly

Disadvantages of Intranet

Important disadvantages of Intranet include the following:

- Risk of Security to the corporate information resources
- Needs to change the work culture for effectiveness of internet
- Danger of reduction in face to face interaction between employees leading to impersonisation of the company

Successful Strategies for Intranet

For effective success of Intranet in a company, one may implement the following strategies:

1. **Include widely used applications and make them simple to use:** Use the intranet to simplify employee's lives. For instance, by putting travel expense reports on-line, employees do not have to waste time filling out hard-copy reports, making copies for numerous people, and sending them through regular or interoffice mail, which can take days. Instead, they can complete reports and send them to as many people as needed. The recipients receive them in moments.
2. **Secure the system:** Security of intranets is vital. If the information on an intranet is corrupted (such as an inaccurate posting of company job openings) or if a competitor accesses the information (such as pricing policies for different products), it can lead to distrust.
3. **Integrate databases into intranet applications:** Databases are at the heart of intranet applications. The data and information that employees access from the intranet come from one or more databases. Companies must invest the time and money to build databases that are accurate, complete, and reliable.
4. **Invest in excellent network capacities:** Clearly, networks are essential for the success of intranets. Without a robust network infrastructure, an intranet simply will not be able to function. If the network is frequently down or if the network is too slow, employees will get frustrated and may not use the intranet.

5. **Motivate employees to use the intranet:** Change is not easy. Many people prefer to do things the way always have. To convince people of the benefit of change, intranets must be easy to use with user-friendly, intuitive interfaces. Further, companies should give incentives encouraging employees to use the intranet.

EXTRANET

It refers to private network which operates similarly to an intranet but is directed at customers or suppliers (people outside the organization) rather than at employees. An extranet is a computer which allows controlled access from the outside, for specific business or educational purposes. In a business-to-business context, an extranet can be viewed as an extension of an organization's internet that is extended to users outside the organization, usually partners, vendors, and suppliers, in isolation from all other Internet users. For decades, institutions have been interconnecting to each other to create private networks for sharing information. One of the differences that characterize an extranet, however, is that its interconnections are over a shared network rather than through dedicated physical lines Extranet provides information customers need such as detailed product description, frequently asked questions about different products, offices maintenance information warranties and how to contact customer service and sales office. Earlier, it was difficult for customers to access much of this information because paper version of it at the customer site became scattered and out dated. By using extranet, companies are making this type of information increasingly available at a single interactive site that is easy to navigate.

Successful Strategies for Extranet

Some of the important strategies necessary for success of extranet are discussed as under:

1. Understand the return on investment: The business should develop its extranet with specific goals in mind, such as improving customer satisfaction, reducing operating costs, increasing sales, or any other goal. Companies must establish clear goals and work toward them because extranets are expensive.

2. Select your audience and meet its needs: Extranets are designed to cater to the external entities of a business, such as customers, suppliers, government regulators, and stockholders. The company should carefully select the entity or entities that it wants the extranet to serve. The information needs of a stockholder are quite different from the information needs of a supplier. Once a decision is made about the audience for the extranet, the next step is to carefully identify specific information problems the extranet will address.

3. Be willing to change: An extranet is a work in progress. Companies must continue to invest in the extranet if it is to meet the changing needs of its audience. Otherwise, the extranet will become quickly outdated, defeating its purpose.

4. Keep things simple: People want clean, crisp, easy-to-click-on applications. Because many visitors may not be proficient with the Internet, it is important to make extranets intuitive and easy to use. Users do not want to spend an enormous amount of time on clerical functions, so such functions, in particular, should be easy to use.

5. 24 hours a day: Extranets should be up and running 24 hours a day, 7 days a week. Visitors should be able to access the extranet anytime from anywhere. In the case of global companies, this becomes imperative, given the time different between different countries.

6. Work with end users: When IT staffs try to build an extranet without help, the project's chances of success sharply diminish. Successful extranets are a joint venture between IT and the business end users.

APPLICATIONS OF THE INTERNET

1. Communication: Internet has become an indispensible means of communication now days. Internal communication mode such as E-mail has become the synonym for business communication. Now it is the time where most of the business communication happens over e-mail only.

E-mail is the most popular internet service which refers to sending business communication electronically over a network to single recipient or to many recipients. The receiver can retrive the mail at his or her convenience or the user is automatically notified when there is E-mail in the electronic mail box. An E-mail system requires messaging system that stores and forward the messages to the right individual and mail program that allow the user to send and receive messages. E-mail messages on the Internet can be transmitted from one user to another often in seconds. Some more details on E mail are covered later in this chapter.

2. Management of Business Operations: Internet has become a must have resource for all business concerns. Now most of the organisation owns their web portals where one may get ins and outs of the organisation. Internet has brought remarkable changes in the working of the business organisations.

3. Education: Internet is extensively used presently in providing education. Now for getting an internationally recognized degree, it is not necessary for someone to go thousands of miles away, he may use online education facility and get recognized sitting at home. Many organisation have emerged which are providing free online education through MOOCS (Massive open online course). One needs to simply register with them online and they can sit at home freely. This has become possible only through the Internet.

4. Research and studies: Internet has proved to be a boon for research and studies. Now, most of the good libraries have got digitized and these are available online. One may get their online access by paying the requisite fee. In addition to the online libraries, ample ofmaterial is freely available on internet. Researches may find enormous details about a topic in just a click. This has become possible only through the Internet.

5. E-commerce: E Commerce is another application of internet which has makes everyone's life easier. Now sitting at home, one may buy railway tickets, transfer money from one account to another, buy insurance policies, and buy house hold goods. E-commerce has benefited business, consumer and even to the government.

6. E-governance: E-governance is another application of internet. In the age of internet, government has also taken serious steps for computerisation of government offices. This will help in elimination of various disadvantages of bureaucracy.

The above list of internet application is just indicative and students may enumerate various others applications too.

ELECTRONIC MAIL

Electronic Mail is the abbreviated form of acronym e-mail. It is one of the most important applications of internet. It is a fast and efficient method to exchange messages and other data. The following section covers its advantages and disadvantages.

Advantages of E-Mail

Some of the major advantages of e-mail are summarised as follows:

1. Speed: E-mail messages can be transmitted very quickly. A typical message containing 400 words, for example, can be transmitted in under a second. As a means of communication, e-mail is considered extremely fast, with some messages able to reach their destination in a matter of minutes. Since e-mail is considered to be an extremely fast method of communication, users often use the derisory term 'snail mail' to refer to the conventional postal system.

2. Cost: The cost of sending or receiving messages is considered very low. Hundreds of messages can be sent or received for the cost of a brief telephone call, making e-mail for cheaper than the postal service.

3. Multiple copies: E-mail allows multiple copies of the same basic message to be created and transmitted. As an example, Eudora, a leading e-mail package, uses a special directory to hold the names and e-mail addresses of friends and colleagues. Using some of the functions of the directory, groups of people can be assigned an alias (sometimes known as a nickname), for example the name of a department might be used as an alias for all of the people working there. A message can be created in the usual, way and addressed to the alias. When the message is transmitted, copies are sent automatically to each of the people belonging to the group.

4. Auditing: Even the simplest e-mail package will provide a number of features that allow users to audit their messages. Most programs allow users to keep copies of any messages they produce, automatically marking them with the date and time they were created. Some programs can automatically create receipts that can be used to check if a message sent to another user has been received, or even if the message has been read.

5. Sharing data: E-mail messages can be used to transmit data files to other users. Files can be attached to messages and transmitted in the usual way. All types of data can be sent in this way, including word processor files, spreadsheet data, graphics and database files.

6. Multimedia: The latest e-mail packages allow users to include multimedia elements in their messages. Messages can include a variety of different elements, including graphics, video, hyperlinks to information on the Internet and sound files.

7. Group work: E-mail supports group work and remote working. Group work involves several people working on the same project, using IT to help them communicate with each other and share data files. Remove working (Teleworking) involves people working away from a central office - perhaps at home - but staying in contact through e-mail and other methods.

8. Flexibility: The hardware and software used for handling e-mail can also be used for a variety of other purposes. A typical modem, for example, can also be used to send or receive fax messages.

Disadvantages of E-mail

Some of the main disadvantages of e-mail are summarised as follows:

1. Routing: E-mail messages seldom take the most direct route to their destinations. A message sent from Manchester to London, for example, might travel through Liecester, Birmingham and Nottingham before reaching its final destination. This can lead to a number of difficulties.

- The time taken to receive the message can be very long
- There are more opportunities for the message to become lost or garbled
- There are more opportunities for messages to be intercepted

2. Cost: In order to send or receive e-mail, organisations must have access to the correct hardware and software. The expense of buying new equipment, such as a PC with modem, can mean that it is beyond the reach of smaller companies. Organisations needing to deal with large volumes of data may need to invest in fibre-optic cabling or microwave transmitters.

3. Technical issues: Since using an e-mail service requires a certain level of technical knowledge, novice users may find it difficult to operate the hardware and software involved. This can place a burden on an organisation in terms of training and technical support requirements.

4. Spam: Unwanted messages, such as advertisements, are received by most e-mail users. The act of sending out these messages is usually called spamming. Dealing with unwanted or unnecessary e-mail messages can place a great burden on an organisation's resources.

5. Security: Unless they are encrypted, e-mail messages can be intercepted relatively easily. This makes e-mail unsuitable for sending confidential information unless special precautions are taken.

INTERNET PROTOCOLS

The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order.

IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However, IP Version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

IP Address Format

The 32-bit IP address is grouped eight bits at a time, separated by dots, and represented in decimal format (known as dotted decimal notation). Each bit in the octet has a binary weight (128, 64, 32, 16, 8, 4, 2, 1). The minimum value for an octet is 0, and the maximum value for an octet is 255. An example of IP address is as given below:

An IPv4 adress (dotted-decimal notation)

172	–	16	–	254	–	1
⬇		⬇		⬇		⬇
10101100		00010000		1111111		00000001

One byte = Eight bits

Thirty-two bits (4-8), or 4 bytes

Internet Protocol Characteristics

1. The IP protocol resides in the Internet layer, as we have already said. The IP protocol is the protocol in

the TCP/IP stack that is responsible for letting the machine, routers, switches and etcetera, know where a specific packet is going. This protocol is the very heart of the whole TCP/IP stack, and makes up the very foundation of everything in the Internet.

2. The IP protocol encapsulates the Transport layer packet with information about which Transport layer protocol it came from, what host it is going to, and where it came from, and a little bit of other useful information. All of this is precisely standardized, down to every single bit.
3. The IP protocol has a couple of basic functionalities that it must be able to handle. It must be able to define the datagram, which is the next building block created by the transport layer (this may in other words be TCP, UDP or ICMP for example).
4. The IP protocol also defines the Internet addressing system. It means that the IP protocol is what defines how to reach between hosts, and this also affects how one is able to route packets.
5. IP must also be able to decapsulate and encapsulate the IP datagram (IP data) and send or receive the datagram from either the Network access layer, or the transport layer.
6. IP protocol is responsible for routing packets from one host to another, as well as packets that we may receive from one host destined for another.
7. The IP protocol is also a connectionless protocol, which in turn means that IP does not "negotiate" a connection. A connection-oriented protocol on the other hand negotiates a "connection" (called a handshake) and then when all data has been sent, tears it down. TCP is an example of this kind of protocol; however, it is implemented on top of the IP protocol.

ELECTRONIC COMMERCE (E-COMMERCE)

Electronic commerce or E-commerce is a term for any type of business, or commercial transaction that involves the transfer of information across the Internet. It covers a range of different types of businesses, from consumer based retail sites, through auction or music sites, to business exchanges trading goods and services between corporations. It is currently one of the most important aspects of the Internet to emerge.

In Year 1997 OECD (Organization for Economic Corporation and Development, defines that E-Commerce refers generally to all the forms of transactions related to commercial activities, including both organizations and individuals, that are based upon the processing and transmission of digitized data, including text, sound and visual images.

E-commerce allows consumers to electronically exchange goods and services with no barriers of time or distance. Electronic commerce has expanded rapidly over the last few years and is predicted to continue at this rate, or even accelerate. In the near future the boundaries between "conventional" and "electronic" commerce will become increasingly blurred as more and more businesses move sections of their operations onto the Internet.

European Commission in Year 1997 defines, that Electronic Commerce is about doing business electronically. It is based on the electronic processing and transmission of the data, including text, sound, and video. It encompasses many diverse activities including electronic trading of goods and services, online delivery of digital content, electronic fund transfers, electronic share trading, electronic bills of lading, commercial auctions, collaborative design and engineering, online sourcing, public procurement, direct consumer marketing, and after sales service. It involves both products (e.g. consumer goods, specialized medical equipment) and services (e.g. information services, financial and legal services); traditional activities (e.g. health care, education) and new activities (e.g. virtual malls).

Thus, E-commerce refers to the paperless exchange of business information using Electronic Data Interchange, electronic mail, electronic bulleten board, electronic funds transfers and other networked based technologies. It

is not only automates manual process and paper transaction but also help organisations move to a fully electronic environment and change the way they operate.

In a holistic sense electronic commerce can be summarized as:

- It is a business strategy.
- It uses technology to achieve business goals.
- It improves external business relationships.
- It is an evolution in the way companies Internet.
- It provides information to facilitate delivery of goods and services.
- It supports change initiatives and reinforces business process re-engineering.

Elements of E-commerce

1. A product or a service: In case of E-Commerce, it is virtual product shown on a web site. One can demonstrate multimedia presentation of the product and all its features on the web page itself, which may not be possible in case of physical product of commerce activity.

2. A place to sell the product: In the e-commerce case, a website displays the products in all ways & act as a place for E-Commerce.

3. A way to get customers to visit your website: In case of E-Commerce search engines and linkages with other web sites play an important role in helping the customers to reach web sites of the e-organizations.

4. A way to accept orders: The orders are accepted on the web site itself. On the web pages of the E-commerce companies shopping carts are being provided. One can click on the icon and fill in the shopping card to order items to be purchased and it is accepted by the E-comm. Company as order from the customer.

5. A way to accept money: In case of traditional commerce, buyers and sellers are in direct contact with each other. The payments in E-commerce are made using Electronic Fund Transfer in various form using credit cards, smart cards, e-checks, etc. The information of payment is routed through Value Added Networks (VANs) and Payment Gateway Systems, etc.

6. A fulfilment facility to ship product to customers: The shipment of the product to the customer is made through third party. The most of the E-commerce companies are having their chain of suppliers in various localities and items are shipped through these suppliers to the customers.

7. A way to accept returns: As is the case of commerce, in case of E-commerce all the trading companies have the system of accepting the returns if the goods and services are not to the satisfaction of the customer or not upto the standards/ specifications mentioned in the product catalogue or brochures hosted on the web pages.

8. A way to handle warranty claims: Sometimes if the product breaks in the way or some other problems crop up with the product. In such situation, warranty claims are to be honoured as in the case of commerce.

9. A way to provide customer service: The main tools of the customer service are E-mail, On-line forms, on-line knowledge bases and frequently asked questions.

Type of E-commerce

E-commerce types represent a range of various schemas of transactions which are distinguished according to their participants. Usually E-commerce is divided into three general most well-known types, but the notion is much wider. Here four such models are specified.

1. B2B or Business to Business

2. B2C or Business to Consumer

3. C2C or Consumer to Consumer

4. C2B or Consumer to Business

B2B OR BUSINESS TO BUSINESS

It is considered as one of the most perspective and extensively developing E-commerce trend nowadays. It refers to electronic commerce between businesses and also supplies chain technology, which is the largest and most successful e-commerce technology nowadays. The parties of B2B schema are "Business Partners". Internet platforms give an opportunity to considerably simplify all steps of the operations, make the trade more immediate. An example of a schema B2B is selling site templates to companies for using as a design base, besides any other interactions involving bulk deliveries are included. B2B means an established working relationship therefore it is a better solution to deliver comparing to B2C, although it needs to link together two complex accounting systems.

Characteristics of B2B E-commerce

(a) It requires two or more business entities interacting with each other directly or through an intermediary.

(b) The intermediaries in B2B may be the market makers and directory service providers that assist in matching the buyers and sellers and striking a deal.

(c) The business application of B2B electronic commerce can be utilized to facilitate almost all facets of the interactions among organizations, such as Inventory Management, Channel Management, Distribution Management, Order fulfilment and delivery, and payment management.

(d) The B2B electronic commerce can be

- Supplier-Centric,
- Buyer-centric, or
- Intermediary-centric.

Supplier-Centric B2B E-commerce

In a supplier centric B2B E-commerce, a supplier sets up the electronic commerce market place for various buyer businesses to interact with the supplier at its electronic market place. Typically, a dominant supplier in the domain of products sets up such a market place. The supplier may provide customized solutions and pricing to fit the needs of buyers' businesses. Usually, differential price structure is dependent upon the volume and loyalty discount. Example, Cisco Connection Online (CCO)

Buyer-Centric B2B E-commerce

In a Buyer centric B2B E-commerce, the major business with high volume purchase capacity creates an electronic marketplace for purchase and acquisition. The electronic marketplace is used for placing requests for quotations (RFQs) and carry out the entire purchase process on-line by the buyer. This kind of facility may be utilized by high volume and well recognized buyers, as they may have adequate capacity and business volumes to lure suppliers to bid at the site. Example, General Electric's Trading Process Network

Intermediary-Centric B2B E-commerce

In Intermediary-Centric B2B E-commerce, a third party may set up the electronic marketplace and attract both

the buyer and seller businesses to interact. The Buyers and Sellers, both benefit from the increased options in terms of pricing, quality, availability and delivery of goods. The third party electronic marketplace acts as a hub for both the suppliers and buyers, where buyers place their request for the quotations and sellers respond by bidding electronically leading to a match and ultimately to a final transaction. It is essential that Intermediary Company represent large number of the members in that specific markets segment, i.e., both the buyers and the sellers. The Intermediary reduces the need of buyers and sellers to contact a large number of potential partners on their own. Example, IndiaMart.com

B2C OR BUSINESS TO CONSUMER

It has lately gained a big popularity due to simplified and accelerated way to buy products. Business to Consumer refers to selling and buying of goods and services via the web. The parties are: a company (a web retailer) who trades to an individual (a web customer). Retail trading (via online shops) is the most well-know example of such a type of transactions allowing consumers to purchase by lower prices and with more convenience. The disadvantages of B2C E-Commerce type are selling to un-trusted strangers and extra effort to get customer and payment information. However, B2C almost always involves customer typing information into an order screen therefore it is a better solution to provide comparing to B2B.

In B2C E-commerce, the businesses offer a set of merchandise at given prices, discounts and shipping and delivery options and the sellers and consumers both benefit:

1. Through the round the clock shopping
2. Accessibility from any part of the world,
3. Increased opportunity for direct marketing,
4. Customizations and
5. Online customer service

The B2C model of electronic commerce transaction is ideally suited for the following:

1. Goods that can be easily transformed into the digital format such as books, music clips and videos, software packages
2. Items that follow a standard specifications: printer ribbons, ink cartridges etc
3. Highly rated brand items or items with return security: Dell & Compaq Computers, Electronic Gadgets from Sony etc.
4. Items that may be sold in packets that cannot be opened even in physical stores, Kodak film rolls
5. Relatively cheap items: where the savings outweigh the risks
6. Items that can be experienced online such as Music, Videos etc

C2C or Consumer to Consumer

It refers to online dealing of goods and services between people. The parties are two consumers (individuals). This type of transaction is fulfilled due to online market dealer like auction sites, becoming more and more popular nowadays (for example eBay).

Character of C2C E-commerce

1. It promotes opportunity for consumers to transact goods or services to other consumers present on Internet.

2. The C2C in many a situations models the exchange systems with a modified form of deal making.
3. For the deal making purposes large virtual consumer trading community is developed. The customer operates by the rules of this community to compete, check and decide his own basic transaction prices.
4. It mimics the traditional economic activities corresponding to 'classified ads' and auctions of personal possessions.
5. Much of the transactions in this category correspond to the small gift items, craft merchandise and similar items that are normally sold through the 'flea' markets or Bazaars

C2B OR CONSUMER TO BUSINESS

It is an emerging concept where consumers demand specific products or services from respective businesses by presenting themselves as a buyer group. Example of this type is contacting a tour and travel operator via their website for purchasing a holiday package as well as such sites as CTB and SpeakOut.com. These sites provide consumers with market strategies. They are also used by businesses to gain insight into consumer wants.

Characteristics of E-commerce

1. The transactions originated by the customer have the set of specifications and the required price for a commodity, service or an item.
2. The business entity is expected to match the requirements of the consumers to the best possible extent.
3. The Consumer to Business (C2B) enables a consumer to determine the price of a product and/or service offered by a company.
4. It reduces the bargaining time and increases the flexibility at sales place for both the merchant and the consumer. For Example, PriceLine.com

E-COMMERCE SECURITY

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. It can be measured on the following dimensions.

- Integrity : Prevention against unauthorized data modification
- Authenticity : Authentication of data source
- Confidentiality : Protection against unauthorized data disclosure
- Privacy : Provision of data control and disclosure
- Availability : Prevention against data delays or removal
- Non-repudiation : Prevention against any party from reneging on an agreement after the fact

E-Commerce Threats

Threats may refer to anyone with the capability, technology, opportunity, and intent to do harm. Potential threats can be foreign or domestic, internal or external, state-sponsored or a single rogue element. Details of some threats in e-commerce are as given:

1. Intellectual property threats: Use existing materials found on the Internet without the owner's permission, e.g., music downloading, domain name (cyber squatting), software pirating.

2. Client computer threats: This is about spying software like Trojan horse, or of other computer software attacks like Active contents, Viruses etc.

3. Communication channel threats: It includes Sniffer program, Backdoor, Spoofing, and Denial-of-service, etc.

4. Server threats: It covers Privilege setting, Server Side Include (SSI), Common Gateway Interface (CGI), File transfer, Spamming etc.

Counter Measure

Counter measure is a procedure that recognizes, reduces, or eliminates a threat. Now the counter measure adopted for different type of E-commerce threat are discussed below –

1. Intellectual property protection

- Through Legislature & Authentication

2. Client computer protection

(a) Privacy: Cookie blockers

(b) Digital certificate

(c) Browser protection

(d) Antivirus software

(e) Computer forensics expert

3. Communication channel protection

(a) Use of Encryption

(b) Use of Secure Sockets Layer (SSL)

(c) Use of Secure Hyper Text Transfer Protocol (S-HTTP)

(d) Use of Digital signature

4. Server protection

(a) Access control and authentication

(i) Digital signature from user

(ii) Username and password

(iii) Access control list

(b) Firewalls

Minimizing Security Threats

1. Perform a risk assessment: A list of information assets and their value to the firm.

2. Develop a security policy: A written statement on:

- What assets to protect from whom?
- Why these assets are being protected?
- Who is responsible for what protection?

- Which behaviours are acceptable and unacceptable?

3. Develop an implementation plan: It is a set of action steps to achieve security goals.

4. Create a security organization: An organization or a unit to administer the security policy

5. Perform a security audit: A routine review of access logs and evaluation of security procedures.

SUPPLY CHAIN MANAGEMENT

It can be understood as the integration of key business processes from the supplier to the end customer for the smooth flow of products in the value chain. It involves all the parties involved, directly or indirectly, in fulfilling a customer's request. It not only includes the manufacturers, but also suppliers, transporters, warehouses, retailers, and even customers. Each stage in the supply chain is connected through the flow of products, information, and money.

A supply chain is a network of facilities and distribution options that performs the functions of procurement of materials, transformation of these materials into intermediate and finished products, and the distribution of these finished products to customers. Supply chains exist in both service and manufacturing organizations, although the complexity of the chain may vary greatly from industry to industry and firm to firm.

A simple example of Supply Chain may be a very simple supply chain for a single product, where raw material is procured from vendors, transformed into finished goods in a single step, and then transported to distribution centres, and ultimately, customers. Realistic supply chains have multiple end products with shared components, facilities and capacities.

Supply chain management is typically viewed to lie between fully vertically integrated firms, where the entire material flow is owned by a single firm and those where each channel member operates independently. Therefore coordination between the various players in the chain is the key in its effective management. Cooper and Ellram (1993) compare supply chain management to a well-balanced and well-practiced relay team. Such a team is more competitive when each player knows how to be positioned for the hand-off. The relationships are the strongest between players who directly pass the baton, but the entire team needs to make a coordinated effort to win the race.

Role of E-Commerce in a Supply Chain Management

Internet capabilities are having a profound impact on organizations' supply chains. Increasingly, companies are recognizing that the efficient and effective flow of information and materials along their supply chains is a source of competitive advantage and differentiation.

E-supply chain management (e-SCM) is the collaborative use of technology to enhance B2B processes and improve speed, agility, real-time control, and customer satisfaction. It involves the use of information technologies to improve the operations of supply chain activities (e.g., E-procurement), as well as the management of the supply chains (e.g., planning, coordination, and control). E-SCM is not about technology change alone; it also involves changes in management policies, organizational culture, performance metrics, business processes, and organizational structure across the supply chain. The success of an e-supply chain depends on the following:

1. The ability of all supply chain partners to view partner collaboration as a strategic asset. Tight integration and trust among the trading partners generate speed, agility, and lower cost.
2. A well-defined supply chain strategy. This includes a clear understanding of existing strengths and weaknesses, articulating well-defined plans for improvement, and establishing cross-organizational objectives for supply chain performance. Senior executives' commitment is also essential and must be reflected through appropriate allocation of resources and priority setting.

3. Information visibility along the entire supply chain. Information visibility refers to the information about inventories at various segments of the chain, demand for products, capacity planning and activation, synchronization of material flows, delivery times, and any other relevant information that must be visible to all members of the supply chain at any given time. To enable visibility, information must be managed properly: with strict policies, discipline, and daily monitoring. It must also be shared properly.
4. Speed, cost, quality, and customer service. These are the metrics by which supply chains are measured. Consequently, companies must clearly define the measurements for each of these four metrics, together with the target levels to be achieved. The target levels should be attractive to the business partners.
5. Integrating the supply chain more tightly. An e-supply chain will benefit from tighter integration, both within a company and across an extended enterprise made up of suppliers, trading partners, logistics providers, and the distribution channel

CUSTOMER RELATIONSHIP MANAGEMENT

Customer relationship management (CRM) is an information industry term for methodologies, software, and usually Internet capabilities that help an enterprise manage customer relationships in an organized way. For example, an enterprise might build a database about its customers that described relationships in sufficient detail so that management, salespeople, people providing service, and perhaps the customer directly could access information, match customer needs with product plans and offerings, remind customers of service requirements, know what other products a customer had purchased, and so forth.

CRM has come a long way in a few short years. Today, CRM is the central customer repository for all things "customer". In our age of the distributed workforce, going to the backroom to pull the customer's file from the cabinet is not practical. Further, as multiple people from departments all over your company have the need for direct interaction with the customer, this central customer record is critical. More complex than a rolodex or contact manager, CRM is enabling businesses of all sizes to be more efficient and predictably and thoughtfully service, sell and market to their customers.

According to one industry view, CRM consists of:

- Helping an enterprise to enable its marketing departments to identify and target their best customers, manage marketing campaigns and generate quality leads for the sales team.
- Assisting the organization to improve telesales, account, and sales management by optimizing information shared by multiple employees, and streamlining existing processes (for example, taking orders using mobile devices)
- Allowing the formation of individualized relationships with customers, with the aim of improving customer satisfaction and maximizing profits; identifying the most profitable customers and providing them the highest level of service.
- Providing employees with the information and processes necessary to know their customers understand and identify customer needs and effectively build relationships between the company, its customer base, and distribution partners.

E-Commerce & CRM

In the age of the global economy, customers want to buy your product or service when it is convenient for them. The need to have rich descriptions, images and details about your products online is driven by customer demand. That demand is only half the battle, the customer then wants to be able to instantly purchase that product and of course, get it right away, after all your competitor can offer that to them. Today's e-Commerce solutions have graduated to a level far beyond a simple shopping cart. Customers want the ability to manage all aspects of the purchase and their relationship with you through this means. Perhaps most important to this phenomenon is the

experience the customer receives after the order confirmation is complete. Order execution to the customer and if necessary back to you, must be simple, quick and seamless.

Harnessing the power of the Internet to drive a closer relationship with customers should be the goal of every business. Over the last several years, many companies who invested in CRM and E-Commerce technology lost their way as they believed it was an electronic panacea designed to eliminate the need to talk to their customers and orders would just flow in because they had a shopping cart on their website with colorful product images. E-Commerce and CRM are tools designed to learn more about customers, their preferences and a clever way to market and re-market to them. However, most importantly, these tools are and should be a convenience for your customer, not your company.

ELECTRONIC DATA INTERCHANGE

Electronic Data Interchange (EDI) is the computer-to-computer exchange of business documents in a standard electronic format between business partners. Now we will discuss the basic element of the definition of EDI given above

Computer-to-computer exchange: EDI replaces postal mail, fax and email. While email is also an electronic approach, the documents exchanged via email must still be handled by people rather than computers. Having people involved slows down the processing of the documents and also introduces errors. Instead, EDI documents can flow straight through to the appropriate application on the receiver's computer (e.g. the Order Management System) and processing can begin immediately.

The EDI process looks like this: no paper, no people involved:

Business documents: These are any of the documents that are typically exchanged between businesses. The most common documents exchanged via EDI are purchase orders, invoices and Advance Ship Notices. But there are many, many others such as bill of lading, customs documents, inventory documents, shipping status documents.

EDI Exchanges the information in Standard format: Because EDI documents must be processed by computers rather than humans, a standard format must be used so that the computer will be able to read and understand the documents. A standard format describes when each piece of information is and in what from (e.g. integer, decimal, mmddyy). Without a standard format, each company would send documents using its company-specific format and, much as an English-speaking person probably doesn't understand Japanese, the receiver's computer system doesn't understand the company-specific format of the sender's format. There are several EDI standards in use today, including ANSI, EDIFACT, TRADACOMS and XML. And, for each standard there are many different versions, e.g. ANSI 5010 or EDIFACT version D12, Release A. When two businesses decide to exchange EDI documents, they must agree on the specific EDI standard and version. Businesses typically use an EDI translator – either as in-house software or via an EDI service provider – to translate the EDI format so the data can be used by their internal applications and thus enable straight through processing of documents.

Information is exchange between/among Business partners: The exchange of EDI documents is typically between two different companies, referred to as business partners or trading partners. For example, Company A may buy goods from Company B. Company A sends orders to Company B. Company A and Company B are business partners.

BENEFITS OF EDI

It document re-keying

By removing the manual keying of key business documents such as Orders, Invoices, Acknowledgments and Dispatch Notes your company can benefit significantly by:

- Reduced labour costs
- Elimination of human keying errors
- Faster document processing
- Instant document retrieval
- Remove reliance on the postal service

It Eliminate Paper Work

Paper-based transactions have some inherent disadvantages when compared with the electronic transactions:

- Stationery and printer consumable costs
- Document storage costs
- Lost documents
- Postage costs

It Reduce Lead Times and Stockholding

Electronic trading documents can be delivered far more quickly than their paper counterparts, thus the turnaround time from order to delivery can be reduced.

- By using EDI for forecasting and planning, companies are able to get forward warning of likely orders and to plan their production and stock levels accordingly.
- Companies receiving advanced shipping notes or acknowledgments know in advance what is actually going to be delivered, and are made aware of shortages so alternate supplies can be sourced.
- Integrating electronic documents means they can be processed much faster, again reducing lead times and speeding up payments.

It Increase quality of the trading relationship

Electronic trading documents when printed are much easier to read than copies faxed or generated on multi-part stationery by impact printers.

- Accurate documents help ensure accurate supplies.
- Batches of electronic documents are usually sequentially numbered; therefore missing documents can easily be identified, not causing companies to wade through piles of paper.

It gives a Competitive Edge

The organisation which uses EDI gates relatively competitive advantage over the organisation which uses the manual data interchange processes.

ELECTRONIC FUND TRANSFER (EFT)

Electronic funds transfer is one of the oldest electronic payment systems. EFT is the groundwork of the cash-less and check-less culture where and paper bills, cheques, envelopes, stamps are eliminated. EFT is used for transferring money from one bank account directly to another without any paper money changing hands. The most popular application of EFT is that instead of getting a pay-check and putting it into a bank account, the money is deposited to an account electronically. EFT is considered to be a safe, reliable, and convenient way to conduct business.

The advantages of EFT contain the following:

- Simplified accounting
- Improved efficiency
- Reduced administrative costs
- Improved security

Electronic Payment Portal

Payment portal or Payment gateway is an e-commerce application service provider service that authorizes payments for e-businesses, online retailers, bricks and clicks, or traditional brick and mortar. It is the equivalent of a physical point of sale terminal located in most retail outlets. Payment gateways protect credit card details by encrypting sensitive information, such as credit card numbers, to ensure that information is passed securely between the customer and the merchant and also between merchant and the payment processor.

The Benefits of Electronic Payments

1. **Speed**: Sending cash or cheques by post for goods is slow, and has security and currency conversion implications.
2. **Convenience**: Electronic payments ensure that your store is open for business globally, 24-hours a day, seven days a week.
3. **Efficiency**: The following points contribute to its efficiency.
   (a) Electronic payment systems leave behind an electronic documented audit trail, streamlining your auditing and accountancy processes.
   (b) Bank wires are cumbersome and expensive.
   (c) Accepting payments online streamlines the buying cycle. By making your order, stock, purchase, payment and dispatch processes electronic, from website to back office, you don't have to re-key order data.
   (d) Shopping site software can be easily integrated with popular back office packages, such as Sage, to automate ordering, stock control, invoicing and accounting systems.
4. **Reduced costs**: Accepting online payments means that many banking processes become automatic.
5. **Increased customer base**: Online payments take advantage of impulse buyers. 95 per cent of electronic purchases are by credit card. If your website doesn't offer payment by credit cards as an option, you could lose out on this market

MOBILE COMMERCE

M-commerce is a term that is used to refer to the growing practice of conducting financial and promotional activities with the use of a wireless handheld device. The term m-commerce is short for mobile commerce, and recognizes that the transactions may be conducted using cell phones, personal digital assistants and other hand held devices that have operate with Internet access. While still in its infancy, the concept of m-commerce has been refined in recent years and is beginning to become more popular.

It is quite different from traditional e-Commerce. Mobile phones impose very different constraints than desktop computers. But they also open the door to a slew of new applications and services. They follow you wherever you go, making it possible to look for a nearby restaurant, stay in touch with colleagues, or pay for items at a store.

Key Components of M-commerce Applications

- Mobile storefront modules are an integral part of m-commerce apps, where all commodities and services

are categorized and compiled in catalogues for customers to easily browse through the items on sale and get essential information about the products.

- Mobile ticketing module is an m-commerce app component that is closely linked to promotional side of commercial business and enables vendors to attract customers by distributing vouchers, coupons and tickets.
- Mobile advertising and marketing module empowers merchants to leverage m-commerce channels in order to manage its direct marketing campaigns, which are reported to be very effective especially when targeted at younger representatives of digital information consumers.
- Mobile customer support and information module is a point of reference for information about a particular retailer, its offerings and deals. The news about the company, current discounts, shop locations and other information is either pushed to users' m-commerce apps or can be found in m-commerce app itself.
- Mobile banking is inextricably linked to selling process via m-commerce apps, because no purchase can be finalized without a payment. There are various options for executing mobile payments, among which are direct mobile billing, payments via sms, credit card payments through a familiar mobile web interface, and payments at physical POS terminals with NFC technology.

Characteristics of Mobile Commerce

1. Fast Processing: One important characteristic of mobile commerce is that it allows the user to process a transaction fast. Not only does the customer receive his item almost instantly via download, e-mail or another form of electronic delivery, the business owner receives payment for his product or service more quickly compared to traditional methods. The customer must set up a payment option, such as a credit card or an agreement to pay using a specified account, to process the payment immediately before downloading the item. Of course, the speed of delivery is dependent on the reliability of the Internet and network services.

2. Reduced Business Costs: Mobile commerce also helps reduce costs for the seller. She rarely needs to pay for a separate office space, overhead costs or employees. In some cases a small business owner who sets up a mobile commerce operation doesn't need an office at all. The seller can monitor sales online or by receiving statements from a processing service. The main expense for this type of business owner is advertising to disseminate information on how users can access the product or service. The lowered cost allows the business owner to take advantage of a higher per-sale profit. He also can offer the product at a lower price compared to delivery in other formats.

3. Little Need for Maintenance: Another characteristic of mobile commerce is that it requires very little maintenance from the seller. The owner sets the product up for mobile delivery one time and then receives payment for sales automatically. From time to time, he may need to perform a few maintenance duties, such as correcting a technology error or updating the product, but overall it is a selling format that requires very little management compared with other selling strategies.

Future of M-commerce

The most prominent m-commerce trend is its own growth. According to Forrester, annual m-commerce sales are predicted to quadruple to $31 billion in the next five years. In 2012, some ecommerce sites (like Amazon) saw remarkable growth, while most businesses experienced only limited m-commerce success. However, one thing they all have in common is that they now universally recognize m-commerce as an important way to enhance their brand, increase their sales and keep up with competitors. In short, the future of m-commerce is bright, and looks like it's getting even brighter.

Another trend in m-commerce is that customers desire more information on mobile websites. Studies show that 80% of smart phone users want more product information when shopping on their mobile devices. A large part of m-commerce's appeal may be convenience, but if that convenience comes at the sacrifice of information, customers will be sure to look elsewhere. The larger trend here is that ultimately, businesses are in uncharted waters when it comes to their mobile offerings, they're still finding out what works and what doesn't.

BLUETOOTH

Bluetooth allows two devices to be connected to each other wirelessly. The most common use of Bluetooth technology is in hands-free devices such as headsets used with mobile phones. Bluetooth technology can also be used to transfer data between two electronics devices without using wires.

Bluetooth was invented in 1994 by Ericsson. The company later started working with a larger group of companies called the Bluetooth Special Interests Group, or "SIG," to develop the technology into what it is today. Bluetooth is not owned by any one company and is developed and maintained by SIG. The name Bluetooth came from a code name originally used by SIG for the project and is a reference to a 10th century Danish king named Harold Bluetooth, who was responsible for uniting Norway, Sweden, and Denmark.

Bluetooth technology was designed primarily to support simple wireless networking of personal consumer devices and peripherals, including cell phones, PDAs, and wireless headsets. Wireless signals transmitted with Bluetooth cover short distances, typically up to 30 feet (10 meters). Bluetooth devices generally communicate at less than 1 Mbps.

Features of Bluetooth Technology

Bluetooth technology uses radio waves to send information between two devices that are close to each other. Unlike traditional radio waves, Bluetooth waves typically can only travel 33 feet or less. Bluetooth networks feature a dynamic topology called a piconet or PAN. Piconets contain a minimum of two and a maximum of eight Bluetooth peer devices. Devices communicate using protocols that are part of the Bluetooth Specification.

Uses of Bluetooth Technology

Bluetooth is used is mobile phones, headsets, headphones, MP3 players, computers, boom boxes, laptops, computer mice, GPS units, and car stereos. Almost any Bluetooth device can be paired with another Bluetooth device in order to exchange information.

Benefits of Bluetooth Technology

Bluetooth technology enables two devices to be connected together wirelessly, eliminating the clutter and confusion typically associated with wires. Bluetooth can be used to allow users to make hands-free calls using their mobile phone and headset or speakerphone in their ear car. Bluetooth can also be used to connect a computer mouse to home computers, headphones to MP3 players, digital cameras to printers, and it can wirelessly send data from your computer to another device.

WI-FI

Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A common misconception is that the term Wi-Fi is short for "wireless fidelity," however this is not the case. Wi-Fi is simply a trademarked term meaning IEEE 802.11x.

The Wi-Fi Alliance, the organization that owns the Wi-Fi (registered trademark) term specifically defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards.

How Wi-Fi Works?

Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave propagation. A wireless network uses radio waves, just like cell phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here's what happens:

- A computer's wireless adapter translates data into a radio signal and transmits it using an antenna.
- A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection.

The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.

Features of Wi-Fi

WiFi has brought a new aspect in the ground of networking. The broadcast of data is completed via radio waves and the cost of cables for network lying down. Wi-Fi enables a user to get access to internet anywhere in the given location. Now you can make a network in Hotels, Libraries, colleges, universities, campus, private institutes, and coffee shops and even on a public place to make your business more profitable and connect with their client any time. Wi-Fi makes waves for business with their highly effective cable less media.

LESSON ROUND-UP

- The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies.
- The World Wide Web (abbreviated as WWW commonly known as the web), is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia, and navigate between them via hyperlinks
- A Web-browser is a piece of software that acts as interface between the user and inner workings of the internet specifically the World Wide Web
- Web addresses refers to particular pages on a web server which are hosted by company or organisation.
- Intranet refers to a private network which uses Internet technology and is designed to meet the internal information needs of the employees. It is accessible only by authorised employees, contractors and customers
- Extranet refers to private network which operates similarly to an intranet but is directed at customers or suppliers rather than at employees. Extranet provides information customers need such as detailed product description, frequently asked questions about different products, offices maintenance information warranties and how to contact customer service and sales office
- Electronic Mail is the abbreviated form of acronym e-mail. It is one of the most important applications of internet. Electronic mail (E-mail) is a fast and efficient method to exchange messages and other data
- The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.
- Electronic commerce or ecommerce is a term for any type of business, or commercial transaction that involves the transfer of information across the Internet. It covers a range of different types of businesses, from consumer based retail sites, through auction or music sites, to business exchanges trading goods and services between corporations. It is currently one of the most important aspects of the Internet to emerge. It is basically classified as

1. B2B or Business to Business refers to electronic commerce between businesses and also supplies chain technology, which is the largest and most successful e-commerce technology nowadays.
2. B2C or Business to Consumer refers to selling and buying of goods and services via the web.
3. C2C or Consumer to Consumer refers to online dealing of goods and services between people.
4. C2B or Consumer to Business is growing trend where consumers demand specific products or services from respective businesses by presenting themselves as a buyer group.

– A supply chain is a network of facilities and distribution options that performs the functions of procurement of materials, transformation of these materials into intermediate and finished products, and the distribution of these finished products to customers

– E-supply chain management (E-SCM) is the collaborative use of technology to enhance B2B processes and improve speed, agility, real-time control, and customer satisfaction. It involves the use of information technologies to improve the operations of supply chain activities (e.g., e-procurement), as well as the management of the supply chains (e.g., planning, coordination, and control)

– CRM (customer relationship management) is an information industry term for methodologies, software, and usually Internet capabilities that help an enterprise manage customer relationships in an organized way

– Electronic Data Interchange (EDI) is the computer-to-computer exchange of business documents in a standard electronic format between business partners.

– Electronic funds transfer is one of the oldest electronic payment systems and used for transferring money from one bank account directly to another without any paper money changing hands.

– M-commerce is a term that is used to refer to the growing practice of conducting financial and promotional activities with the use of a wireless handheld device.

– Bluetooth allows two devices to be connected to each other wirelessly. The most common use of Bluetooth technology is in hands-free devices such as headsets used with mobile phones. Bluetooth technology can also be used to transfer data between two electronics devices without using wires.

– Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections.

SELF-TEST QUESTIONS

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. What do you mean by the term ‘Internet’? State its basic applications.
2. What are the term internet and intranet? Are these the same? Discuss.
3. What is the mechanism being used by many communication to communicate with its suppliers/ customers? Discuss and state its difference with internet.
4. What are the differences between ‘Internet’ Intranet’ and Extranet? Explain.
5. What do you mean by electronic mail? State its basic features.
6. What do you mean by the term www? State its basic features and differences with internet.
7. What do you mean by ‘Internet Protocols’? State its basic characteristics.
8. What do you mean by e-commerce? State its various features.

9. Explain about different classifications of e-commerce.
10. Explain the application of e-commerce in supply chain management and customer relationship management.
11. What do you mean by the term e-security? Explain different dimensions of e-security and how to check the security threats.
12. What do you mean by EDI? State its characteristics and advantages.
13. What do you mean by the acronym 'EFTS'? Explain its basic features, advantages and security issues.
14. What do you mean by the term 'M Commerce'? Discuss about is future prospective.
15. Write short note on Bluetooth and Wi-Fi applications.

Lesson 8
Management Information Systems – An Overview

LESSON OUTLINE

- MIS Concepts
- Evolution & Elements of MIS
- Structure of MIS
- Characteristics of MIS
- Myths about MIS
- Computerized MIS
- Approaches to MIS Development
- Pre-requisites of an Effective MIS
- Impact of MIS on different levels of corporate management
- Constraints in operating MIS
- Limitation of MIS
- Miscellaneous Information Systems
- Entrusting MIS in a Corporate Enterprise

LEARNING OBJECTIVES

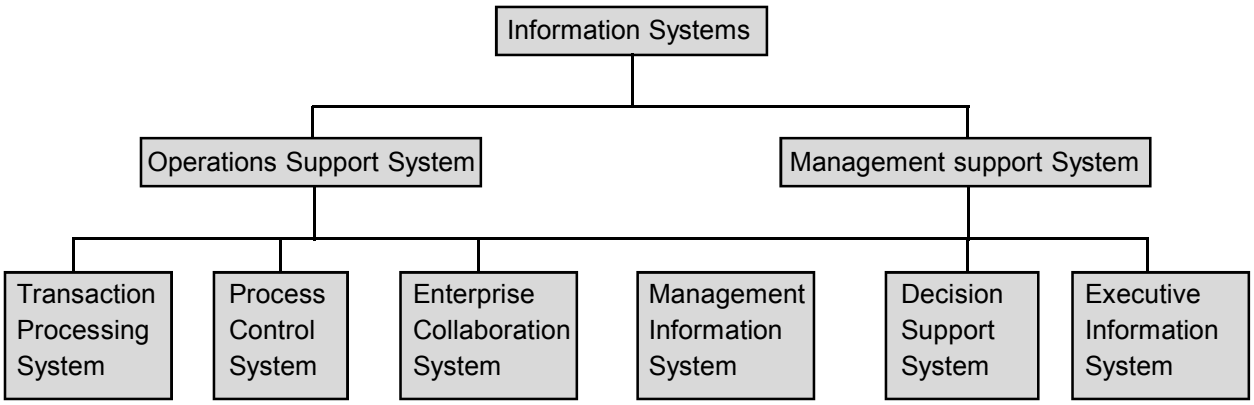
In present business scenario, specific, correct, integrated, reliable information is vital for success for an organisation. The success of a business decision depends on the reliability and correctness of the information. Management Information System provides the necessary information to different levels of management as per their specific needs. After going through this lesson, students will be able to

- Understand the basics of MIS: concepts, evolution, and characteristics.
- Understand the MIS requirements of different levels of management
- Review the MIS system of an organisation with respect to its appropriateness for the organisation
- Understand the basics of decision support system, artificial intelligence and expert system and their relation with MIS.

The objectives of an effective Management Information System (MIS) is providing Right Information to the right person at the right place at the right time in the right form at the right cost.

MIS CONCEPTS

Executives in an organization provide leadership and direction for planning, organizing, staffing, supervising, and controlling business activities. Each of these business activities involves decision making process. For making decisions, executives need the information. The required information is to be provided by information specialist or by data processing department. With the increasing competition in the era of information economy, the demands for organized, need base information is increasing day by day. Depending on the hierarchy the information need differs, accordingly different types of information systems are required. To achieve this goal, different types of information systems are devised by the organizations. The MIS is derived from these information systems used in the organizations A classification of various information systems is shown in the figure below. Through there are other information systems that also exists.



As it is shown MIS basically a part of information systems family. It is a pre specified reporting system for managers. It provides information to the managers in the form of routine reports. The main purpose of MIS is to provide timely, specific and accurate information at all levels in an organization. It is a broad concept rather than the single system. Some MIS activities are highly integrated with routine data processing, while other MIS applications are designed for a particular knowledge work activity or decision making function.

Major postulates of Management Information Systems are:

1. Information form of a MIS is periodic, exception and based on demands.
2. Information formats are pre-specified and fixed.
3. Information is provided by extraction and manipulation of operational data.
4. It provides information about the performance of the organization.
5. It supports the intelligence and implementation stages of decision making.
6. It supports structured decisions for operational and tactical planning and control.

MIS Requirements

A well-defined MIS provides information to all levels of management for the following purpose.

- To report the organization performance to tax authorities, shareholders, regulatory authorities and other stakeholders such as suppliers and customers etc.
- To prepare future plans for short and long term basis.
- To exercise day-to-day control on various operations in the different functional areas in the organization.

- To allocate different type of resources to different functional areas.
- To allow management by exception.
- To develop database of business partners and to devise procedures to deal with them.
- To develop the training tools for the new recruits in the organization at all levels.

EVOLUTION AND ELEMENTS OF MIS

IS is an age-old concept used to manage the various activities in the organizations. Before the emergence of electronic computing machine, it was existing in its manual form. It has been used as a mean to develop structured decision making processes in the organizations at all levels for internal as well as external controls. However, in early days specifically in a monopoly situation, it is being used as a tool of analyzing and developing routine reports mainly related to major parameters of business activities. These reports are simple and numeric in nature. In some cases, simple analysis relating achievements and targets is reported. But today in the era of information economy and free markets, the success of an organization largely depends on its information systems. As far as its evolution is concerned, it can be linked to the following four disciplines.

Management Accounting

The field of accounting consists of two major areas, i.e. financial accounting and management accounting. Financial Accounting is concerned with measurement of income for specific periods of time such as month or a year and the reporting of financial status at the end of the period. The first one is known as an income statement and other one as balance sheet. Though it is very important to see the status of finances but these two statements are of limited use as far as managerial decision making is concerned. In fact these statements are more relevant to the investors. The other branch of accounting, i.e., Management Accounting deals with relevant costs end other analysis useful for managerial control and managerial decisions. It employs techniques such as capital budgeting, break even analysis, transfer pricing etc. Its focus is on the preparation of budgets and measurement of performance based on the budgets. It is oriented towards internal controls and management decisions. Historically, accounting department was always responsible for data processing because the first application of processed data was related to accounting function. Management accounting information was used to carry analysis, to identify specific information requirement of executives for performing their functions in their respective departments. For example, to determine the break-even point, the information requirements are fixed costs, variable cost and the selling price of the product. To find out economic order quantity one needs to know carrying cost, holding cost, product demand for the year and purchasing cost/order cost.

These set of information are always a part of MIS, therefore the birth of MIS can be traced to management accounting. However, the support systems which provide users with access to data and models are beyond the scope of traditional management accounting.

Management Science/Operational Research

Management Science/Operational Research is the application of scientific method and quantitative analysis techniques to management problems. The use of management science methods emphasizes on the use of systematic approach to problem solving and application of scientific method to investigation. It utilizes mathematical models and mathematical and statistical procedures for analyzing problems. Finally, it aims at achieving optimal decision of optimum policy.

Management Science techniques were incorporated in the DSS which is a component of MIS, to make quantitative and analytical information available to the users of MIS. The information systems make use of models, and computer based solution algorithms. In addition, these systems provide quantitative information and procedures to facilitate model building for future plans and activities and to simulate the real situation even before they occur.

Management and Organization Theory

MIS is a support system for organizational functions; therefore, it draws upon concepts of organization, organization behavior, management, and decision making. The field of management and organization theory has provided many important concepts and philosophies which are key to understand the functions of MIS. Some of these concepts are:

- Behavioural theory of organizational and individual decision-making.
- Individual motivation.
- Group processes and group decision making.
- Leadership techniques.
- Organizational change process.
- Organizational structure and design.

There are several management theories-behavioural, empirical, decision, quantitative and management process. Out of these, decision, quantitative and management process are more relevant to us. According to decision theory, the most important task of managers is to make decisions.

The second theory known as "Management Process" is the most widespread approach of management. Under this, management is defined in terms of what managers do. According to this, management performs the functions of planning, organizing staffing, directing and controlling.

The knowledge of these management theories enabled the MIS designers to ascertain the type of decisions made and functions performed by executives in business organizations.

Computer Science

Computers were not originally planned for processing information but today this is the major use for which they are applied in business situations. The reasons for this are their speed of processing, calculating and retrieval of data. In fact, computer technology has been considered as a major factor in inducing MIS development. It has come as a significant tool in information processing and storage.

From the above discussion, it is quite apparent that MIS has been evolved from various disciplines in management. It maintained and provided the necessary information to its executives for planning, controlling and decision-making purposes. For example, control of inventory is an important management function. At the time when no integrated MIS was in use, perhaps the Inventory In-charge managed the function based on the information emanating from his department like the information that certain items have been exhausted or are nearing exhaustion. He would then have taken steps to replenish the stocks in the usual manner. However, with the development, the information which he needs now includes-cost of maintaining inventories, purchase schedule, economic order quantities, lead time, rate of consumption, etc.

In this approach of integrated MIS, management theories and specially the financial management concepts have contributed the enrichment. Further, when one has to manage a very large number of inventories here, he takes the aid of computer.

ELEMENTS OF MIS

MIS is a system that helps management in the process of decision making. The three elements of MIS are Management, Information and System. It is necessary to understand these three components:

Management

The term "Management" as defined by Marry Follett is "The art of getting things done through people" It also

refers to a set of functions and processes designed to initiate and coordinate group efforts in an organized setting, directed towards promoting certain interests, preserving certain values and pursuing certain goals. It involves mobilization, combination, allocation and utilization of physical, human and other needed resources in a judicious manner by employing appropriate skills, approaches and techniques. It is a process of conceiving and converting certain worthwhile ideas into results by getting things done through people by offering them monetary and other inducement in return for their contributions.

In short "Management" may be thought of as the sum total of these activities which relate to the laying down of certain plans, policies and purposes, securing men, money, materials and machinery needed for their goal achievements; putting all of them into operation, checking their performance and providing material rewards and mental satisfaction to the men engaged in the operation.

Information

It is a source for increment in knowledge. In MIS, it is obtained by processing data in to a form meaningful to the users. To illustrate, the concept, let us discuss the following situations; if somebody throws the word eleven during discussion, it means nothing to the participant. It is a data item, but it is placed within a context familiar to the intended recipient. Let us analyze another situation, if a manager is asking a question, "What are the sales of the packaged goods by marketing department and projection for the next quarter?" The answer would be 11 only. Here, it is information not the data item since the number 11 is being used in a context.

System

A physical system is a set of components that operate together to achieve a common objective or multiple objectives. These objectives are realized in the outputs of the system. An efficient system uses its inputs economically in producing its outputs. An effective system produces the outputs that best meet the objectives of the system. MIS can be thought of as a system (set of hardware, software, manpower, procedures, etc) to provide timely and accurate information to the management users in an organisation. The objective of the management information system is to provide formal informational support to the members of the organization.

STRUCTURE OF MANAGEMENT INFORMATION SYSTEM

Management Levels and their information needs

The levels of management consist of top, middle, and first line management (supervisory). The activities in the organizations are of three types:

- Strategic planning,
- Tactical and
- Operational.

Each of these levels to perform - strategic planning, tactical, and operational activities and requires different set of information. The activities and information needs of three levels of management are illustrated in the following.

1. Top level (Strategic level) Management and their information requirements

Top management is defined as a set of management positions, which are concerned with the overall tasks of designing directing and managing the organization in an integrated manner. They are responsible for interacting with representatives of the external environment, such as financial institutions, political figures, and important clients of the organization.

The structure of top level normally consists of Chairman and members of the Board of Directors, Chief Executive Officer and the heads of the major departments of the company. In fact, this level consists of those executives,

whose responsibilities relate to the whole organization or in other words, they are accountable for effectiveness and efficiency of the operations of the organization as a whole.

Top management's main responsibility is in the direction of determining the overall goals and objectives of the business. It deals mainly with long-term strategic plans, policy matters and broad objectives of the company. Also, it establishes a budget framework under which the various departments will operate.

Top management needs the information on the trends in the external environment (economic, technological, political and social) and on the functioning of the internal organizational sub-system. Apart from historical information, top management requires on-going or current information also which is generated through forecasts of the future. Thus, mostly the information utilized by top management is futuristic and external in nature. Much of the information so generated for strategic planning purpose tends to be incomplete and not fully reliable. It may not be available on time. For control purposes, top management receives summary and "exception reports" (For example on production, sales, cash, profits, and so on) from the middle management. The distinction between strategic planning information requirement and tactical information requirement is not always clear because both systems use some of the common information.

Characteristics of Information required for Strategic Planning

1. Ad hoc Basis: The information may be produced either regularly or periodically. For example, top management uses periodic accounting system reports such as the income statement, balance sheet, statement of sources and uses of funds, and capital statements in its planning functions. However, strategic planning information is more often produced when it is needed, on an ad hoc basis.

2. Unexpected Information: The information produced by the system may not be the same that was anticipated. For example, economic forecast information may be requested for the economy as a whole and for the industry in particular. The result of the economic forecast may be a surprise to the organization planners.

3. Predicted nature: The information produced is usually predictive of the future events rather than descriptive of past events. Long range planners try to set a course for an organization through an uncharted future. Their primary task is to choose a route that will improve the organization's level of success.

4. Summary Form: The information produced is usually not detailed but in summary form. Long range planners are not usually interested in detailed information; they are concerned with more global data. For example strategic planners may not be interested in the customer invoices but overall buying trends for their product vis-à-vis the product of the competitors.

5. External Data: A large part of data used for input to the system is acquired from the external sources. To mention, rate of borrowed capital, investment opportunities, demographic characteristics of a market group, and economic conditions etc. and the example of this type of information.

6. Unstructured format**:** The data used for input to the system may contain data that are unstructured in format. For example: forecasts of future stock market trends may be using the opinions of stock buyers, sales people, or market analysts obtained in casual conversations.

6. Subjectivity: The input to the system may be highly subjective in nature.

2. Middle level (Tactical level) Management and their Information Needs

level management is defined as a group of management positions, which tend to overlap the top and supervisory management levels in the hierarchy. Middle management positions consist of heads of functional departments and chiefs of technical staff and service units. Middle management, therefore, includes such people as the Manager of Sales, the Manager of Purchasing, Finance Manager, and the Manager of Personnel etc.

Middle management may be viewed as "administrative" management in the sense that it is responsible for the elaboration, classification and operationalization of organization goals, strategies and policies in terms of action

programmes and norms of performance. Middle management is concerned with the task of formulating pragmatic operating policies and procedures for the guidance of supervisory management.

The nature of information required at the middle management level is less diverse and complex. Middle management is fed with information both from top management and supervisory management. Much of the information used by the middle management is internal in nature. Middle management does not require much "futuristic" information since its decisions are not strategic and long range in nature. For example, the information needs of a sales manager are: corporate sales goals and targets, strategies and policies for operatinalising them, he also needs information on sales potential and trends in different market segments, geographical territories, competitive conditions and so on. Further, he needs information on weekly sales turnover from different zones and for different products, customer complaints, delay in dispatches, finished goods inventory position and the like for the purposes of control. Tactical Information Systems are designed to generate a variety of reports, including summary reports, exceptional reports, and ad hoc reports.

Characteristics of Information required for Tactical Planning

1. Predictive Nature: The information from a tactical system is sometimes produced periodically. For example, a branch credit manager for an organization may receive a weekly report showing the total dollar amount of accounts that are more than 60 days overdue, 90 days overdue, and in hands of a collection agency. The report might compare the three amounts with the same data from other branches of the organization. The same data can be compared for different time periods may be this year and last two years to see the trends. Based on this information, credit manager can decide whether the overdue account totals are within the normal range for the branch or whether the difference between the amounts warrants special managerial action or decisions. Thus, this information system provides the means by which the credit manager can quickly identify problems and bring them under control. On the other hand, tactical information systems can produce information when it is needed on ad hoc basis.

2. Unexpected Findings: The information provided by a tactical information system may not be the information that was expected to be produced. For example: querying an accounting system database, a manger can find the characteristics of major customer related to credit difficulty. It may have relation with customer position and type of employer. Investigation may reveal that overdue problem is with those customers whose employer had a cut in its workforce. The unemployment of these customers is creating an overdue problem. As a credit agency, it has to analyze the purchasing of these customers as a fresh.

3. Comparative Nature: The information produced is usually comparative in nature rather than merely descriptive. They provide managers with information that alerts them to major variation from the accepted standards. These types of information systems are similar to the control process systems that monitor output of the system continuously and provide feedback when output parameters are at variance with accepted standards.

4. Summary Form: The information produced is not detailed but is in summary form, however, in comparison to the strategic planning systems, it may be more elaborate. For example: a credit manager is not interested in a detailed listing of each customer account and its balance. In large organizations, there would be an enormous quantity of data and would not, therefore, be information to the manager. The manager needs information relating to credit performance or balances of accounts that are overdue or in collection.

5. Both External and Internal Sources: The data used, as input to the system may not always confine to sources internal to the organization. It may be from external sources also. For example: the credit manager may compare the information pertaining to problems to other branches, to other periods from the same organization, or to a goal set up by top management. The credit manager may like to compare sometimes it with the experience of the whole industry.

Supervisory level (Operational level) Management and their Information Needs

Supervisory management is defined as a team of management positions at the base of the hierarchy. It consists

of section officers, office managers and superintendents, foreman and supervisors who are directly responsible for instructing and supervising the efforts of rank and file, clerical and "blue-collar" employees and workers. Supervisory management is also called operation management" in the sense that it is concerned with implementing operational plans, policies and procedures for purposes of conversion of inputs into outputs. At the supervisory level, managers are responsible for routine, day-to-day decision and activities of the organization, which do not require much judgement and discretion. The function and process of the supervisory management are standardized as far as possible. The perspective of supervisory management is generally short-range and insular. It functions in a relatively closed environment.

Supervisory management mostly needs internal information on operational aspects of the functioning of activity units. It in fact, generates internal information for example, on purchase and sales, production, use of inputs etc. at the operating level. It also receives information from the middle management levels on operational plans and programmes. The nature of information is routine and structured. It tends to be reliable and relatively complete. There is little element of complexity of uncertainty involved in the information.

Characteristics of Information required for Supervisory Planning

1. Repetitiveness: The information produced by these systems is usually repetitive in nature at periodic intervals such as daily, weekly, or monthly.

2. Predictability: The information they produce usually does not contain any surprises any surprises for the manager or the users of the information. These systems produce results at the expected time. For example: People are paid by the system what they are expected to be paid and customers are billed for what they purchased.

3. Emphasis on the past: The information generated by the systems usually describes the past. For example: payroll accounting systems describes the work done by the employees in the past for which they are being paid. Invoices describe past sales to customers.

4. Detailed nature: The information produced is very detailed. To mention, as an example, pay-checks provide detailed information on the work week of each employee along with all allowances and deductions. Customer invoices describes the details of purchases.

5. Internal origin: The data for operational system usually spring entirely from internal sources. That is data for pay-checks come from internal documents of the organization.

6. Structured form: The form of the data input and the form of the output produced by the operational information systems is structured. That is the data on time cards are carefully formatted in identical fashion on each. Or the data on each customer invoice are carefully formatted in identical fashion.

7. Great accuracy: The accuracy of the data used as input to such systems and of the output produced by such systems is usually very high. The data input and information output are carefully checked in a variety of ways.

Comprehensive Structure of MIS

The structure of a MIS is known as comprehensive if it possesses the following characteristics:

- It should be closely directed by management.
- It should integrate various sub-systems of the management.
- It should avoid duplication and redundancy of data.
- It should make the dissemination of information an effective one.
- It should be capable of meeting the information requirement of managers at different functions.

Taking into consideration the above characteristics, the suitable structure of a comprehensive MIS may be a federation of information sub-systems for different functions, viz. production, material management, marketing,

finance, engineering and personnel. Each sub-system of information system is supposed to provide information support to executives for operational control, management control and strategic planning.

The MIS structure can be described in terms of support for decision making, management activity, and organizational functions. These three approaches are synthesized into MIS structure.

MIS is nothing but a conceptual framework that allows one to describe an existing or planned information system. Physical structure defines the way of implementing the MIS. Both the structures are described here.

Conceptual Structure of MIS

It is defined as a federation of functional units, each of which embedded with four major information processing components: Transaction processing, operational control information system support, managerial control information system support, strategic planning information system support. Each of the subsystem of the information system has some unique data files, which are used only by that subsystem. There are files that need to be accessed by more than one application and need to be available for general retrieval. These files are organized in the form of a database, which is managed by the data base management system.

A further amplification of the structure is the introduction of common software. In addition to application programs written especially for each subsystem, there are common applications, which serve multiple functions. Each subsystem has linkages to these common applications. Severals models are available which can be used by many applications.

The information requirement of executives for operational control, management control and strategic planning itself depend upon-operational function, level of management activity and type of decision-making. Different operational functions have different information requirements. Their information requirements vary not only in content but in characteristics as well.In fact, the content of information depends upon the activities to be performed under an operational function. Also an operational function influences the characteristics which a particular information must possess. For example, the information used for preparing employees payroll by the accounts department should be highly accurate.

The level of management activity too influences the characteristics of information. For example, strategic planning requires more external information and information on the behavior of relevant and likely future events. Management control requires more accurate, precise, current and repetitive information. Operational level requires information in detailed form about the performance.

The information or data requirements of each sub-system can be met by developing two types of data files, viz., unique and common. Unique data files may meet the specific information requirements of each operational function at different level of management activity for making programmed and non-programmed decisions. Common data file, stores data/information meant for general use in the decision-making process. The data stored in the data files is usually in the raw form and thus, requires processing. Processing of data may be performed by using softwares and decision models kept under model base. The use of data, in database may be controlled by Data Base Management System.

A conceptual make up of MIS is basically the visualization of all discussed sub systems their data requirements, processing, to allow a smooth generation and flow of information as required by different users.

Physical Structure of MIS

The physical structure of an MIS is the application of all the conceptual development for the purpose. It is identical to the conceptual structure in the sense that conceptual structure works on a theoretical plane while physical system works on an empirical plane.

Integrated processing of data is required for achieving MIS goals. Physical execution is achieved by designing several related applications as a single system in order to simplify the interconnections and reduce duplication

of input. A good example is an order entry system. The recording of an order initiates a sequence of processing, each step using new data but also much of the data from processing. A large number of documents and reports are prepared from the initial entry of the order plus later entry of actual quantity shipped, freight, amounts received on account, and returns and allowances. An integrated order entry system crosses functional boundaries.

Issues of MIS Structure

One of the important issues regarding the structure of MIS is an existence of informal information systems. There are both formal and informal systems within organization systems. Documents and other records, usually indicating compliance's with pre-specified rules and procedures manifest the formal system. The informal systems may process information that is vital to organizational functioning but without formal records of that process.

CHARACTERISTICS OF MIS

Some of the main characteristics of MIS are listed as under.

1. Comprehensiveness: Management Information System is comprehensive in nature. It takes inputs from transactions processing systems and process information primarily for managers at all levels. It caters to the need of large variety of people in different hierarchy as routine information requirement exist practically at all levels. Therefore reporting system in the form of MIS is most sought after information system in any organization.

2. Co-ordinated: Management information system is centrally co-ordinated to ensure that information is passed back and forth among the sub-systems as needed and to ensure that information system operates efficiently.

3. Sub-systems: A MIS is composed of sub-systems or quasi separate component system that is the part of the overall - unified system. Each of these systems shares the goals of the management information system and of the organization. Some of the systems serve just one activity or level in the organization, while others serve multi-levels or multiple activities. The overall structure of the multiple systems should be carefully established as a part of long range system planning.

4. Integration: A MIS is rationally integrated, so as to become more meaningful. Sub-systems are integrated so that the activities of each are inter-related with those of the others. This integration is accomplished primarily by passing data between these systems. Computer programmes and files can be designed to facilitate data flows among the systems, and manual procedures are also used to accomplish this integration. While integration makes information processing more efficient by reducing both intermediate processing and the incidence of independent generation of the same data by multiple departments, an even more important benefit is that it provides more timely, complete and relevant information. Senior managers particularly, benefit from integrated systems because they need cross functional information. Although total information of sub-systems is neither achievable nor desirable, a substantial degree of integration is required for an effective management information system.

5. Transformation of Data into Information: A MIS transforms data into information in variety of ways. When data is processed and is useful to a particular manager for a particular purpose, it becomes information. There are many different ways in which data must be transformed within an information system. For example, cost data for a particular organization may be summarized on a full-cost, variable-cost, and standard-cost basis for each organization unit, as well as by each cost type, customer type, and product, line. The numerous ways in which MIS should transform data into information are determined by the characteristics of the organizational personnel, the characteristics of the task for which information is needed.

6. Enhance Productivity: A MIS enhances productivity in several ways. It enables routine tasks such as document preparation to be carried out more efficiently, it provides higher levels of service to external organizations and individuals, it supplies the organization with early warnings about internal problems and external threats, it gives early notice of opportunities, it facilitates the organization's normal management processes and it enhances managers' ability to deal with unanticipated problems.

7. Conforms to Managers' Styles and Characteristics: A management information system is developed in recognition of the unique managerial styles and behavioural patterns of the personnel who will use it, as well as the contributions made by managers. At the organization's more senior levels, the management information system is likely to be carefully tailored to each individual manager's personal tastes. At the organization's lowest levels, the management information system is more likely to be tailored to the unusual way in which clerical and operations personnel use information and interact with the information system. For middle managers, the information system is tailored to the general characteristics of managers. For professional and technical personnel, the information system is tailored to the nature of the specialized task, but with attention also given to the way the minds of these specialists process information.

8. Relevant Information: A MIS should provide only relevant information. Determining what information is relevant may be difficult in situations in which analyses vary for different managers or according to particular circumstances, such as in the case of special problems. Systems designers must carefully consider the human factor when developing a management information system. Otherwise, the resulting system will be ineffective and probably will be discarded by its users.

9. Uses Established Quality Criteria: A management information system must be designed to the required tolerance for timeliness, relevance, and accuracy of information. These tolerances vary from task to task and from level to level within an organization.

10. Feedback: A management information system should provide feedback about its own efficiency and effectiveness. The reporting of computer malfunctions and transactions processing error rates is a simple example of this feedback. Statistics prepared by the system about who uses each system facility and how much they use each one are more sophisticated forms of feedback. Computer programs can record and report how much computer time is used by each user, how many pages are printed for each user, and how much internal data file space is utilized by each user's data, as examples; these and other usage statistics can be used for managerial analysis or as basis for charging each user for computer usage if desired.

11. Flexibility: It must be designed to be easily modified if, for example, different information is needed because the environment changes or if the organization undertakes new activities (such as introducing new products) which require new modes of processing. The information system should be capable of being easily expanded the accommodate growth or new types of processing activities and also easily contracted.

12. Modularity: The MIS should be composed of many modules or sub-systems rather than be designed as one and only one for a few large systems.

13. Selective Sharing of Data: Another desirable quality of an MIS is selective sharing of data. Two or more managers often need to utilize the same information; the system should have features, which allow ready access to information by multiple managers. An advanced feature that promotes this sharing is data bases. On the other hand, it is often important to reserve certain information for the exclusive use of only selected managers. Sometimes, this need extends down to the record or field level, in which case some parts of a record are available to all managers, but only certain managers permitted to examine other parts. For example, an employee's current address or marital status may be needed by employee or other personnel, but access to information about pay rate, hours worked, gross pay, and other details of payments may be restricted to certain payroll managers. This selective sharing quality can be established by controls that are part of the computer programs.

14. Computerized: It is possible to have a MIS without using a computer. But its use increases the effectiveness of the System. In fact, its use equips the system to handle necessary attributes of the computer to MIS, for example accuracy and consistency in processing data and reduction in staff. These needs in management information system make the computer a prime requirement.

MYTHS ABOUT MIS

Let us clarify some of the misconceptions or "myths" about MIS:

1. The study of management information system is about the use of computers: This statement is not true. MIS may or may not be computer based, computer is just a tool. Whether it should be used while installing a MIS depends largely on several factors, e.g., how critical is the response time required for getting an information; how big is the organisation, and how complex are the needs of the information processing.

2. More data in reports means more information for managers: This is a misapprehension. It is not the quantity of data, but its relevance, which is important to managers in the process of decision-making. Data provided in reports should meet information requirements of managers. It is the form of data and its manner of presentation which is of importance to business managers. Unorganised mass of data bring confusion.

3. Accuracy in reporting is of vital importance: The popular belief is that accuracy, in reporting should be of high order. At the operating level, it is true. Other examples, where accuracy is really important can be; the dispensing of medicine; the control of aircraft; the design of a bridge etc. Accuracy, however, is a relevant but not an absolute ideal. Higher levels of accuracy involve higher cost. At higher decision levels, great accuracy may not be required. The degree of accuracy is closely related to the decision problem. Higher management is concerned with broad decisions on principle and objective. A fairly correct presentation of relevant data often is adequate for top management decision. For a decision, on a few project proposals top management is not interested in precise rupee terms of the project cost. A project cost estimated at a fairly correct figure is all what it wants.

Basic Requirement of MIS

In the present context, most of the organizations are using computer-based management information system in the era of information economy. The basic requirements of a computer based MIS are listed as below :

1. Hardware: It refers to the physical computer equipment and associated devices. The hardware must provide five basic functions, i.e., input of data entry, output, secondary storage for data and programmes, central processor (Computation, Control, and primary storage) and communication.

2. Software: It is a broad term; it means the instructions or programs that direct the operation of the hardware. The software can be classified into two major types: System Software and Application Software.

3. Database: The database contains all data utilized by the application software. An included set of stored data which is often referred to as file. The physical existence of the stored data is known as database.

4. Procedures: Formal operating procedures are physical components because they exist in a physical from such as a manual or instruction booklet. Basically, three major types of procedure are required:

- User Instructions (for users of the application to record data, employ a terminal to enter or retrieve data, or use the result)
- Instructions for preparation of input by data preparation personnel
- Operating instructions for computer operations personnel.

5. Operations Personnel: It includes personnel such as Computer operators, system analysts, programmers, data preparation personnel.

COMPUTERIZED MIS

The notion management Information System refers to the formal system installed in an organization for purposes of collecting, organizing, storing and processing data and presenting useful information to management at various levels. It serves as an aid to managerial functions of planning and control. Many medium sized and large

enterprises find it convenient to computerize their MIS to make it automatic and highly organized. The advent of high-speed electronic computers has proved to be a boon to organizations for making their Management Information Systems very sophisticated and efficient by computerizing them. The vary character and content of MIS have undergone significant changes as a result of computerization; so much so, MIS has almost come to mean computer based MIS. There are non-computer-based management information systems also.

Features of Computer based MIS

1. Organization and updating of huge mass of raw data of related and unrelated nature derived from internal and external sources at different period of time.
2. Ability to process data into information with accuracy and high speed. It involves making complex computations, analysis, comparisons and summarization's. Though humans can do the processing, the computer's ability to process huge data is phenomenal, considering its speed, reliability and faithfulness in perfectly following the set of instructions.
3. Super-human memory, tremendous volume of data and information and the set of instructions can be stored in the computer and can be retrieved as and when needed. Management can get any bit of stored information from the computer in a matter of seconds.
4. The input data in the computer can be processed into a number of different outputs and for a variety of purposes. The system is so organized that managers at different levels and in different activity units are in a position to obtain information in whatever form they want, provided that relevant "Programmes" or instructions have been designed for the purpose.
5. The information processing and computer technology have been so advanced that managers are able to obtain real time information on-going activities and events without any waiting period.
6. Computer based MIS opens up new vistas for management to make efficient timely decisions on vital operations of the enterprise and major strategic and tactical problem. It also helps organizations to gain substantial economies by reduction of clerical and computational time.

APPROACHES TO MIS DEVELOPMENT

For developing MIS following three approaches are used.

Top down approach

The development of MIS under top down approach begins by defining the objectives of the organization, the kind of business it is in, and the constraints under which it operate. The activities or functions for which information would be required are also identified. The crucial strategic and tactical decisions are also defined and the decisions necessary to operate the activities are specified. From the activities or functions and the decisions to be made, the major information requirements are ascertained.

This approach develops a model of information flow in the organization, which acts as a guide for designing the information system. By using the model of information flow various information sub-systems may be defined. Each sub-system comprises of various modules. A module is a basic unit for information system's development. The selection of module for developing system is made on the basis of the priority assigned to them. The various sub-systems and their modules are coordinated to achieve the objective of integration. The information system so developed is viewed as a total system fully integrated rather than as a collection of loosely coordinated sub-systems.

As the name indicates, top management takes the initiative in formulating major objectives, policies and plans in a comprehensive manner and communicates them down the line to middle and supervisory management levels for translating them into action plan. This approach only concentrates on implementation and day-to-day control.

Bottom up approach

The development of information system under this approach starts from the identification of life stream systems. Life stream systems are those systems, which are essential for the day-to-day business activities. The examples of life stream systems include - payroll, sales order, inventory control and purchasing etc. The development of information system, for each life stream system starts after identifying their basic transactions, information file requirements and information processing programs.

After ascertaining the data/information requirements, files requirements and processing programs for each life stream system, the information system for each is developed. The next step is towards the integration of data kept in different data files of each information system. The data is integrated only after thoroughly examining various applications, files and records. The integrated data enhances the sharing ability and evolving ability of the database. It also ensures that uniform data being used by all programs. Integrated data also provides added capability for inquiry processing and ad hoc requests for reports.

The next development under bottom up approach may be the addition of decision models and various planning models for supporting the planning activities involved in management control. Further, these models are integrated to evolve model base. The models in the model base facilitate and support higher management activities. They are useful for analyzing different factors, to understand difficult situations and to formulate alternative strategies and options to deal them.

A comparison of top down and bottom up approaches reveals the following points:

- Top management takes the main initiative in formulating major objectives, strategies and policies, for developing MIS under top-down approach. In the bottom up approach it is the supervisory management who identifies the life stream systems for which MIS may be developed.
- Middle and supervisory management levels have a little role in the development of system under top down approach. Under bottom up approach, management refrains from guiding the development of system developed by supervisory level.
- The information system developed under top down approach is more consistent with the systems approach and is also viewed as a total system, which is fully integrated. The information system developed under bottom up approach is developed through an orderly process of transition, building upon transaction processing sub-system. This system may not be integrated.

Integrated Approach of MIS Development

If used objectively, it can overcome the limitations of the above two approaches. This approach permits managers at all levels to influence the design of the system. Top management will identify the structure and design of MIS suitable to the concerned department. The design is presented to the lower level management for their views and modification. The lower management is permitted to suggest changes, additions, or deletions and return the design with their suggestions to the top level for approval. The revised design is drawn and evaluated by the top level and sent down again in a modified form for further consideration if required. This is an iterative process. It continues until a final design is achieved, that satisfies the requirement at all levels in the organization.

PRE-REQUISITES OF AN EFFECTIVE MIS

The pre-requisites of an effective MIS are nothing but mainly its resources and management support. These are described in the following section :

Qualified Systems and Management Personnel: One of the important pre-requisites of well-defined MIS is that qualified personnel's at all levels should man it. These experts should take into account views of their fellow employees. The personnel's of the MIS comprises of at least two category of personnel viz.:

(i) Systems, communication, and Computer Experts;

(ii) Management Experts.

Systems, communication and computer experts should also be capable of understanding management concepts to facilitate the understanding of problems faced by the concern. They should be well versed with the process of decision making and information requirements for planning and control functions. Management experts on the other hand should also understand clearly the concepts and operations of a computer. This basic knowledge of computer based systems will be useful to the management experts and will help them in understanding the problems of another category of experts. This will help the management in dealing with hiring suitable experts, recruiting fresh candidates and developing them to meet the specific requirement of the organization. Top management in the organization should also take in to account the turnover of the experts in the field of MIS. In addition, there is a third category of the personnel's who are very important and they are the users of the system.

Database

The word is now taking new name such as data warehouse, which is being used presently in, large corporates. Database is consolidation of many files, which contain the data of the organization. The data in a database is organized in such a way that access to the data is improved and data redundancy is reduced. It also increases the data integrity.

The main feature of database is that all subsystems will utilize the same database kept in different files. The other important features of databases are:

I. Avoiding uncontrolled data redundancy and inconsistency: Application shares the data stored in a database, rather than owning private files that would often store redundant data. This reduces the storage costs; there is no need to update multiple copies of the same data. This prevents the possibility that inconsistent data will reside in multiple files.

II. Program-Data Independence: When the database is managed by a DBMS, programs can be written independent of the actual physical layout of the data or even of the total logical structure of the data. DBMS knows these structures; it thus provides the mapping from a logical view of the data in a given application to the actual physical layout of the data on the storage device.

III. Flexible Access to shared data: The database approach has opened data for access to users and applications. Query languages enable end users to access data directly. Applications can be written to use any data stored in corporate databases, rather than to rely only on specially created files.

IV. Reliability: The reliability of the stored data is ensured by the DBMS managed databases themselves, rather than by special programming. A variety of relationships between entities may be rather easily defined.

V. Centralized Control of data: There are many advantage of centralized control of database: Few are listed in the following:

(a) Global planning and consist evolution of the data resources are possible.

(b) Security may be maintained by specifying the authorization for data access and modification to the uniform interface for all programs and users- that is to the DBMS; these security measures may be employed to protect the privacy of individuals i.e. the stored data of the concern.

(c) Integrity constraints may be imposed to further ensure the accuracy of data in the database.

(d) Corporate wide standards can be enforced in naming and representing the data.

Support of Top Management

For a MIS to be effective, it should receive full support of top management. The basic reason for this is that the resources involved in computer based information system are large and growing larger and larger in view of the importance of technology in the present context. To get these resources for implementing the MIS, the support of top management is essential.

Control and Maintenance of MIS

Control of the MIS means the operation of the system as it was designed to operate. Sometimes, users develop their own procedure or short cut methods to use the system, which reduces its effectiveness. To check such habits of users, the management at each level in the organization should devise methods for information control. Maintenance is closely related to control. During the maintenance systems management will discover needs for improvement in the system. However, formal methods of changing and documentation have to be identified by the management.

Evaluation of MIS

An effective MIS should be capable of meeting the information needs of its executives in future as well. To maintain this capability evaluation of MIS and timely action thereof is required. The evaluation of MIS should take in to account the following:

- Flexibility in built, with the system to meet any expected and unexpected information requirement in future.
- Ascertaining the views of the users and the designers about the capabilities and deficiencies of the system.
- Guiding the appropriate authority about the steps to be taken to keep the effectiveness of MIS alive.

COMPUTER AND ITS EFFECT ON MIS

The effects of applying computer technology to information systems can be listed below:

1. Increase in speed of processing and retrieval of data: Modern business situations, are characterized by, high degree complexity, keen competition and high risk and reward factors. This invariably calls for system capable of providing relevant information with minimum loss of time. Manual systems howsoever well organized often fail to match the demand for information for decision-making. Computer with its unbelievably fast computational capability and systematic storage of information with random access facility has emerged as an answer to the problems faced by management. Processing of data in relevant form and design and retrieval of it, when needed, in fact requires considerably less time and facilitate the management action and decision-making. The speed of computer processing is in nano-range, i.e.; an operation takes only billionths of a second. This characteristic of computer has accounted for as a major factor in inducing MIS development. Computers today are capable of meeting varied type of information requirement of executives.

2. Expanded Scope of use of information system: The importance and utility of information system in business organizations was realized by most of the concerns, after the induction of computers for MIS development. System experts in business organizations develop areas and functions, where computerized MIS could be used to improve the working of concern. This type of applications hitherto, not feasible under the manual system. For example, it was made possible by using an on line real time system to provide information to various users sitting at a remote distance from a centrally located computer system.

3. Widened scope of analysis: The use of computer can provide multiple type of information accurately and in no time to decision-makers. Such information equips an executive to carry out a thorough analysis of the problem

and to arrive at the final decision. Computers are capable of providing various types of sales reports for example, Area wise sales; Commission of each sales man; product wise sales etc. These reports are quite useful in analyzing the sales department working and to ascertain their weaknesses, so that adequate measures may be taken in time. In this way, the use of computer has widened the scope of analysis.

4. Complexity of system design and operation: The need for highly processed and sophisticated information based on multitudes of variables has made the designing of system quite complex. During the initial years, after the induction of computer for MIS development, systems experts faced problems in designing systems and their operations. The reason at that time was the non-availability of experts required for the purpose. But these days the situation is better. The manufacturers have developed some important programs (software) to help their users. Some private agencies too are there who can perform the task of developing programs, to cater the specialized needs of their customers, either on consultancy basis or on contract.

5. Integrates the working of different information sub-systems: A suitable structure of management information system may be a federation of information sub-system, viz., production, material, marketing, finance, engineering and personnel. Each of these sub-systems is required to provide information to support operational control, management control and strategic planning. Such information may be made available by common-data-base. This common-data -base may meet out the information requirements of different information sub-system by utilizing the services of computers for storing, processing, analyzing and providing such information as and when required. In this way, computer technology is useful for integrating the day-to-day working of different information sub-systems.

6. Increased the effectiveness of information systems: Information received in time is of immense value and importance to a concern. Prior to the use of computer technology for information purposes, it was difficult to provide the relevant information to business executives in time even after incurring huge expenses. The use of computer technology has overcome this problem. Now, it is quite easy to provide timely, accurate and desired information for the purpose of decision-making. Hence, we can conclude, that the use of computer has increased the effectiveness of information system also.

7. More comprehensive information: The use of computer for MIS, enabled system experts to provide more comprehensive information to executives on business matters.

IMPACT OF MIS ON DIFFERENT LEVELS OF CORPORATE MANAGEMENT

Top level of corporate management spends mostly it's time for business planning. The major responsibilities of this level include long and short-range planning, resource and capacity analysis, setting of profit and budget goals, and in general establishing the business objectives of the company. It is thus apparent that there is a heavy planning and lesser control element in the work domain of top level management.

Presently, the impact of computers and MIS on the working of this level is minimum. The reasons for lesser computer effect on top level are:

(i) Unstructured nature of data

(ii) Slow acceptance and use of operations research techniques

(iii) Non-availability of suitable systems and computer experts

(iv) Reliance on intuitive abilities.

The impact of MIS on top level too is far less than at the middle or supervisory level. This fact is apparent from the following table, which has been constructed on the basis of several surveys.

	Decision Making Process	Job Contents	Job Members
Top Management	Scant Influence	Scant Change	No Influence
Middle Management	Moderate Influence	Moderate Change	Scant Influence
Lower or Supervisory level	Major Influence	Major Change	Moderate Influence

In fact MIS in its present form is more effective for control than for planning. Therefore, it can be concluded that the impact of MIM on top management level is almost non-existent.

The potential impact of computers on top level management may be quite significant. An important factor, which may account for this change is the fast development in the area of computer science. It is believed that in future computers would be able to provide simulation models to assist top management in planning their work activities. For example, with the help of a computer it may be possible in future to develop a financial model by using simulation technique, which will facilitate executives to test the impact of ideas and strategies formulated on future profitability and in determining the needs for funds and physical resources. By carrying sensitivity analysis with the support of computers, it may be possible to study and measure the effect of variation of individual factor to determine the final results. Also the availability of a new class of experts will facilitate effective communication with computers. Such experts may also play a useful role in the development and processing of models. In brief, potential impact of computers would be more in the area of planning and decision-making.

Futurists believe that in future top management will realize the significance of techniques like simulation, sensitivity analysis and management science. The application of these techniques to business problems with the help of computers would generate accurate, reliable, timely and comprehensive information to top management. Such information will be quite useful for the purpose of managerial planning and decision-making. Computerized MIS will also influence in the development, evaluation & implementation of a solution to a problem under decision-making process.

The impact of computers and MIS on middle management is moderate. This level of management translates the management objectives into plans, arranges resources to achieve such objectives and goals as laid down by top management. Also it reviews the result of operations performed at the supervisory level. It thus acts as a bridge between the other two levels. The information provided by computer serves only limited purpose to middle management. Such information is quite effective for carrying out an analysis of the operations but has little impact on the formulation of organizational plans.

Potential impact of computers and MIS on middle management level will be significant. It will bring a marked change in the process of decision-making. At this level, most of the decisions will be programmed and thus will be made by the computer, thereby drastically reducing the number of middle level manager's requirement. For example, In the case of inventory control system, computer will carry records of all items with respect of their purchase, issue and balance. The reorder level, reorder quantity etc. for each item of material will also be stored in computer after its pre-determination. Under such a system as soon as the consumption level of a particular item of material will touch reorder level, computer will inform for its purchase immediately. The futurists also foresee the computer and the erosion of middle management as the vehicles for a major shift to decentralization. The new information technology will enable management to view an operation as a single entity whose effectiveness can only be optimized by making decisions that take into account the entity and not the individual parts.

The impact of computers and MIS today at supervisory management level is maximum. At this level, managers are responsible for routine, day to day decision and activities of the organization, which do not require much judgement and discretion. In a way, supervisory mangers job is directed more towards control function, which are highly receptive to computerization. For control, such mangers are provided with accurate, timely, comprehensive and suitable reports. A higher percentage of information requirements of executives are met out at this level.

Potential impact of computers and MIS on supervisory level will completely revolutionize the working at this level. Most of the controls in future will be operated with the help of computers. Even the need of supervisory mangers for controlling the operation/activities now performed manually will be either fully or partially automated.

In future MIS would provide highly accurate, precise and desired information to control operations with the support of computers.

CONSTRAINTS IN OPERATING A MIS

Major constraints which come in the way of operating an information system are the following :

1. Non-availability of experts, who can diagnose fully the objectives of the organisation and give a desired direction needed for operating information system.

2. Difficulty usually faced by experts, in selecting the sub-systems of MIS, to be designed and operated upon first.

3. Source of availability of experts for running MIS effectively, is not always known to management.

4. Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is non-standardised one.

5. Non-availability of cooperation from staff.

6. Non-availability of heavy financial resources required for running the MIS effectively.

7. Turnover of experts is quite high.

8. It is difficult to quantify the benefits of MIS, so that it can be easily comparable with cost.

9. Perception problems as its utility are not readily perceptible by many users.

LIMITATIONS OF MIS

1. The main limitations of MIS are as follows:

2. The quality of the outputs of MIS is basically governed by the quality of inputs and processes.

3. MIS is not a substitute for effective management .It means that it cannot replace managerial judgement in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision-making and problem solving.

4. MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in the fast changing and complex environment.

5. MIS cannot provide tailor made information packages suitable for the purpose of every type of decisions made by executives.

6. MIS takes into account mainly quantitative factors; thus it ignores non-quantitative factors like morale, attitudes of members of the organization, which have an important bearing on decision-making process of executives.

7. MIS is less useful for making non-programmed decision-making. Such type of decisions is not of routine type and thus they require information, which may not be available from existing MIS to executives.

8. The effectiveness of MIS is reduced in the organization, where the culture of hoarding information and not sharing with others hold.

9. MIS effectiveness decreases due to frequent changes in top management organizational structure and operational team.

MISCELLANEOUS INFORMATION SYSTEMS

Transaction Processing Systems (TPS)

A data processing system processes transactions and produces reports. It represents the automation of fundamental, routine processing to support operations. Prior to computers, data processing was performed manually or with simple machines. A management information system is more comprehensive; it encompasses processing in support of a wider range of organizational functions and management processes. However, every MIS will also include transaction processing as one of its functions.

What does it takes into account to make a data processing system into a management information system? Can a rather mundane data processing system be a MIS if a simple database, retrieval capabilities, and one or two decision models are added? This is not a useful question. MIS is a concept and an orientation toward which an information system design moves rather than an absolute state. Therefore, the significant issue is the extent to which an information system adopts the MIS orientation and supports the management functions of an organization. The answer is usually a matter of degree rather than a simple yes or no.

One important aspect of the difference between MIS and routine data processing is the capability to provide analysis, planning, and decision making support. An MIS orientation means users have access to decision models and methods for querying the database on an ad hoc basis; the database is also, of course, an essential part of routing transaction processing and reporting. Furthermore, a MIS orientation means information resources are utilized so as to improve decision-making and achieve improved organizational effectiveness. Information resources are also used as a means of achieving a competitive advantage.

Decision Support Systems (DSS)

It is computer based information system that combines data, analytical tools, and user-friendly software to support decision-making at the management level. A decision support system (DSS) is an information system application that assists decision-making. DSS tend to be used in planning, analyzing alternatives, and trial and error search for solutions. They are generally operated through terminal-based interactive dialogs with users. They incorporate a variety of decision models.

DSS are more targeted than MIS System. MIS systems provide managers within routine flow of data and assist in the general control of the organization. In contrast, DSS are slightly focused on a specific decision of classes of decision such as routing, querying, on three basic parameters which are given in the following :

(i) **Philosophy**: DSS provides integrated analytical tools, data, model base (a collection of mathematical and analytical models), and a interface to the user in the form of a user friendly software, MIS provides a structured information to the end-users at all level in an organization.

(ii) **System Analysis**: DSS establish what tools are used to incorporate the decision making Process of a organization. Whereas MIS identify information requirement at different levels in the organization.

(iii) **Design:** The design of DSS is based on Iterative Process and keeps on changing with every feedback of the user. On the other hand, MIS deliver a system based on frozen requirements.

Four core capabilities of DSS are

1. **Representations**: It includes the presentation of the information in the form of graphs, charts, lists, reports, formatted reports, symbols, etc. These results are being used for control mechanism.
2. **Operations**: It includes logical & mathematical manipulation of data. These operations are confined to gathering information, generating statistics, preparing reports, assigning risk and values, generating alternatives using simulation etc.
3. **Memory aids**: It also provides updating of databases and memory, viewing of data, work spaces, libraries and linkages among libraries and work places.

4. **Control aids**: It provides the facility to user to control the activity of DSS. It includes a language permitting user control of operations, representations and memory. It also include features such as tutorials, help commands, functions keys, conventions etc.

Executive Information Systems (EIS)

It provides executives information in a readily accessible interactive format. It is a computer based system that accesses data concerning critical success factors of an organization and allows high level executives to display this information on demand. They are meant for top level executives in an organization. The characteristics of a good executive information system are as follows:

(1) Simple use interfaces are crucial. Good systems provide a wide variety of user interfaces such as a mouse, a touch screen, or a keyboard and allow the executive to choose which ever he or she is comfortable with.

(2) An EIS should be secure because the data that is contained and (or accessed by an EIS is obviously important and often proprietary information

(3) An EIS should support what-if-analysis and adhoc queries.

(4) An EIS should have the capability of allowing the executives to drill down into the data

(5) Very quick response time is necessary

(6) Colour graphics capabilities are important for displaying the information

(7) The data used in an executive information system may reside in many different locations efficient network is essential for expert systems.

The following points summarizes the Executive Information System:

It directly supports the value added work in the organization.

Its users are the people who do value added work which requires a special skills.

It can support communication or information sharing between people doing different parts of the task. It may help in explaining the result of the task to customers.

It provides tools, information, or structured methods for making decisions.

Examples of EIS are (I) system to generate competitive bids (ii) system to diagnose machine failures (iii) system to support loan approval process.

Its common features are (I) user friendly interface (ii) user friendly methods of analyzing data.

Artificial Intelligence and Expert Systems

Artificial Intelligence: The effort to develop computer based systems that can behave like humans, with the ability to learn languages, accomplish physical tasks, use a perceptual apparatus, and emulate human expertise and decision making. An example of such an effort is the diagnosis of a specific illness and prescription of a course of treatment by a physician. These are artificial intelligence programs called expert systems that will perform limited diagnosis of an illness with an accuracy rate greater than the physician. The primary areas of artificial intelligence research and applications today are robotics, computer vision, speech recognition, natural language processing, expert systems, and neutral networks.

Expert Systems: It is a knowledge intensive computer program that captures the expertise of a human in a limited domain of knowledge and experience. It helps in organization's value added work. The users of an expert system are the people who do value added work which requires a special skill or expertise. It provides tools, information, and structured methods for decision making. It stores and provides expert knowledge to support decisions in specific areas. Examples of expert system are:

1. System which generate competitive bids
2. System to help sales people and suggest the best choice for the customer.
3. System which helps in diagnose of failures may be machine or human being.
4. Systems to support a loan approval system.
5. Systems to support training in specialized areas where experts are in scarcity.
6. System to find price inconsistencies between different equity markets.

The components of an expert system include a knowledge base and software modules that perform inferences on the knowledge and communicate answer's to a users questions. The components of an expert system are shown in the following fig.2.3.

Limitations of Expert system:

- Expert systems are sometimes overrated.
- Expert systems can be expensive to develop and maintain.
- It is difficult to elicit the knowledge of experts
- It lacks common sense
- Expert system cannot learn.
- The validation of expert systems can be difficult.

ENTRUSTING MIS IN A CORPORATE ENTERPRISE

The MIS in a corporate enterprise is usually entrusted to an officer who is designated as Chief of Management Information Department and reports to chief executive of the concern. To suggest who should succeed in this position in the corporate enterprise requires a thorough analysis of present state of MIS. The MIS presently may be in anyone of the following form:

(a) It may be manual one.

(b) It may be computerized one.

(c) It may be a manual one but is heading for computerization.

Under a manual management information system in a corporate enterprise, the tasks of procuring, refining, analyzing, storing and retrieval of data /information are carried out by manual means. To carry out these functions a set of suitably designed form is used. Each form of this set is used for a specific function.

To specify who has to collect a specific information, the necessary form to be used the frequency of collecting the information and a manual known as MIS manual provides all such related matters guidelines. Such a system of information may be entrusted to a person who possesses the experience of working with several functional areas. Such a person may be either from finance or marketing department. This choice is suitable due to following reasons.

- The person entrusted with MIS knows quite clearly on the basis of his experience and interaction with other departments, the type of decisions made by different executives.
- He can also ascertain the information requirement of executives from his knowledge and experience gained, while working closely with different functional areas.
- He can also perceive the frequency and the changing needs of information requirement of executives.

– His familiarity with the behavior and ways of working of his colleagues also helps him in performing his task well.

In the case of computerized management information system the information is collected manually and is transferred to a computer system for analysis, storage and retrieval. Such type of information system may be entrusted to a computer and system expert, who is well conversant with management concepts and the working of business executives. This choice of entrusting MIS is supported by these reasons.

– The head of management information system possesses the requisite capabilities, which are necessary for developing various applications & guiding the smooth running of system.

– He can also foresee the changing information requirements of executives by analyzing the decisions made and the problems, which may be faced in future.

Lastly, the system, which involves the computerization of the present manual -system may be entrusted to a project leader. This project leader may not directly carryout the task of converting the system but may render all possible help to the outside consultants. The help of outside consultants may be sought till the project leader gains the necessary confidence to run it independently.

The main reasons for this choice are the following:

– Due to lack of project leaders in the area of computers, he may be assisted by outside consultants, till the development of the system is complete and he gains necessary confidence of handling the system independently.

– Since the project leader works closely with outside consultants, so he understands the system quite thoroughly than anyone else.

MIS in Indian Organizations

Although the significance of and need for MIS have been well realized in developed countries like U.S.A., it has not yet been so in countries like India. The rapid advancement of technology and the consequent advent of computers have mainly contributed for the success of MIS in those developed countries. In India, where computers were not heard earlier to 1950s, the big organizations, their financial capacities could not take a clue from their counterparts in those advanced countries and hence lagged behind. Even after three decades of computer advent in India and operations of MIS in certain big organizations, it still has remained a moot point whether it would serve any useful purpose and its installation justified.

It is, however, fallacious to seek any alibi for the present unsatisfactory and unfruitful results of MIS in the Indian organizations.

That the Indian organizations lag behind in the computer technology which is, no doubt essential for the development of MIS, does no longer hold water as an excuse for its inadequate application and operation after three decades of computer introduction.

The major hurdle is the reluctance on the part of industrialists to convince themselves of the usefulness of MIS. With their traditional thinking, they do not extend a wholehearted cooperation and unstinted support to the implementation of MIS, without which any effort in this direction would prove futile. As a result, where MIS has been introduced, it has received only a lukewarm support and has not passed the take off stage. Another important reason for the unsatisfactory functioning of MIS in many Indian organizations is the lack of proper training on the part of the personnel dealing with it. Ineffective handling of the system by these inexperienced people has been mainly responsible for the tardy development of MIS in India. Another constraint is that India being a poor country, many business organizations cannot afford to invest huge funds required for the installations of MIS.

Even though the various problems put forth above are responsible for the slow growth of MIS, they are not

altogether insurmountable. It should be realized that MIS, can be developed in a phased manner without facing any financial burden and the resultant benefits would be more than the expenses in operating the system by exposing them to different training programs designed for purpose. If MIS, is taken up with all the necessary sincerity and confidence, it would deliver the goods expected of it by the Indian organizations also. The efforts made for its development in these organizations would definitely bear fruits.

LESSON ROUND-UP

- MIS refers to the system which is made to provide updated, reliable and relevant information to management for its decision making.
- A well-defined MIS provides information to all levels of management for formulating strategies and policies, for reporting the organization performance to tax authorities, shareholders, regulatory authorities, preparing future plans for short and long term basis, exercising day-to-day control on various operations, allocating different type of resources to different functional areas.
- MIS is not a new concept. It is an age-old concept which is used to manage the various activities in the organizations. Before the emergence of electronic computing machine, it had been existed in its manual form. It has been used as a mean to develop structured decision making processes in the organizations at all levels for internal as well as external controls.
- MIS is a system that helps management in the process of decision making. The three elements of MIS are Management, Information and System.
- MIS not only cater the requirement of Top management but it serves the information requirement of middle level management and operational management too.
- MIS may or may not be computer based, computer is just a tool. Whether it should be used while installing a MIS depends largely on several factors, e.g., how critical is the response time required for getting information; how big is the organisation, and how complex are the needs of the information processing.
- More data in reports means more information for managers: s a misapprehension. It is not the quantity of data, but its relevance, which is important to managers in the process of decision-making.
- The conception that Accuracy in reporting is of vital importance is true only for operating level. For strategic level and middle level, Accuracy is a relevant but not an absolute ideal. Higher levels of accuracy involve higher cost. At higher decision levels, great accuracy may not be required.
- For developing MIS, there are three approaches used, Top down approach, bottom down approach and integrated approach. Under top down approach begins by defining the objectives of the organization, the kind of business it is in, and the constraints under which it operate. The crucial strategic and tactical decisions are also defined and the decisions necessary to operate the activities are specified. From the activities or functions and the decisions to be made, the major information requirements are ascertained. Bottom up approach starts from the identification of life stream systems. Life stream systems are those systems, which are essential for the day-to-day business activities. The development of information system, for each life stream system starts after identifying their basic transactions, information file requirements and information processing programs. After ascertaining the data/ information requirements, files requirements and processing programs for each life stream system, the information system for each is developed. The data is integrated only after thoroughly examining various applications, files and records. Integrated Approach If used objectively, it can overcome the limitations of the above two approaches. This approach permits managers at all levels to influence the design of the system. Top management will identify the structure and design of MIS suitable to the concerned department.

- Major constraints which come in the way of operating an information system are Non-availability of experts, Varied objectives of business concerns, Non-availability of cooperation from staff. Non-availability of heavy financial resources Turnover of experts
- A computer system that combines data, analytical tools, user-friendly software to support decision-making at the management level is called decision support system.
- DD is not a synonym of MIS. DSS provides integrated analytical tools, data, model base and a interface to the user in the form of a user friendly software while MIS provides a structured information to the end-users. DSS establish what tools are used to incorporate the decision making Process of a organization where as MIS identify information requirement at different levels in the organization.
- Artificial Intelligence is the effort to develop computer based systems that can behave like humans, with the ability to learn languages, accomplish physical tasks, use a perceptual apparatus, and emulate human expertise and decision making. An example of such an effort is the diagnosis of a specific illness and prescription of a course of treatment by a physician. These are artificial intelligence programs called expert systems that will perform limited diagnosis of an illness with an accuracy rate greater than the physician. The primary areas of artificial intelligence research and applications today are robotics, computer vision, speech recognition, natural language processing, expert systems, and neutral networks.
- Expert Systems: It is a knowledge intensive computer program that captures the expertise of a human in a limited domain of knowledge and experience. It stores and provide expert knowledge to support decisions in specific areas.

SELF-TEST QUESTIONS

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. What do you understand by the term MIS? Explain about its evolution?
2. What do you mean by Management information system? Is MIS and Computer system same? Explain why management information system is needed.
3. What are basic elements of Management Information System (MIS)? Explain their relative importance in a MIS system.
4. Explain about three tiers structure of Management Information System. Explain the difference between strategic decision making and operating decision making
5. Explain the difference among information requirement of strategic tactical and operational decision making.
6. What are the basic characteristics of management information system in an organisation? Explain
7. State some basic myths about Management information system and the truth behind the misconceptions.
8. What do you mean by Computerized MIS? Explain why computerized MIS is preferred over manual MIS?
9. Explain the difference between Top down approach and bottom up approaches of MIS development.
10. What are the prerequisites of an effective MIS? Explain in detail.
11. What do you mean by Decision support system (DSS)? Explain the difference between DSS and MIS.
12. What do you mean by Artificial Intelligence? Explain its characteristics.
13. What is an executive information system and what are its characteristics?

Lesson 9
Enterprise Resource Management

LESSON OUTLINE

- Enterprise Resource Management (ERM)
- ERP: Objective
- Genesis of ERP
- Different modules of ERP
- ERP: Basic Features
- Characteristics of ERP Solution
- Steps in ERP implementation
- Critical success factor for ERP implementation
- Benefits of ERP
- Limitation of ERP
- Criterion for choosing ERP System/ Vendor
- Popular ERP service

LEARNING OBJECTIVES

ERM (enterprise resource management) describes software that lets an enterprise manage user access to its network resources efficiently. ERM system is also widely known as Enterprise Resource Planning system, same terminology is used everywhere in this lesson. Since ERP is an integral part of most of the organization and in the capacity of a professional /employee one need to deal basic aspects of ERP so its study become very important for a management professional. After going through this lesson, the student will be able to:

- Understand the basic concepts of ERP its usefulness for an organization.
- Know the major issues involved in ERP implementation
- Understand the critical success factor for ERP implementation

Because we have an integrated ERP system that produces consistent data over the years, we can exploit the information to come up with cost reduction and strategy improvement ideas. Data makes it easier to justify these innovations.

Lalit Panda

ENTERPRISE RESOURCE MANAGEMENT

In the fast changing scenario the ability to respond to new customer needs and seize market opportunities as they arise is crucial. Successful companies today recognize that a high level of interaction and coordination along the supply chain will be key ingredient of their continuous success. Enterprises are continuously striving to improve themselves in the areas of quality, time to market customer satisfaction, performance and profitability. The successful organization will be those who can gather, and quickly act upon critical for the companies to execute this union, there is a need for an infrastructure that will provide information across all functions and locations within the organization.

ERM (enterprise resource management) describes software that lets an enterprise manage user access to its network resources efficiently. ERM describes software that manages all of a company's assets and resources, including such basic applications as general ledger, accounts payable and receivable, as well as manufacturing, inventory, and human resources. ERM system is also widely known as Enterprise Resource Planning system. In rest of the lesson, we will be using the word ERP for ERM.

ERP is a cross functional enterprise system driven by an integrated suite of software modules that supports the basic internal business processes of a company. ERP gives a company an integrated real time view of its core business processes, such as production, human resource, sales & distribution etc. ERP software consists of independent modules of integrated functional suites.

ENTERPRISE RESOURCE PLANNING: OBJECTIVES

1. Provide support for all variations of best business practices.
2. Enable implementation of these practices with a view towards enhancing productivity.
3. Empower the customer to modify the implemented business processes to suit the needs
4. Helps in transforming the enterprise functions to be agile, cost-effective and focused on supporting the business objectives.
5. Facilitate the organization making prompt and effective management decisions.

GENESIS OF ERP

ERP is a result of the modern organization attitude towards how their information systems are to be configured to the new business focuses. Merely automating system is no major bottleneck in getting to build software, desperate elements of an organization have to be linked together so that whenever a change in an external "pull' takes place the enterprise is able to adjust to it immediately and effectively. This proactive adaptability of an enterprise around redefined business objectives is called EWI or enterprise wide integration.

The genesis of ERP and its future can be traced in the following systems in an organization:

- Management Information Systems (MIS)
- Integrated Information Systems (IIS)
- Executive Information Systems (EIS)
- Corporate Information Systems (CIS)
- Enterprise Wide Systems (EWS)
- Material Resource Planning (MRP)
- Manufacturing Resource Planning (MRP II)

- Business Process Re-engineering (BPR)
- Enterprise Resource Planning (ERP)
- Intelligence Resource Planning (IRP)
- Money Resource Planning (MRP III)

MODULES OF ERP

The major modules of ERP on functional basis are given in table below. These modules include sales, production, material, finance, and personnel.

Business	Sales	Production	Materials	Finance	Personnel
Forecasting	Forecasting	Planning	Purchase	Accounting	Human Resource
Planning	Planning	Order Control	Inventory	Funds Mgt.	Payroll
Goals	Sales Budget	WIP	Stores	Balance Sheet Processing	Accounting
Objectives	Order Processing	Quality	Valuation	Schedules	Skill Attendance Inventory
Targets	Order Execution	Scheduling	Analysis	Analysis	Analysis
Strategy Control	Delivery Invoicing	Dispatch	Control	Control	Control
Fixed Assets	Maintenance	Quality Control	Cost	Management Accounting	Consolidation of Business operations

Modules of ERP

ERP BASIC FEATURES

Enterprise resource planning (ERP) features and functions help integrate management, staff, and equipment, combining all aspects of your business into one system in order to facilitate every element of the manufacturing process. Typical ERP system modules include features and functions for accounting, human resources (HR), manufacturing management, customer relationship management (CRM), and other business functions. ERP systems with manufacturing management functionality also include features and functions for inventory, purchasing, and quality and sales management. ERP software is often configured with specialized features and functions for a particular industry or type of manufacturing. For example you can compare ERP systems for discrete manufacturing, process manufacturing, engineer-to-order (ETO) manufacturing, distribution, fashion and apparel, mining, etc. To find the best ERP system for your business, it's important to understand which features and functions you need before you compare ERP solutions.

General Features of ERP

- Screen based flow control.
- Application Logic.
- Common service functions such as the currency, date, editing, and help.
- Diagnostic functions.
- Transaction flow control.

- Help functions.
- Central table system for management of parameters, texts and master data, online logical checks and validations.
- Word processing, text, text editing.
- Action massages.
- Enterprise Modeling: Structure/Policy/Rules/Guidelines.

Business System

- Business forecasting for products groups markets.
- Target fixing and allocation by the key parameters.
- Business planning in terms of the resources to execute.
- Strategy formulation and implementation.
- MIS for strategy monitoring and control.
- Business modeling for the strategy development and testing. DSS for resource planning.
- Information base management for management applications.

Sales

- Basic data (master) management.
- Order processing
- Dispatching and invoicing
- Order analysis, forecasting
- Sales analysis, budgets and controls
- Finished goods stores management
- Dealer, distributor management system
- Receivable analysis
- Market/Customer/Product analysis
- Market research information database
- Marketing personnel management
- Sales forecasting and budgeting.

Production

- Basic master data management.
- Bill of materials, classification.
- Process sheet, routing.
- Work order generation, scheduling and control.
- Production Planning: BOM, MRP, MPS and capacity planning.
- Interface of CAD/CAM/CAE systems.

- Quality systems for data capture, analysis, and control.
- WIP tracking, valuation.
- Work station/machine centre management.
- Production-Materials interface.
- Collection of unit data for valuation and costing.

Materials

- Purchasing and procurement.
- Goods receipt and issue system.
- Stock management and valuation.
- Inventory analysis.
- Stores ledger, valuation, analysis, disposal.
- Excise/customs interface.
- Data integration with production, and accounts systems.
- Quotation/Inquiry processing.
- Subcontracting, material accounting and bill passing.

Finance

- General accounting functions.
- Ledger, payables and receivables.
- Subsidiary ledgers.
- Cash-flow management.
- Loan management, funds management.
- Working capital management
- Budgeting, planning and control.
- Balance sheet processing.
- Tax management, status reporting.
- Assets accounting.
- Cost accounting: Cost centers accounting, product costing.
- Cost analysis for business decisions.
- Bank reconciliation.
- Letter of credit management.
- Consolidation of accounts.

Personnel

- Personnel data management.

- Personnel attendance system, time management.
- Payroll accounting: salary, wages, incentives, bonus, income tax and other deductions, and contributions to various public and provident funds.
- Human resources management: Planning, recruitment, training and up-gradation.
- Personnel cost, projection and planning.

Fixed Assets

- Fixed assets accounting: Inventory, register.
- Depreciation accounting.
- Capital work in Progress.
- Fixed assets retirement and disposal.
- Year and processing for balance sheet schedules.

Maintenance

- Plant maintenance planning
- Breakdown, preventive, conditional maintenance.
- Maintenance management: Initiation, planning, execution, control, and cost accounting.
- Monitoring performances for maintenance action as all kinds of productive assets.
- Contract management.

Quality Control

- System of data gathering to assess quality and measure against standard.
- Analysis of quality by process, material, work centre location.
- Analysis of quality by reason and actions taken.
- Building quality assurance data for equipment/process/technology selection.
- Monitoring quality across the organization from input to output for operating decisions and business decisions.

Consolidation of Business Operations

- Accounting by units and divisions with local focus.
- Consolidation by accounts in corporate functions.
- Bringing out comprehensive report system for business decisions.

CHARACTERISTICS OF ERP SOLUTION

- Modular structure
- Scalable architecture.
- Seamless integration of modules.
- RDBMS independent.
- Independence of hardware platform.

- Interface capabilities.
- PC download/upload facility.

Most of the ERP solutions need some changes to suit the environment. The commerce and Corporate Laws differ from country to country and the ERP in such cases need customization to satisfy the local requirements of the business.

The ERP solution has an advantage of fast implementation as the design and development is eliminated being a package. Due to object oriented technology and the client server architecture, the changes are easy to make, which are less at the server and more at the client's end.

Since, it has modular structure; one can implement the solution in a phased manner module by module. It can be implemented first on a smaller scale and expanded subsequently with more users, more locations and more modules as well. Since, the whole solution is a package product, the manufacturer of the package brings out newer versions of the product offering more facilities to the user to improve the utility of the solution.

There are more than a dozen ERP solutions available in the market each having its own speciality. Though, they are characterized as described earlier, they differ in feel, look, presentation, processing efficiency and user-friendliness.

Some of these products are developed as an application in a particular organization and then turned into a packaged solution. In view of this, some of the ERP solutions are more useful and efficient in similar organizations. The specific industry features have been taken care of more efficiently as customized solutions. Since, the designer/developer has choice of RDBMS, front-end tools, the interface tools, and so on the package efficiency changes with the choice of tools. Some of these packages run better, if installed on a particular hardware platform; and used by a particular organization.

Though tools, technology and approach may be same or similar, the manner in which they are used decides the efficiency of the solutions.

STEPS IN ERP IMPLEMENTATION

The steps involved in the implementation of an ERP Solution are listed in the following:

- Identification of the needs for implementing an ERP package.
- Evaluating the "as-is" situation of your business.
- Deciding upon the desired would be situation for your business.
- Reengineering of the business processes to achieve the desired results.
- Evaluation of the various ERP software
- Finalizing of the ERP package.
- Installing the requisite hardware and networks.
- Develop customers the software.
- Finalizing the implementation consultants.
- Implementation of the ERP software.

CRITICAL SUCCESS FACTORS FOR ERP IMPLEMENTATION

A lot has been said about the competitive advantage provided by ERP. An organization decides to take the plunge into the ERP route. The consultants will be hired to bring the "best practices" in the industry. It requires both the knowledge; functional knowledge as well as the software programming skills. The following factors are critical in ERP success.

First and foremost is the top management commitment: The large investments needed to implement ERP ensure that the decisions are invariably taken at the top management level. It is fortunate, but not sufficient. This ensures top management involvement, but it is not tantamount to top management commitment. Here is an example; to be successful, the ERP team must consist of your "best" people, not those that "can be spared" during the project team. Unless top management takes a conscious decision to take out the "best" people for an extended period of time (several months) at the cost of "losing the best people" during implementation, ERP has little chance of success.

The management commitment involves the management of change. ERP is likely to turn the organization "upside down" unleashing lots of energy from vested interests. Unless top management is involved directly, it is impossible for any line manager to face the oppression to such changes.

Another real test of top management commitment is the resistance to over-customization, particularly in the Indian context. One reason why many computerization efforts in Indian organizations have not been particularly successful is not having "systems in place". ERP implementation is a golden opportunity to put such "systems in place". Thanks to excellent IT skills available in many Indian organizations, there is a strong tendency to "do it your way" leading to large-scale customization. We in the Indian corporate scene recognize that there is no point doing such standard processes and practices in any distinctively different "our" way. It is better to follow the "standard" way and concentrate on "innovative" ways of doing better business.

BENEFITS OF ERP

Enterprise Resource Planning (ERP) involves the organization of computing systems, business processes and procedures under one umbrella designed to improve business efficiency. Originally designed for manufacturing organizations, ERP is now available for a wide range of industries, including financial services companies and companies focused on customer service. In the past, ERP systems were designed for very large organizations. However, many suppliers now offer products for small and medium-sized businesses. ERP systems are being implemented by most of the organisation for innumerable benefits. Some of them are as given:

1. Integrated Information

The key benefit of implementing ERP is integration. ERP helps in reducing operational costs by coordinating various departments of the organization. The major idea behind ERP is to control accuracy as well as redundancy of data and data entry. This centralized working system is able to replace multiple, disconnected databases with a single system, incorporate different applications and data sources. It also aims to lowers help desk support and marketing cost. In addition, this real time application has the capabilities of interfacing internal and external entities. Moreover, ERP is an ideal application to improve the cooperation between departments and employees as well as communication with prospects and customers.

2. Standardization of processes

A manufacturing company that has grown through acquisitions is likely to find that different units use different methods to build the same product. Standardizing processes and using an integrated computer system can save time, increase productivity, and reduce head count. It may also enable collaborating and scheduling production across different units and sites.

3. Standardization of human resource information

This is especially useful in a multi-site company. A unified method for tracking employee time and communicating benefits is extremely beneficial, because it promotes a sense of fairness among the workforce as well as streamlines the company as a whole.

4. Effective Management of Repeatable Processes

One of the fundamental objectives of ERP systems are repeatable processes. By creating repeatable processes,

management is able to ensure that tasks are done using organization-wide best practices. Employees are able to improve quality by performing tasks the same way each time.

Repeatable processes also reduce the risk of a key employee leaving with his or her knowledge of how a job is done. These types of processes are also easier to change. Because a large number of people are performing the same set of tasks, finding improvements can be easier. Rolling out those changes organization-wide can also be easier.

5. Lower Training Costs

Standardizing these processes also results in lower training costs. Because the processes are the same throughout an organization, training programs that are standardized, reduce overall development costs. By standardizing processes, training can be patterned and optimized to reduce the time spent in training. Reduced time spent in training means less non-productive time.

6. Reduced Inventory Costs

Many ERP systems, especially systems designed for manufacturing industries, are customizable for lean manufacturing or other parts-control management systems. By linking repeatable processes with inventory usage, a manufacturer can maintain lower parts inventories.

This is possible because of the integration between processes and ordering. Each time a procedure is executed; inventory levels can be updated in real time. Once a pre-defined level of parts inventory is reached, replacements can be automatically ordered from the supplier.

7. Improved Business Visibility

Depending on how a system is implemented, one objective of an ERP system might focus on business performance and operations visibility. By creating reports based on actual manufacturing tasks, the overall performance of the organization can be more easily analyzed and optimized.

Things that might require tracking include time it takes to complete tasks, production levels, and production units per units of time and almost any measurable that could help an organization analyze performance.

8. Increased Profits

By optimizing production through process visibility, the cost per production unit can be reduced. Reducing training costs can, again, add to the bottom line. By reducing inventory levels, less money is tied up in non-liquid business resources which increase available cash to allow a company to make faster business decisions.

9. Enhanced and Efficient Technology

This software enhances day to day management activities. It also supports strategic planning that defines objectives for the business. Since it has better data accessibility, top management can also use this tool to make better and more effective decisions. In addition, ERP system has a capability of eliminating manual activities and streamlining critical business processes for many departments of an organization. The following are some more benefits that improve the efficiency of an ERP system:

10. Easy Reporting

An ERP system improves and customizes reporting. It provides easy technique of generating reports. With better access to data you can generate and manipulate reports anytime you want to.

11. User Friendliness

This robust and user-friendly application easily eliminates problems without over-grown data tables. Moreover, non-technical people can easily access data or information using ERP applications. This handy application also allows you to deal with high volumes because of its real time capability and future based orientation.

12. Easy Data Accessibility

An ERP system enables you to access real time data and increase self-service of critical information. Many ERP vendors are providing mobile functionalities so that you can always remain connected and well-informed in regards your business processes and performance.

13. Increased Security

ERP system not only improves data integrity and security but also enhances the data restrictions, allowing you to keep your customer information and company data safe and secure.

14. Providing Business and Financial Solution

ERP offers the best business and financial solutions for almost every type of organization. By permitting flow of resources and finances into different and vital business activities it enables enterprises to increased efficiencies in its daily operations.

15. Accuracy & Consistency

An ERP enables companies to maintain consistent and accurate data throughout all the departments enabling the complete flow of information to be viewed through a single system. The department heads can see the timing of employees and total work completed. It provides better visibility and helps in improving the performance of the organization.

16. Better Resource Management

This centralized application provides the tools and reporting capabilities to allow management to better allocate valuable resources. This allows decision makers to monitor and take action during crucial times and prevent delays.

For any productive business organization ERP can play a vital role. A successfully implemented centralized ERP system will help in improving alignment of strategies and operations, productivity and insight, financial management and corporate governance. ERP system also enables in reducing costs through increased flexibility and overall risk. Before implementing ERP system be assured in terms of where and how the organisation will benefit, discussion with the potential suppliers of ERP in this regards plays a vital role.

LIMITATIONS OF ERP

Each good system is having some limitations and for these limitations, sometime people become reluctant to implement good system. ERP is also not different and it has also got some limitations. The limitations which are associated with an ERP system are discussed herein:

1. Difficult to implement in running businesses

Implementing an ERP system in a new business can be very effective. Implementing the same system in an older business can be very difficult. All employees must be trained, and there will be significant down time as the business switches all applications over to the new system. Some businesses cannot afford the profit loss this downtime would require. ERP systems also tend to have industry standards for specific types of businesses, and the strict moulds may lower creativity or competitive advantage.

2. Customization is problematic

Every business has its own requirement and there is no ERP which may be suited for all business's requirement so to implement an ERP system in an organisation, first the detailed study about the different processes of a business is done and then various customizations is done to make the ERP suitable for a particular organisation requirement. The customization process involves lot of money and resources which works as a limitation to the implementation of an ERP system in an organisation.

3. Policy Limitations

ERP systems do not fit the business plans of every enterprise. Often, ERP systems must be customized to allow for specific tasks. Not all ERP systems allow this—depending on the system or company the business uses, it may be against policy to make such drastic changes to the application.

4. Ongoing Support

Support for ERP systems often can be difficult to depend on. Technical response can be adept at dealing with minor problems, but major complications with the ERP systems can be beyond the limited customer service available to businesses.

5. Lack of user participation in ERP implementation

The participation of users is very important for successful implementation of ERP projects – So, exhaustive user training and simple user interface might be critical. Moreover involvement of key users at the pre implementation stage and implementation stage is very important and lack of their involvement acts as a limitation for ERP system.

6. Problem of Harmonization of ERP processes with the business processes

Harmonization of ERP systems can be a mammoth task (especially for big companies) and requires a lot of time, planning, and money.

7. Resistance to change

Implementing ERP system in an organisation requires lot of process changes, starting new process etc. In this process, certain people's profile gets redundant and they need to transfer to other processes. Moreover implementing ERP requires people to new the new processes and technologies. All this become a reason of resistance by people which works as a big limitation for ERP implementation.

8. High Annual Charges

Most of the ERP vendors charge large sum of money for annual license renewal that is unrelated to the size of the company using the ERP or its profitability. This acts as a big limitation for an ERP implementation.

9. Cutting Expenses on Training

Success depends on the skill and experience of the workforce, including training about how to make the system work correctly. Many companies cut costs by cutting training budgets. Privately owned small enterprises are often undercapitalized, meaning their ERP system is often operated by personnel with inadequate education in ERP in general. This acts as a big limitation.

10. Dependency on one Vendor/High switching cost

Once an ERP system is implemented it becomes a single vendor lock-in for further upgrades, customizations etc. Moreover once a system is established, switching costs are very high for any one of the partners (reducing flexibility and strategic control at the corporate level).

CRITERION FOR CHOOSING THE ERP SYSTEM/ERP VENDOR

The right Enterprise Resource Planning system can integrate key business functions, boosting the bottom line. The wrong ERP application can drain your IT budget. The difference between the two can be as simple as knowing which questions to ask as you research the options**.** The following five criteria should top your list when evaluating ERP vendors.

1. Functional Specifications. Does the application accommodate your business needs?

Functional compatibility depends on a complex analysis of your company's unique business needs and the ERP industry's varied solutions.

2. Define and prioritize company processes. Identify core corporate functions, and develop a comprehensive picture based on input from all stakeholders.

3. Identify "showstoppers." A showstopper is the "missing feature or unsupported business process that transforms an otherwise great fit into a complete mismatch." Often these glitches lurk beneath the radar, surfacing upon implementation. The software that can count widgets but can't track corn syrup; the application that won't assign dual currency prices to export items—depending on the enterprise, even the most advanced ERP solution can become a nightmare.

You can avoid functional incompatibility by determining that the ERP system is designed for:

- Discrete or process manufacturing
- Work orders or repetitive manufacturing
- Distributor or manufacturer process management
- Multi-plant or a warehouse environment
- Multilanguage and/or multicurrency needs

4. Evaluate your options: Not all ERPs are created equal. A clue to a product's relative strengths is its origin. Some ERP vendors began by developing manufacturing software; others entered the field via a robust human resources package, or a data warehouse solution. The Oracle Accelerate program leverages the company's broad spectrum of world-class business applications to deliver a comprehensive, modular ERP package.

5. Business Model: Does the application mesh with your corporate culture?

Functional compatibility is absolutely crucial—but it's also important to consider structural fit. "You have to examine more subtle issues such as your company's corporate culture and management style," advises business technology expert Derek Slater. An ERP package may look great on paper, but will it mesh with your model of doing business? Consider not only what your company needs to accomplish, but also how it will do so.

For example, hands-on managers may want to drill down to the details; a big-picture executive will be better served by sleeker financials. Oracle's ERP application excels in aggregating data into expansive transaction reports. Other applications favor a more granular approach.

6. Flexibility: Can the application be modified? Will it scale to accommodate evolving needs? Enterprise Resource Planning is a long-range investment. A flexible system will grow with your company, accommodating new specifications as they emerge. Flexibility is also crucial in the implementation phase, to ensure that the program can align with existing business needs and achieve integration. Look for an ERP solution that will accommodate new operating protocols, future business growth, market expansion, and any other initiatives that might arise.

To evaluate ERP flexibility, consider:

- System parameters and default settings
- Custom screen and menu options
- Tools for modifying standard forms
- Data access options and custom reporting
- Modular format

7. Time to Implement: Will the rollout be quick, effective, and painless?

Implementation can be a daunting prospect when company-wide integration is at stake. Check your ERP provider's

implementation track record and methodology. An efficient rollout minimizes the costs and disruption associated with conversion. A speedy, vendor-supported implementation process also promotes user buy-in and a faster time to ROI.

8. Industry Expertise: Does the vendor have a proven track record in your industry?

The ERP solution you choose should come with a pedigree of successful installations in your field. “There are very few companies that don’t have specialized processes dictated by their industry,” says consultant David Dobrin. A proven track record means that the vendor is already well attuned to the particular business requirements of this market sector. “For manufacturers,” for example, “the right system is one that, from its beginning, has been based on a strong process engineering foundation.” Some ERP integration specialists even recommend an on-site visit to an ERP customer in the same industry, if possible. Many ERP providers offer applications customized to a particular industry. The Oracle Accelerate program includes applications for 32 industries, ranging from aerospace to defense to wholesale distribution.

The formula for finding the perfect ERP match is fairly straightforward, provided the team performs the due diligence research. Functional and structural compatibility, flexibility, solid vendor support, and a proven track record add up to an ERP solution that works.

POPULAR ERP SERVICE PROVIDERS

SAP is the world’s largest business software company and the third-largest software supplier overall. Founded in 1972 as Systems Applications and Products in Data Processing, SAP has a rich history of innovation and growth that has made it a recognized leader in providing collaborative business solutions for all types of industries in every major market.

With a mission statement that emphasizes experience, knowledge, and technology for maximizing business, SAP leverages its extensive experience to deliver a comprehensive range of solutions to empower every aspect of business operations for organizations of any size.

Deploying high-quality technology, services, and development resources, SAP delivers a business platform that unlocks valuable information resources, improves supply chain efficiencies, and builds strong customer relationships. The company, headquartered in Walldorf, Germany, employs more than 46,100 people in more than 50 countries, and it serves more than 43,400 customers worldwide.

SAP ERP Key Strengths

1. SAP ERP addresses the core business software requirements of the most demanding mid-size and large organizations – in all industries and sectors.
2. SAP ERP draws from more than 30 years of experience with more than 40,000 customer implementations to deliver powerful functionality, global orientation, and flexible enhancement options.
3. SAP is committed to delivering innovation to its customers through its SAP ERP application. With SAP enhancement packages, organizations can replace the traditional technique of improving and augmenting core processes supported by SAP ERP. Instead of waiting for functionality that is packaged with a new release, they can implement innovation from SAP without having to run a major upgrade project With SAP ERP, customers ensure that their employees can readily access the critical data, applications, and

analytical tools they need to perform all their job functions efficiently and effectively, while also supporting a shared-services organizational model for human resources, finances, and other key processes.

4. SAP supports more than 43,400 customers worldwide, with 105,000 installations in 120 countries. SAP's unique ecosystem consists of 11,000 consulting and education employees, plus 6,000 service and support staff.
5. SAP has a large support organization with 185,000 certified partner employees, 77 trainings centers, six global support centers, nine custom development centers, and genuine 24/7 support, SAP is able to maximize an organization's business and IT success.

ORACLE

Main Highlights of Oracle

Backed by the strength of one of the largest software application companies in the world; committed to technology innovation/integration. Oracle's ERP solution suite helps customers achieve 30-80% lower total cost of ownership, benefit from a predictable cost model, and reduce risk Partner expertise: Oracle solutions leverage third party solutions and add on applications from 19,000 partner companies

After thirty years of providing leading-edge solutions, Oracle remains a major player for database technology and applications in enterprises throughout the world. The company is the world's leading supplier of software for information management, and the world's second largest independent software company. Oracle technology can be found in nearly every industry, and in the data centers of 98 of the Fortune 100 companies. Oracle is the first software company to develop and deploy 100 percent internet-enabled enterprise software across its entire product line: database, business applications, and application development and decision support tools.

Oracle was one of the first companies to make its business applications available through the internet—an idea that is now pervasive. With the release of Oracle Fusion Middleware, Oracle has begun debuting new products and functionality that reflect the company's goal to connect all levels of enterprise technology to help customers access the knowledge they need to respond to market conditions with speed and agility. Today, Oracle Real Application Clusters, Oracle E-Business Suite, Oracle Grid Computing, support for enterprise Linux, and Oracle Fusion all fuel a commitment to innovation and results that has defined Oracle for thirty years.

Oracle applications are now running in over 1,500 public sector organizations, 10 of the world's top 10 banks, 20 of the world's top 20 telecom companies, and 10 of the top 10 academic universities worldwide.

Oracle ERP Key Strengths

1. Oracle's ERP solution suite helps customers achieve 30% - 80% lower total cost of ownership, benefit from a predictable cost model, and reduce risk.
2. With Oracle's powerful, on-demand software technology, over 3.6million end users are able to increase their productivity and gain competitive advantage, resulting in a superior ownership experience.
3. Oracle Enterprise Manager is the only management software that provides complete management solution for business applications, using a unique top-down approach. It provides strong monitoring and management that encompasses end-user experience, application flows, and the underlying software and system infrastructure.
4. Oracle offers proven and open solutions—and a network of partner expertise. The company's solutions are built on open standards and leverage third-party solutions and add-on applications. Oracle's 19,000-strong partner network delivers deep, industry-specific functionality and best practices.

Highlights

Backed by the strength of Microsoft, one of the largest IT companies in the world, it uses very familiar Microsoft interface. Headquarters at Redmond, the company was founded in 1975, New Mexico, USA. It offers complete business management software: ERP, e-commerce, supply chain, manufacturing, CRM, HR, project accounting etc.

The following ERP Solutions are offered by the company:

1. Microsoft Dynamics GP (formerly Microsoft Great Plains)
2. Microsoft Dynamics NAV
3. Microsoft Dynamics AX

Customer Focus

Microsoft distributes its products primarily through the following channels: OEM; distributors and resellers, and online services. Its customers include individual consumers, small and medium-size organizations, enterprises, governmental institutions, educational institutions, internet service providers, application developers, and OEMs.

The company's ERP solution suite, Microsoft Dynamics, offers integrated, adaptable business applications for small and medium-sized organizations and divisions of large enterprises. These integrated solutions—delivered through a worldwide network of experienced Microsoft Certified Partners—work like and with familiar Microsoft software and help automate and improve financial, customer relationship, and supply chain management.

Highlights

Infor is the 10th largest software company in the world, with approximately $2.1 billion in revenue. Over the past six years, Infor has grown to become one of leading business software companies in the world by building and acquiring some of the best solutions in the world. A company unparalleled in application breadth, market experience, open technology and global reach, Infor has 8,000+ employees, direct offices and implementation and support capabilities in 100 countries, and over 70,000 customers worldwide.

The thought leaders at Infor understand that their customers want to reduce the number of vendors they work with and Infor strives to continue as their trusted "vendor of choice." Infor has a consistent 95% customer retention rate — one of the highest in the industry — and 72% of its license revenues are generated by its current customers. Additionally, over 1,000 new customers chose Infor last year for its unparalleled application breadth, open technology, and global reach. The company is committed to continuing its growth by broadening its best-in-class focus, and by providing the most innovative solutions and services globally.

Offers a variety of ERP solutions that help companies in a wide spectrum of subsectors automate, plan, collaborate, and execute based on their unique business requirements. It is world's tenth largest software company. Over 70,000 customers worldwide with 95% customer retention rate, the company serves mid-market manufacturers. Headquartered at Alpharetta, Georgia, it was founded in 2002.

ERP Solutions it offers includes:

Infor ERP Baan/LN

Infor ERP SyteLine

Infor ERP VISUAL

Infor ERP BPCS/LX

Infor ERP Adage

Customer Focus:

Infor's customer base comprises mid-market discrete manufacturing enterprises in industrial equipment, high-tech electronics, automotive, metal and plastic fabrication, and aerospace sectors, and mid-market process manufacturers in consumer goods, chemical, and food and beverage markets.

LESSON ROUND-UP

- ERM (enterprise resource management) describes software that lets an enterprise manage user access to its network resources efficiently. ERM (enterprise resource management) also describes software that manages all of a company's assets and resources, including such basic applications as general ledger, accounts payable and receivable, as well as manufacturing, inventory, and human resources.
- ERM system is also widely known as Enterprise Resource Planning system.
- ERP system is implemented in organisation for providing support for all variations of best business practices, enabling implementation of these practices for enhancing productivity, helping in transforming the enterprise functions to be agile, cost-effective and focused on supporting the business objectives and to facilitate the organisation making prompt and effective management decisions.
- The basic modules of an ERP system includes, supply chain, finance, material, finance, human resource. Each module of an ERP system has got some module. For example finance module contain finance, treasury. Cost, account receivable, accounts payable and fixed assets accounting module.
- Various characteristics of an ERP system include Modular structure, Scalable architecture. Seamless integration of modules, RDBMS independent, Independence of hardware platform, Interface capabilities, PC download/upload facility.
- The steps involved in the implementation of an ERP Solution include Identification of the needs for implementing an ERP package, deciding the desired results, Reengineering of the business processes to achieve the desired results. Selecting of ERP package, Installing the requisite hardware and networks, finalizing the implementation consultants. Implementation of the ERP software.
- Critical success factor for implementing ERP includes top management commitment, the management of change and the resistance to over-customization.
- For any productive business organization ERP can play a vital role. A successfully implemented centralized ERP system will help in improving alignment of strategies and operations, productivity and insight, financial management and corporate governance. ERP system also enables in reducing costs through increased flexibility and overall risk. Before implementing ERP system be assured in terms of where and how the organisation will benefit, discussion with the potential suppliers of ERP in this regards plays a vital role.
- Implementing an ERP system in a new business can be very effective. Implementing the same system

in an older business can be very difficult. All employees must be trained, and there will be significant down time as the business switches all applications over to the new system. Some businesses cannot afford the profit loss this downtime would require. ERP systems also tend to have industry standards for specific types of businesses, and the strict molds may lower creativity or competitive advantage.

– Major ERP players in the market are SAP, BAAN.ORACLE, and Microsoft Dynamics. In all of these SAP and Microsoft dynamics captures a bigger market share while others are having significant share.

SELF-TEST QUESTIONS

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. What do you mean by the term “ERM’? Explain the basic objectives of implementing ERM.
2. What are the critical success factors for implementing ERP in an organisation? Explain in details.
3. What do you mean by the term ERP? Explain its features, its advantages and limitations?
4. AB and Limited want to implement SAP in the organisation while it has been using another ERP presently. What are the consideration which AB limited needs to keep in consideration while switchover to SAP?
5. Who are the major players in ERP implementation? Explain two of them in detail.
6. While selecting an ERP system, what are the criterions which need to be kept into consideration?

Lesson 10
E-Governance in India

LESSON OUTLINE

- Meaning of governance
- Meaning of governance
- History of E Governance in India
- Models of e governance
- Benefits of E Governance
- E Governance evolution in India-Challenges
- E governance action plan
- Requirements for implementing successful E governance
- National E-governance division
- National e governance plan
- E governance infrastructure
- State wide area network (SWAN)
- National service delivery gateway (NSDG)
- Common Service centre

LEARNING OBJECTIVES

E-Governance is the use of information and communication technologies to support good governance.E-governance is the natural progression from computerization of Government departments with the developments in information and communication technology and increasing access of internet based services and platforms to common people.

E governance has revolutionized the entire government machinery and it has helped in removing various disadvantages of government regulatory system. It is the result of e governance revolution that we are able to perform functions like book railway/bus ticket online, file our tax return instantaneously and get access of company's master data instantaneously. The benefits of e governance are many more and list is very long.

After reading this lesson, one would be able to

- Understand the meaning of E Governance
- Learn about Various models of e-governance
- Know about national e-governance division and national e- governance plan
- Learn about E governance infrastructure, SWAN and NSDG

E-Governance in India has steadily evolved from computerization of Government Departments to initiatives that encapsulate the finer points of Governance, such as citizen centricity, service orientation and transparency. The National e-Governance Plan (NeGP), takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision and a shared cause. In this section we are highlighting the initiatives of the Central and State governments to bring public services closer to the citizens.

MEANING OF E-GOVERNANCE

E-Governance or 'electronic governance' is basically the application of Information and communications Technology to the processes of Government functioning in order to bring about 'Simple, Moral, Accountable, Responsive and Transparent' (SMART) governance. This would generally involve the use of IcTs by government agencies for any or all of the following reasons: (a) Exchange of information with citizens, businesses or other government departments (b) Speedier and more efficient delivery of public services (c) Improving internal efficiency (d) Reducing costs / increasing revenue (e) Re-structuring of administrative processes and (f) Improving quality of services.

Although the term 'e-Governance' has gained currency in recent years, there is no standard definition of this term. Different governments and organizations define this term to suit their own aims and objectives.

Gartner Group defines e-governance as: "the continuous optimization of service delivery, constituency participation, and governance by transforming internal and external relationships through technology, the Internet and new media."

The UNESCO definition (www.unesco.org) is: "E-governance is the public sector's use of information and communication technologies with the aim of improving information and service delivery, encouraging citizen participation in the decision-making process and making government more accountable, transparent and effective. E-governance involves new styles of leadership, new ways of debating and deciding policy and investment, new ways of accessing education, new ways of listening to citizens and new ways of organizing and delivering information and services. …….. Its objective is to engage, enable and empower the citizen."

According to Keohane and Nye (2000), "Governance implies the processes and institutions, both formal and informal, that guide and restrain the collective activities of a group. Government is the subset that acts with authority and creates formal obligations. Governance need not necessarily be conducted exclusively by governments. Private firms, associations of firms, nongovernmental organizations (NGOs), and associations of NGOs all engage in it, often in association with governmental bodies, to create governance; sometimes without governmental authority." Clearly, this definition suggests that e-governance need not be limited to the public sector. It implies managing and administering policies and procedures in the private sector as well.

Basically, e-Governance is generally understood as the use of Information and communications Technology (IcT) at all levels of the Government in order to provide services to the citizens, interaction with business enterprises and communication and exchange of information between different agencies of the Government in a speedy, convenient efficient and transparent manner.

Dr. APJ Abdul Kalam, former President of India, has visualized e-Governance in the Indian context to mean:

> "A transparent smart e-Governance with seamless access, secure and authentic flow of information crossing the interdepartmental barrier and providing a fair and unbiased service to the citizen."

E-GOVERNANCE EVOLUTION: HISTORY AND PRESENT STATUS

Global shifts towards increased deployment of IT by governments emerged in the nineties, with the advent of the World Wide Web. The technology as well as e-governance initiatives have come a long way since then. With the increase in Internet and mobile connections, the citizens are learning to exploit these new modes of access in wide ranging ways. They have started expecting more and more information and services on-line form governments and corporate organizations to further their civic, professional and personal lives, thus creating abundant evidences that the 'new 'e-citizenship' is taking hold.

The concept of e-Governance has its origins in India during the seventies with a focus on development of in-house government applications in the areas of defense, economic monitoring, planning and the deployment of IT to manage data intensive functions related to elections, census, tax administration etc. The efforts of the

National Informatics Center (NIC) to connect all the district headquarters during the eighties was a very significant development.

From the early nineties, IT technologies were supplemented by ICT technologies to extend its use for wider applications with policy emphasis on reaching out to the rural areas and taking in greater inputs from NGO's and private sector as well. There has been increasing involvement of international agencies under the framework of e-governance for development to catalyze the development of e-governance laws and technologies in developing countries.

The technology as well as e-governance initiatives have come a long way since seventies. For governments, the more overt motivation to shift from manual processes to IT-enabled processes may be increased efficiency in administration and service delivery, but this shift can be conceived as a worthwhile investment with potential for returns.

Interactions in E-Governance

The advent of new information and communication technologies has made electronic governance as a tool to enhance the following relationship:

- Government to Government
- Government to Citizen
- Citizen to Government
- Government to Private and other Sectors.
- Private and NGOs Sector to Government.

E-governance is beyond the scope of e-government. While e-government is defined as a mere delivery of government services and information to the public using electronic means, e-governance is not just about government web site and e-mail. It is not just about service delivery over the Internet. It is not just about digital access to government information or electronic payments. E-governance will allow citizens to communicate with government, participate in the government's policy-making and to communicate with each other. The e-governance will truly allows citizens to participate in the government decision-making process, reflect their true needs and welfare by utilizing e-government as a tool.

MODELS OF E-GOVERNANCE

There are five models of E-Governance. These models are briefed in the following:

1. Broadcasting/Wider-Dissemination Model

The model is based on dissemination of governmental information already available in the public domain into the wider public domain through the use of ICT and convergent media.

This model could be applied in the following possible ways:

- Putting Government Laws and Legislations online
- Making available the names, contact addresses, e-mails, fax numbers of local/national/regional/international government officials online.
- Make available information pertaining to Government Plans, Budgets, Expenditures, and Performances online.
- Put key judicial decisions which are of value to general citizens and create precedence for future actions online

2. Critical Value Information – Flow Model

This model is based on the principle of dissemination/channelising of information of critical value to targeted audience or in wider public domain through the use of ICT and convergent media. This model requires a foresight and understanding of the "use value" of particular information set and locating users to whom the availability of particular information set would make a critical difference.

This model could be applied in the following possible ways:

- Making available the corruption related data about particular Ministry/Division/Officials online to its electoral constituency or to the concerned governing body.
- Making available Research studies, Enquiry reports, Impact studies commission by the Government online to the affected parties.
- Making available Human Rights Violations of the Government or allied authorities online for access by Judiciary, NGOs and concerned citizens.
- Making available Critical Environmental Information available to local inhabitants such as radioactivity spills, effluents discharge information on ratings of the company etc.

3. Comparative Analysis Model

Comparative Knowledge Model is one of the least-used but a highly influential model. The model, if used innovatively, can harness the potential and capacity offered by the communication technologies and aims it towards better governance.

This model could be applied in the following possible ways:

- To learn from historic policies and actions and derive learning lessons for future policy-making.
- To evaluate the effectiveness of the current policies and identify key learning in terms of strengths and shortcomings in policies.
- To effectively establish conditions of precedence, especially in the case of Judicial or legal decision-making (example for resolving patent-related disputes, public goods ownership rights), and use it to influence/advocate future decision-making.
- To enable informed decision-making at all levels by enhancing the background knowledge and providing a rationale for future course of action.
- To evaluate the performance and track-record of a particular decision-maker/decision-body.

4. Interactive-Service Model

Interactive-Service model is a consolidated model of the earlier models and opens up avenues for direct participation of individuals in the governance processes. Fundamentally, ICT have the potential to bring in every individual in a digital network and enable two-way/interactive flow of information amongst them. The potential of ICT for the governance is fully leveraged in this model and leads to greater participation, efficiency and transparency in functioning of the government as well as savings in time and costs relating to decision-making.

This model could be applied in the following possible ways:

- To establish an interactive communication channel with key Policy-makers and planners.
- To conduct electronic ballots for the election of government officials and other office bearers.
- To conduct public debates/opinion polls on issues of wider concern before formulation of policies and legislative frameworks.

- Filling of grievances, feedback and reports by citizens with the concerned government body.
- Establishing decentralized forms of governance.
- Performing governance functions online such as revenue collection, filing of taxes, governmental procurement, payment transfer etc.

BENEFITS OF E-GOVERNANCE

E-Governance is about reform in governance, facilitated by the creative use of Information and communications Technology. It is expected that this would lead to:

- *Better access to information and quality services for citizens*: IcT would make available timely and reliable information on various aspects of governance. In the initial phase, information would be made available with respect to simple aspects of governance such as forms, laws, rules, procedures etc. later extending to detailed information including reports (including performance reports), public database, decision making processes etc. As regards services, there would be an immediate impact in terms of savings in time, effort and money, resulting from online and one-point accessibility of public services backed up by automation of back end processes. The ultimate objective of e-Governance is to reach out to citizens by adopting a life-cycle approach i.e. providing public services to citizens which would be required right from birth to death.
- *Simplicity, efficiency and accountability in the government*: Application of IcT to governance combined with detailed business process reengineering would lead to simplification of complicated processes, weeding out of redundant processes, simplification in structures and changes in statutes and regulations. The end result would be simplification of the functioning of government, enhanced decision making abilities and increased efficiency across government – all contributing to an overall environment of a more accountable government machinery. This, in turn, would result in enhanced productivity and efficiency in all sectors
- *Expanded reach of governance*: Rapid growth of communications technology and its adoption in governance would help in bringing government machinery to the doorsteps of the citizens. Expansion of telephone network, rapid strides in mobile telephony, spread of internet and strengthening of other communications infrastructure would facilitate delivery of a large number of services provided by the government. This enhancement of the reach of government – both spatial and demographic – would also enable better participation of citizens in the process of governance.

E-GOVERNANCE EVOLUTION IN INDIA

Stages of e-Governance Evolution

It is evident that e-Governance is intrinsically linked with the development of computer technology, networking of computers and communication systems. In developing countries, such technologies and systems became available with a perceptible time lag as compared to developed nations. However, in the case of India, with the liberalization of the economy from the early 1990s onwards, there has been a convergence in the availability of cutting edge technologies and opportunities in the field of e-Governance. Generally speaking, the Indian experience demonstrates that the onset of e-Governance proceeded through the following phases:

(a) Computerisation:

In the first phase, with the availability of personal computers, a large number of Government offices got equipped with computers. The use of computers began with word processing, quickly followed by data processing.

(b) Networking:

In this phase, some units of a few government organizations got connected through a hub leading to sharing of information and flow of data between different government entities.

(c) Online presence:

With increasing internet connectivity, a need was felt for maintaining a presence on the web. This resulted in maintenance of websites by government departments and other entities. Generally, these web-pages/websites contained information about the organizational structure, contact details, reports and publications, objectives and vision statements of the respective government entities.

(d) On-line interactivity:

A natural consequence of on-line presence was opening up of communication channels between government entities and the citizens, civil society organizations etc. The main aim at this stage was to minimize the scope of personal interface with government entities by providing downloadable Forms, Instructions, Acts, Rules etc. In some cases, this has already led toon-line submission of Forms. Most citizen-government transactions have the potential of being put on e-Governance mode.

Challenges before Stakeholders

1. Lack of IT Literacy and awareness regarding benefits of e-governance

There is general lack of awareness regarding benefits of e-governance as well as the process involved in implementing successful G-C, G-G and G-B projects. The administrative structure is not geared for maintaining, storing and retrieving the governance information electronically. The general tendency is to obtain the data from the files (print) as and when required rather than using Document Management and workflow technologies. Lately the use of DMS and workflow technologies has been able to find its use only in those departments where there is perceptible lightening of workload of the subordinate staff.

2. Underutilization of existing ICT infrastructure

To a larger extent, the computers in many departments are used for the purpose of word processing only, resulting in the underutilization of the computers in terms of their use in data processing capacities for supporting management decisions. The time gap between the procurement of the hardware and development of the custom applications is so large that by the time application is ready for use, the hardware becomes obsolete.

3. Attitude of Government Employees

The psychology of government servants is quite different from that of private sectors. Traditionally the government servants have derived their sustenance from the fact that they are important repositories of government data. Thus any effort to implement DMS and workflow technologies or bringing out the change in the system is met with resistance from the government servants.

4. Lack of coordination between Govt. Department and Solution developers

Designing of any application requires a very close interaction between the Government department and the agency developing the solutions. At present the users in Government departments do not contribute enough to design the solution architecture. Consequently the solution developed and implemented does not address the requirements of an e-governance project effectively and hence does not get implemented.

5. Resistance to re-engineering of departmental processes

Successful implementation of e-governance projects requires lots of restructuring in administrative processes, redefining of administrative procedures and formats which finds the resistance in almost all the departments at all the levels. Additionally there is lack of expertise of departmental MIS executives in exploiting data mining techniques, updation and collection of real time content onto website etc. Therefore the content as is collected or maintained by various e-governance portals is unreliable or full of gaps. In such a scenario, it's difficult for any e-governance solution to achieve its intended results.

6. Lack of Infrastructure for sustaining e-governance projects on national level

Infrastructure to support e-governance initiatives does not exist within government departments. The agony is that the government departments are not equipped to be in a position to project the clear requirements nor are there any guidelines for involving private sector. Whatever efforts have been made by various Government organizations may be defined as islands of computerization. The infrastructure creation is not guided by a uniform national policy, but is dependent on the needs of individual officers championing a few projects. Therefore, the required networking and communication equipment is either nonexistent in Government departments, or if it exists at all, it does not serve any tangible purpose as far as the requirement of e-governance project is concerned. The use of connectivity options provided by Government agencies like NICNET etc. are used in a very limited manner for data transmission purpose between various locations viz. District, State , Center etc. and is mainly utilized for e-mail and Internet purpose only.

E-GOVERNANCE ACTION PLAN – STRATEGIES FOR TODAY; VISION FOR FUTURE

Most state governments have formed the IT task force and have their IT policies in place. Although policies may have lofty goals, much seems to have happened only in automation and computerization. The drawback is that these IT policy documents are not made based upon the requirements and inherent capabilities of the state but are based on the surveys and strategies used by other nations or other states. Though it is wise to take examples from the successful e-governance strategies of other states and countries, it is equally essential that we customize our state policies after a careful study of the parameters applicable to the particular state in question.

Govt. leaders in India are starting to realize that e-governance is the key to drive today's economy with an increased participation from citizens. Providing services online is no longer going to remain optional for local and central government as demand for providing services @ internet speed has been coming from the citizens.

In this era of accountability and performance measurement, governments will face increasing pressure to make the services more accessible to their citizens. The pressure comes directly from the new legislatures and government policies to implement high-end technologies in governing the nations; but also indirectly and perhaps more intensely from citizens. The citizens now a day are not using government services in isolation, but are simultaneously making transactions and interacting with the corporate world. In addition to this direct or indirect pressure, governments must themselves study & realize the cost saving benefits e-Governance techniques produce.

E-governance is about more than streamlining processes and improving services. It's about transforming Governments and renovating the way citizens participate in democracy. So how does a government agency cuts through the clutter and builds a strategy to facilitate the transition to successful online or "e" service delivery. If the government waits, its perceived as being out of touch with the citizen needs and loses an opportunity to realize the tremendous benefits of online service delivery and larger citizen participation in overall service delivery. Yet if the e-governance projects are started and implemented in haste, they are doomed to fail. According to one of the surveys conducted by a reputed agency, 75% of e-governance projects fail because of poor understanding and planning.

The real challenge is how to develop and sustain successful e-governance projects and deliver state of the art e-services to citizens. Unfortunately it is not as easy as adding "e" in front of government service delivery mechanism. Successful e-governance initiatives can never be taken in haste. Particularly for the democratic nation of the billion people like India, e-Governance should enable seamless access to information and seamless flow of information across the state and central government in the federal setup. No country has so far implemented e-governance system for one billion people.

REQUIREMENTS OF IMPLEMENTING SUCCESSFUL E-GOVERNANCE

Some of the requirements for implementing successful e-governance across the nation are:

1. E-Governance framework across the nation with enough bandwidth to service a population of one billion.
2. Connectivity frameworks for making the services reach rural areas of the country or development of alternative means of services such as e-governance kiosks in regional languages.
3. National Citizen Database which is the primary unit of data for all governance vertical and horizontal applications across the state and central governments.
4. E-governance and interoperability standards for the exchange of secure information with non-repudiation, across the state and central government departments seamlessly.
5. A secure delivery framework by means of virtual private network connecting across the state and central government departments.
6. Data centers to handle the departmental workflow automation, collaboration, interaction, exchange of information with authentication.

For success of an e-governance project and superior service delivery, it is imperative that the government agencies focus on whole citizen experience. Focusing on the citizen is essential for long term success. The govt. agencies need to integrate information from each and every point of citizen interaction. The overall architecture for e-Governance needs to ensure that the architecture components are extensible and scalable to adapt to the changing environments. The e-Governance applications that are emerging as islands of successes have to be interoperable.

Suggestion for implementing successful e-governance

(a) Create Literacy and commitment to e-governance at high level

The most important requirement is a training program for policy makers in E-Governance (Senior Public Servants), politicians and IT task force members. The training program needs to be focused according to the requirements of the policy makers at the top. Such programs can be need based and outsourced when required. In addition it should be made mandatory for all the stake holders in implementation and maintenance of e-governance services to have the general IT skills. There may be specific requirements for training in certain specific projects. Such programs can be need based and outsourced when required. A few suggestive programs include e-governance training, Building web interfaces for citizen interaction, Document management and workflow applications, security and PKI solutions, Office Automation, networking etc.

(b) Conduct Usability Surveys for assessment of existing e-governance projects

There is a varying degree of development of e-governance among the different states. A few States have leapfrogged into a digital era whereas a few are yet to start with any initiative. There is a tremendous divergence in the extent of implementation of the concept of e-Governance. It is, therefore, not possible to come up with a framework for implementation of e-Governance which is straightaway applicable to all states and the Central Government. Therefore an e-readiness exercise should be carried out in all states, government departments to understand their level of acceptability of the e-governance.

(c) Starting with implementation of pilot projects and replicating the successful ones

The pilot projects taken in various states should be accessed for their achievement levels. They should be classified as success or failure according to the desired output written down before implementation of the projects. The study should be carried out by an independent agency for the implementation agency. The study should be carried out at each stage of implementation. Bottlenecks and causes of delays should be documented, even

though they are removed later. The successful projects should be replicated over the nation with members drawn from the implementing team. The projects, which could not achieve the desired outcome, should be documented for possible causes of failure. Various bottlenecks and causes of delay should be identified.

(d) Follow the Best Practices in e-governance

The study of Best Practices will bring forward the best practices being followed in some states, nationally and internationally. The national and international Best Practices study will give a great momentum to the process of E-Governance. The State Governments will not have to re-invent wheel every time and they can learn from the developments already made.

(e) Build National resource Database of e-governance projects

This would allow any organization planning an IT project to instantly ascertain whether any such project has already been implemented anywhere in the country. Intending implementers would know who the key people in similar projects are and how to reach them. It is well known that it is much easier to replicate a solution than to evolve it the first time around. So the lead-time to implement projects can be reduced substantially.

If a project is already in operation in a similar environment somewhere in the country, acceptance by all concerned is much faster and smoother elsewhere. So change management becomes much easier and the time and effort involved in such implementations. Due recognition would accrue to the pioneers who created the successes. It would enable others to learn from them if they wish.

For implementing agencies, be they Government owned organizations like NIC, CDAC and State PSUs or private IT companies, it offers a unique opportunity to derive the full return and reward, both domestically and internationally, from their successes and the IPRs/ products that they have created. It would help create an archive of e-governance applications in the country.

(f) Have clearly defined Interoperability policy

The e-governance architecture needs to ensure that the components are scalable and adaptable to the future requirements. It has also to ensure that the local architecture fits into the State level and the same into National and Global architecture. Interoperability is a major criterion while defining the architecture.

(g) Manage and Update content on govt. websites efficiently and regularly

Content is the 'heart' of any IT project. The govt. agency has to keep in mind some of the important technical guidelines, while developing the software and computerization, to facilitate the future integration. The department also needs to address the security of transactions and messages. The process of content development encompasses a whole range of activities starting with a comprehensive study of the system and identification of the objectives. It ends up with delivery of the intended benefits to the citizens or other users of the IT System. The govt. agencies must ensure that the data on the sites is always updated and relevant.

Conclusion

It is evident from above discussion that objectives of achieving e-governance and transforming India go far beyond mere computerization of stand-alone back office operations. It means, to fundamentally change as to how the government operates, and this implies a new set of responsibilities for the executive and politicians. It will require basic change in work culture and goal orientation, and simultaneous change in the existing processes. Foremost of them is to create a culture of maintaining, processing and retrieving the information through an electronic system and use that information for decision making. It will require skilled navigation to ensure a smooth transition from old processes and manual operations to new automated services without hampering the existing services. This can be achieved by initially moving ahead in smaller informed initiatives in a time bound manner and avoiding large and expensive steps without understanding the full social implications. Every small step thus taken should be used to learn about hurdles and improve upon the next steps, both in terms of

direction and magnitude. The proposed changes are likely to be met with a lot of inertia which cannot be overcome by lower and middle level officials with half hearted attempts to diffuse the technology. The change in the mindset to develop and accept the distributed and flat structured e-governance system is required at the top level system to beat the inertia.

NATIONAL E-GOVERNANCE PLAN

Over the years, a large number of initiatives have been undertaken by various State Governments and Central Ministries to usher in an era of e-Government. Sustained efforts have been made at multiple levels to improve the delivery of public services and simplify the process of accessing them.

E-Governance in India has steadily evolved from computerization of Government Departments to initiatives that encapsulate the finer points of Governance, such as citizen centricity, service orientation and transparency. Lessons from previous e-Governance initiatives have played an important role in shaping the progressive e-Governance strategy of the country. Due cognizance has been taken of the notion that to speed up e-Governance implementation across the various arms of Government at National, State, and Local levels, a programme approach needs to be adopted, guided by common vision and strategy. This approach has the potential of enabling huge savings in costs through sharing of core and support infrastructure, enabling interoperability through standards, and of presenting a seamless view of Government to citizens.

The National e-Governance Plan (NeGP), takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision, a shared cause. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is evolving, and large-scale digitization of records is taking place to enable easy, reliable access over the internet. The ultimate objective is to bring public services closer home to citizens, as articulated in the Vision Statement of NeGP.

> **"Make all Government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realise the basic needs of the common man"**

The Government approved the National e-Governance Plan (NeGP), comprising of 27 Mission Mode Projects (MMPs) and 8 components, on May 18, 2006. The Government has accorded approval to the vision, approach, strategy, key components, implementation methodology, and management structure for NeGP. However, the approval of NeGP does not constitute financial approval(s) for all the Mission Mode Projects (MMPs) and components under it. The existing or ongoing projects in the MMP category, being implemented by various Central Ministries, States, and State Departments would be suitably augmented and enhanced to align with the objectives of NeGP.

Implementation Strategy, Approach and Methodology of NeGP

Implementation of e-Governance is a highly complex process requiring provisioning of hardware & software, networking, process re-engineering and change management. Based on lessons learnt from the past and the experience from successful e-Governance applications, the approach and methodology adopted for NeGP contains the following elements:

(i) ***Common Support Infrastructure:*** NeGP implementation involves setting up of common and support IT infrastructure such as: State Wide Area Networks (SWANs), State Data Centres (SDCs), Common Services Centres (CSCs) and Electronic Service Delivery Gateways.

(ii) ***Governance:*** Suitable arrangements for monitoring and coordinating the implementation of NeGP under the direction of the competent authorities have also been substantially put in place. The programme also involves evolving/ laying down standards and policy guidelines, providing technical support, undertaking capacity building, R&D, etc. DEITY is required to adequately strengthen itself and various institutions like NIC, STQC, CDAC, NISG, etc. to play these roles effectively.

(iii) ***Centralised Initiative, Decentralised Implementation:*** e-Governance is being promoted through a centralised initiative to the extent necessary to ensure citizen-centric orientation, to realise the objective of inter-operability of various e-Governance applications and to ensure optimal utilisation of ICT infrastructure and resources while allowing for a decentralised implementation model. It also aims at identifying successful projects and replicating them with required customisation wherever needed.

(iv) ***Public-Private Partnerships (PPP):*** PPP model is to be adopted wherever feasible to enlarge the resource pool without compromising on the security aspects.

(v) ***Integrative Elements:*** Adoption of unique identification codes for citizens, businesses and property is to be promoted to facilitate integration and avoid ambiguity.

(vi) ***Programme Approach at the National and State levels:*** For implementation of the NeGP, various Union Ministries/Departments and State Governments are involved. Considering the multiplicity of agencies involved and the need for overall aggregation and integration at the national level, NeGP is being implemented as a programme, with well-defined roles and responsibilities of each agency involved. For facilitating this, appropriate programme management structures have also been put in place.

(vii) ***Facilitator role of DEITY:*** DEITY is the facilitator and catalyst for the implementation of NeGP by various Ministries and State Governments and also provides technical assistance. It serves as a secretariat to the Apex Committee and assists it in managing the programme. In addition, DEITY is also implementing pilot/ infrastructure/ technical/ special projects and support components. DARPG's responsibility is towards Government Process Re-engineering and Change Management, which are desired to be realised across all government departments. Planning Commission and Ministry of Finance allocate funds for NeGP through Plan and Non-plan budgetary provisions and lay down appropriate procedures in this regard.

(viii) ***Ownership of Ministries:*** Under the NeGP, various MMPs are owned and spearheaded by the concerned line Ministries. In case there are any ongoing projects which fall in the MMP category, they would be suitably enhanced to align them with the objectives of NeGP. For major projects like Bharat Nirman, Rural Employment Guarantee Schemes, etc. the line ministries concerned are advised to make use of e-Governance as also automation techniques from the inception stage. States have been given the flexibility to identify a few additional state-specific projects, which are relevant for the economic development of the State.

NATIONAL E-GOVERNANCE DIVISION (NEGD)

The Capacity Building Scheme under the National e-Governance Plan (NeGP) of Government of India envisions establishment of an institutional framework for State-Level decision-making including setting-up of State e-Mission Teams (SeMTs) having relevant expertise and experience to provide technical and professional support to States and Union Territories.

For this purpose, the Department of Information Technology (DIT), Government of India, has created NeGD as an autonomous business division within Media Lab Asia, under the Ministry of Communications and Information Technology, Government of India, for taking up the tasks being carried out by the Programme Management Unit National e-Governance Plan (PMU-NeGP) at DIT.

Functions of NeGD

1. Programme Management of NeGP, inter-alia including facilitating and supporting DIT in undertaking the following tasks and responsibilities assigned to DIT under NeGP:
   (a) Facilitating implementation of NeGP by various Ministries and State Governments
   (b) Providing technical assistance to Central Ministries and State Line Departments
   (c) Serving as a secretariat to the Apex Committee
   (d) Undertaking technical appraisal of all NeGP projects to examine issues such as overall technology architecture, framework, standards, security policy, service delivery mechanism, sharing of common infrastructure etc.
   (e) Human Resource Development, Training and Awareness Building
   (f) Framing core policies, technical assistance, R&D, awareness and assessment and creation of organization structure
   (g) Acting as a Central Agency for an effective implementation of Capacity Building Scheme inter-alia involving provisioning of manpower at various SeMTs across States/ UTs
2. Positioning of a Capacity Building Management Cell for effective management of manpower at SeMTs together with management of other Scheme activities including training, setting up HR policies, etc.

E-GOVERNANCE INFRASTRUCTURE

E-governance infrastructure in Indian may be understood with the help of following figure.

The infrastructure required for implementing E governance in India is categorized as

1. State Wide Area Network (SWAN)

2. Data Centre
3. NSDG
4. Common Services Centers

STATE AREA WIDE NETWORK (SWAN)

Wide Area Network is an advanced telecommunication infrastructure, which is used now-a-days extensively, for exchange of data and other types of information between two or more locations, separated by significant geographical distances. The medium of connectivity can be copper, optical fiber cable or wireless, as may be found feasible. Such wide area networks, in a way, create a highway for electronic transfer of information in the form of voice, video and data. Department of IT in Government of India is implementing an approved Scheme known as State Wide Area Network (SWAN) Scheme, envisaged to create such a connectivity in each State / UT, to bring speed, efficiency, reliability and accountability in overall system of Government-to-Government (G2G) functioning.

SWAN Features

A wide area network deployed in a State or UT would have two components viz.

– Vertical Component

– Horizontal Component

The vertical component of SWAN is implemented using multi-tier architecture (typically, three-tier) with the State/UT Headquarter (SHQ) connected to the each District Head Quarter (DHQ) which in turn gets connected to the each Block Head Quarter (BHQ). Each SHQ, DHQ and BHQ point of connection is called a Point of Presence (PoP), which is a point of bandwidth aggregation for several network links getting connected at this point. The bandwidth provisioning for network connectivity between all the above PoPs is a minimum of 2 Mbps. Presently, the connectivity provisioning between every SHQ and DHQ is for 4 Mbps and DHQ to every BHQ is 2 Mbps. For the horizontal component, the government departments at each tier are connected to the respective PoPs.

The SWAN aims to create a dedicated Closed User Group (CUG) network of minimum speed of 2 Mbps by connecting around 7500 pops, providing Data, Voice & Video connectivity to more than 50,000 govt. offices. The networks aim at increasing the efficiency of the government delivery mechanism and optimize the performance. The backbone thus created would provide reliable, vertical and horizontal connectivity within the State / UT administration and would facilitate electronic transactions between all the government departments.

To ensure desired Quality of Service (QoS) by the Network Operator and the Bandwidth Service Provider, a Third Party Audit mechanism has been created in the SWAN Scheme which would monitor the performance of the SWAN network in each State / UT. The Third Party Audit (TPA) agency shall perform for a period of five years from the date of final acceptance test of the network and primarily monitor the compliance of the Service Level Agreement (SLA) which the State / UT would enter with the Network Operator and also with the Bandwidth Service Provider.

Status of SWAN Implementation as on April, 2012

– Till date individual SWAN proposals have been considered and approved for 33 States/UTs with an total DeitY outlay of Rs. 1,964.97 crore and Rs 562.41 have been released so far.

– The SWANs in 19 States/UTs namely, Haryana, Himachal Pradesh, Punjab, Tamil Nadu, Gujarat, Karnataka, Kerala, Jharkhand, Chandigarh, Delhi, Puducherry, Tripura, Lakshadweep, West Bengal, Sikkim, Chhattisgarh, Uttar Pradesh, Orrisa and Maharashtra have been implemented.

- The SWANs in 4 States namely, Assam, Madhya Pradesh, Bihar, Uttarakhand are in advanced stage of implementation, Network trials are being conducted at different tiers of SWAN.
- The SWANs in 4 States/ UTs namely, Andhra Pradesh, Arunachal Pradesh, Manipur, Meghalaya have identified the Network Operator and implementation is underway.
- The SWANs in 4 States namely, Jammu & Kashmir, Rajasthan, Mizoram, Nagaland, have initiated the bid process to identify the Network Operator for implementation.
- The 2 UTs namely Dadra & Nagar Haveli and Daman & Diu are in RFP/BOM finalization stage.
- The State of Goa and UT of Andaman & Nicobar Islands have implemented Wide Area Networks outside SWAN Scheme.
- Special arrangement has been made with BSNL for providing bandwidth at concessional tariff.

STATE DATA CENTRE

State Data Centre (SDC) has been identified as one of the important element of the core infrastructure for supporting e-Governance initiatives of National eGovernance Plan (NeGP).

Under NeGP, it is proposed to create State Data Centres for the States to consolidate services, applications and infrastructure to provide efficient electronic delivery of G2G, G2C and G2B services. These services can be rendered by the States through common delivery platform seamlessly supported by core Connectivity Infrastructure such as State Wide Area Network (SWAN) and Common Service Centre (CSC) connectivity extended up to village level. State Data Centre would provide many functionalities and some of the key functionalities are Central Repository of the State, Secure Data Storage, Online Delivery of Services, Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration etc. SDCs would also provide better operation & management control and minimize overall cost of Data Management, IT Resource Management, Deployment and other costs.

Department of Information Technology (DIT) has formulated the Guidelines to provide Technical and Financial assistance to the States for setting up State Data Centre. These Guidelines also include the implementation options that can be exercised by the State to establish the SDC.

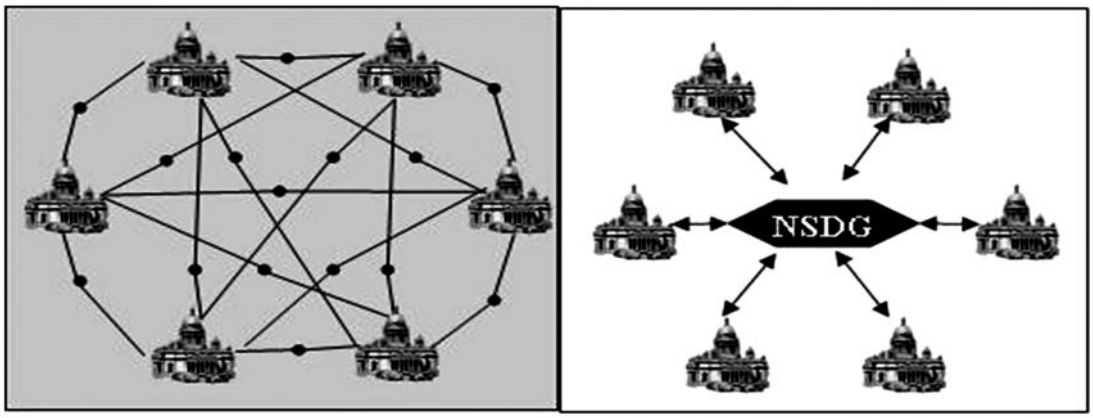
NATIONAL SERVICE DELIVERY GATEWAY (NSDG)

The National e-Governance Plan (NeGP) of the Govt. of India aims to make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realize the basic needs of the common man. One of the goals of the Government to meet this vision is the need to cooperate, collaborate and integrate information across different departments in the Centre, States and Local Government. Government systems characterized by islands of legacy systems using heterogeneous platforms and technologies and spread across diverse geographical locations, in varying state of automation, make this task very challenging. The National e-Governance Service Delivery Gateway (NSDG), a MMP under the NeGP, can simplify this task by acting as a standards-based messaging switch and providing seamless interoperability and exchange of data across.

Vision of NSDG

The emergence of many e-governance applications for different departments to provide online services to citizens, businesses and government would require increasing interactions amongst departments and with external agencies at various levels in Government. Departments would need to develop connectors/adaptors for point to point connections between departments creating a mesh as shown in figure given below and also tight coupling between applications. This would lead to applications that are difficult to maintain and upgrade in case of version change and change in government policies and business rules. The NSDG is an attempt to reduce such point to

point connections between departments and provide a standardized interfacing, messaging and routing switch through which various players such as departments, front-end service access providers and back-end service providers can make their applications and data inter-operable. The NSDG aims to achieve a high order of interoperability among autonomous and heterogeneous entities of the Government (in the Centre, States or Local bodies), based on a framework of e-Governance Standards.



Objectives of the NSDG

The objectives of the NSDG are

1. To act as a core infrastructure for achieving standards-based interoperability between various e-Government applications implemented at various levels and geographically dispersed locations.
2. To evolve Gateway messaging standards and build a government owned Central Gateway based on these standards.
3. Act as a catalyst in enabling the building of Standards based e-Governance applications with Gateway as the middleware to ensure interoperability
4. Enable integration across Centre, State or Local Governments there by enabling Integrated Service Delivery and a Service Oriented Architecture (SOA) leading to joined up government
5. Help protect the legacy investments in software and hardware by easily integrating them with other technology platforms and software implementations
6. De-link the back-end departments/Service Providers (SP) from the front-end Service Access Providers thereby
   (a) Ensuring separation of concerns of service access from the service implementation i.e. separates the Portal, CSC, Kiosks etc from the government services which reside in the backend departments.
   (b) Encouraging competition at the front-end by allowing independent service access providers to provide services with varying levels of complexity, cost and service quality levels.
7. Enable adding of shared services on to the core services as and when required,as special common services of the Gateway without affecting the core functionality of the Gateway, thereby providing flexibility and modularity.
   (a) encourage back-end services to be plugged into the infrastructure as and when they are ready,
8. Reduce the cost of e-Governance Projects by rationalizing, distributing and optimizing the services framework
9. Use PKI infrastructure for secure transactions. Provision exists for encryption of department payload to

ensure confidentiality of department data. The gateway provides digital signature and certificates to all stakeholders interacting with the gateway for identification, authentication and authorization. Transaction and audit logs help track government data.

10. Use PKI infrastructure for secure transactions. Provision exists for encryption of department payload to ensure confidentiality of department data. The gateway provides digital signature and certificates to all stakeholders interacting with the gateway for identification, authentication and authorization. Transaction and audit logs help track government data.
11. Enable transaction logging and time stamping for tracking of transactions and centralised control
12. Help the Departments backend workflow evolve gradually as the Gateway acts as a middleware de-linking the backends from the front end. This means that even the departments which do not have the complete automation or work flow at the back can still deliver e-Service to the citizens in a limited manner through the Gateway. To cite as an example, a server may be put up at the department for message exchange with Gateway in absence of readily available infrastructure at the department.

COMMON SERVICES CENTERS

In the year 2006, The Government of India launched CSC Scheme for setting up of more than one lakhs (100,000) internet enabled centers in rural areas under the National e-Governance plan (NeGP) in a Public Private Partnership (PPP) mode.

The Common Services Centers (CSC) are proposed to be the delivery points for Government, Private and Social Sector services to rural citizens of India at their doorstep . The CSC Scheme is envisaged to be a bottom-up model for delivery of content, services, information and knowledge, that can allow like–minded public and private enterprises – through a collaborative framework – to integrate their goals of profit as well as social objectives, into a sustainable business model for achieving rapid socio–economic change in rural India.

As on 31st December 2012, a total of 99,247 CSCs are operational in thirty three States/UTs. 100% CSCs have been rolled out in 10 (Ten) States (Arunachal Pradesh, Chandigarh, Gujarat, Kerala, Madhya Pradesh, Manipur, Meghalaya, Mizoram, Sikkim & Tripura). More than 70% of the rollout has been completed in 12 (Twelve) States (Assam, Bihar, Chhattisgarh, Himachal Pradesh, Jharkhand, Maharashtra, Pondicherry, Punjab, Rajasthan, Uttar Pradesh, Uttaranchal and West Bengal). As of November 2012, approximately 10,000 CSCs are providing financial services including banking, micro&finance and insurance services to over 1.8 lakhs citizens.

The State Governments like Andhra Pradesh, Assam, Bihar, Gujarat, Haryana, Jharkhand, Kerala, Maharashtra, Orissa, Rajasthan, Tamil Nadu, Uttar Pradesh and West Bengal have issued Government Orders / Notifications to the various departmental heads / District Level authorities/ Stakeholders for use of CSC to deliver various G2C Services. The various G2C Services offered are: Agricultural services, RTI Services, NREGA MIS Data Entry service, Postal Products, Land Records, Issuance of Birth and Death Certificates, Utility Services, Electoral Services, Transport Services, Grievances, e-District Services, etc. Financial Inclusion has started in the States of Andhra Pradesh, Jammu & Kashmir, Madhya Pradesh, Meghalaya, Maharashtra, Tripura and Uttar Pradesh.

LESSON ROUND-UP

- *'E-governance is the application of information & communication technologies to transform the efficiency, effectiveness, transparency and accountability of informational & transactional exchanges with in government, between govt. & govt. agencies of National, State, Municipal & Local levels, citizen & businesses, and to empower citizens through access & use of information'*.
- There are five models of E-Governance e.g.
  - Broadcasting/Wider-Dissemination Model

  - Critical Value Information - Flow Model
  - Comparative Analysis Model
  - Interactive-Service Model (G2C2G)
  - Virtual reality

- There are various challenges to governance evolution in India as *Lack of IT Literacy and awareness regarding benefits of e-governance, Underutilization of existing ICT infrastructure, attitude of government department* Lack of coordination between Govt. Department and Solution developers, Resistance to re-engineering of departmental processes, Lack of Infrastructure for sustaining e-governance projects on national level
- For getting the e governance implemented following may be done
  (a) Create Literacy and commitment to e-governance at high level
  (b) Starting with implementation of pilot projects and replicating the successful ones
  (c) Follow the Best Practices in e-governance.
  (d) Build National resource Database of e-governance projects
  (e) Have clearly defined Interoperability policy
  (f) Manage and Update content on govt. websites efficiently and regularly
- National E-governance division (NeGD) has been formed by Government of India as an autonomous business division within Media Lab Asia, under the Ministry of Communications and Information Technology, Government of India, for taking up the tasks being carried out by the Programme Management Unit National e-Governance Plan (PMU-NeGP) at DIT.
- The National e-Governance Plan (NeGP), takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision, a shared cause.

  The Government approved the National e-Governance Plan (NeGP), comprising of 27 Mission Mode Projects (MMPs) and 8 components, on May 18, 2006.
- Wide Area Network is an advanced telecommunication infrastructure, which is used now-a-days extensively, for exchange of data and other types of information between two or more locations, separated by significant geographical distances. Such wide area networks, in a way, create a highway for electronic transfer of information in the form of voice, video and data. Department of IT in Government of India is implementing an approved Scheme known as State Wide Area Network (SWAN) Scheme, envisaged to create such a connectivity in each State / UT, to bring speed, efficiency, reliability and accountability in overall system of Government-to-Government (G2G) functioning.
- The National e-Governance Plan (NeGP) of the Govt. of India aims to make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realize the basic needs of the common man. The National e-Governance Service Delivery Gateway (NSDG), a MMP under the NeGP, can simplify this task by acting as a standards-based messaging switch and providing seamless interoperability and exchange of data across.
- In the year 2006, The Government of India launched CSC Scheme for setting up of more than one lakhs (100,000) internet enabled centers in rural areas under the National e-Governance plan (NeGP) in a Public Private Partnership (PPP) mode. The Common Services Centers (CSC) are proposed to be the delivery points for Government, Private and Social Sector services to rural citizens of India at their doorstep.

– The CSC Scheme is envisaged to be a bottom-up model for delivery of content, services, information and knowledge, that can allow like–minded public and private enterprises – through a collaborative framework – to integrate their goals of profit as well as social objectives, into a sustainable business model for achieving rapid socio–economic change in rural India.

SELF-TEST QUESTIONS

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. What do you mean by the term E-governance? Explain its importance and history in India.
2. Explain the different e-governance models being used in India.
3. Explain the challenges being faced by government in implementing e governance in India.
4. Write a short note on e governance action plan.
5. What do you mean by national e governance division?
6. Write a short note on National e governance plan.
7. Explain the different constituent of E governance infrastructure in India.
8. Write a short note on
   (a) State wide area network (SWAN)
   (b) National service delivery gateway (NSDG)
   (c) Common Service centre

Lesson 11
Systems Audit – An Overview

LESSON OUTLINE

- Nature, Significance and Scope of Systems Audit.
- Steps Involved in Conducting Systems Audit
- Systems Audit and Management Functions
- Systems Audit of Computerized Secretarial Functions
- Norms and Procedure for Computerization, Computers Control and Security
- Testing of Computer Systems – Documentation Standards, Policies and procedures and Audit Approach

LEARNING OBJECTIVES

Information systems auditing or systems audit is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently.

It is done to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity. System audit supports traditional audit objectives and management objectives.

The knowledge of system audit is very important for all professionals as system has become an integral part of all processes. Most of our work has become systemized and information technology driven so it become necessary for a company secretary to know about basic concepts relating to systems audit.

After going through this lesson, one should be able to –

- Understand about the nature and scope of system audit
- Understand the information system audit process
- Understand the relationship between information system audit and different functions of management.
- Design a information system audit plan
- Carry out the system audit of secretarial function

The systems audit, unlike the other audits, is not restricted to audit of reported items only. It has to take into cognizance the choice, use and risk of Technology. It has to look at the realities of business processes and constantly changing legal framework.

INTRODUCTION

Increasing competition in business has driven companies to compress their internal processes and focus more on the customers and external business environment. In the process, more and more of business processes have been brought under the purview of systems based on information technology. There has been an increase in complexity by several orders of magnitude. The arrival of the World Wide Web and the shift of traditional computer systems into their "web-based" avatar have only added new dimensions in the form of threats to security.

A Company Secretary cannot function effectively in this information age without adequate knowledge of the benefits and demerits of information systems. The Company Secretary addresses the vital areas of good corporate governance and compliance within the regulatory framework of the applicable laws. S/he is also a custodian and user of the top level MIS that goes to the Board of Directors, besides the Secretarial Systems.

This study lesson has been prepared to provide an insight into the subject of Systems Audit in the modern context of enterprise systems and connectivity with Buyers, Suppliers and other Stakeholders.

What is system Audit?

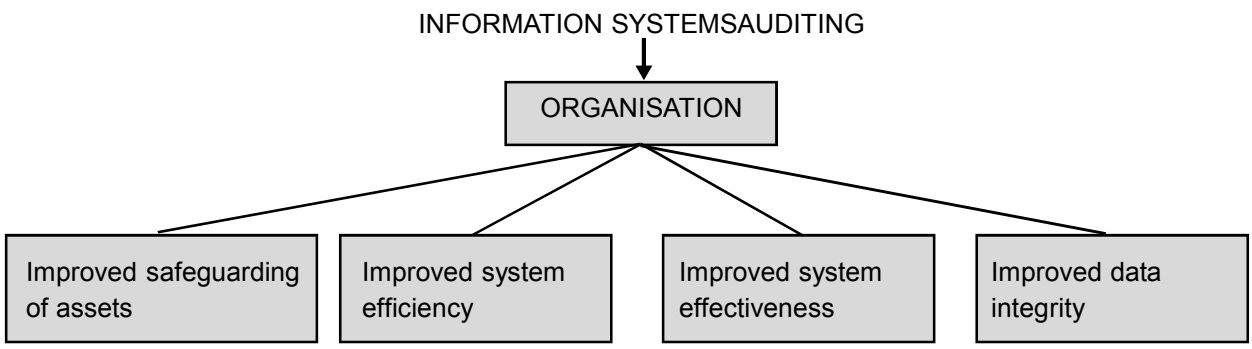
50 years ago most of our information & data processing needs were fulfilled manually; today computers are used extensively to process data and to provide decision-making. The information system does not necessarily mean the computer based information system. The Information Technology is a major component of Information System and in itself not a solution. Nowadays, with the widespread availability of powerful microcomputers and packaged software, the Information Technology is the backbone of information system. Because computers play a large part in assisting us to process data and to take decisions. It is important that their use be controlled. The uncontrolled use of computers can have a widespread impact on society. For example, inaccurate information causes misallocation of resources within the economy and fraud can be perpetrated because of inadequate system controls.

Information systems audit has been focused on whether the systems safeguard the assets, maintain data integrity, and facilitate the achievement of objectives of the company.

Information Systems Auditing Defined

Information systems auditing or systems audit is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently. Thus, information systems auditing supports traditional audit objectives; attest objectives (those of the external auditor) that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditor) that encompass not only attest objectives but also effectiveness and efficiency objectives.

Sometimes information systems auditing has another objective-namely, ensuring that an organization complies with some regulation, rule or condition. For example, a bank might have to comply with a government regulation about how much it can lend;



Asset Safeguarding Objectives

The information system assets of an organization include hardware, software, facilities, people (knowledge), data files, system documentation, and supplies. Like all assets, they must be protected by a system of internal control. Hardware can be damaged maliciously. Proprietary software and the contents of data files can be stolen or destroyed. Supplies of negotiable forms can be used for unauthorized purposes. These assets are often concentrated in one or a small number of locations, such as a single disk. As a result, asset safeguarding becomes an especially important objective for many organizations to achieve.

Data Integrity Objectives

Data integrity is a fundamental concept in information systems auditing. It is a state implying data has certain attributes: completeness, soundness, purity, and veracity. If data integrity is not maintained, an organization no longer has a true representation of itself or of events. Moreover, if the integrity of an organization's data is low, it could suffer from a loss of competitive advantage. Nonetheless, maintaining data integrity can be achieved only at a cost. The benefits obtained should exceed the costs of the control procedures needed.

Why Data integrity is Important?

Three major factors affect the value of a data item to an organization and thus the importance of maintaining the integrity of that data item:

1. The value of the informational content of the data item for individual decision makers: The informational content of a data item depends on its ability to change the level of uncertainty surrounding a decision and, as a result, to change the expected payoffs of the decisions that might be made. These notions have been well developed within statistical decision theory.
2. The extent to which the data item is shared among decision makers: If data is shared, corruption of data integrity affects not just one user but many. The value of a data item is some aggregate function of the value of the data item to the individual users of the data item. Thus, maintenance of data integrity becomes more critical in a shared data environment.
3. The value of the data item to competitors: If a data item is valuable to a competitor, its loss might undermine an organization's position in the marketplace. Competitors could exploit the informational content of the data item to reduce the profitability of the organization and to bring about bankruptcy, liquidation takeover, or merger.

System Effectiveness Objectives

An effective information system accomplishes its objectives. Evaluating effectiveness implies knowledge of user needs. To evaluate whether a system reports information in a way that facilitates decision making by its users, auditors must know the characteristics of users and the decision-making environment.

Effectiveness auditing often occurs after a system has been running for some time. Management requests a post audit to determine whether the system is achieving its stated objectives. The evaluation provides input to the decision on whether to scrap the system, continue running it, or modify it in some way.

Effectiveness auditing also can be carried out during the design stages of a system. Users often have difficulty identifying or agreeing on their needs. Moreover, substantial communication problems often occur between system designers and users. If a system is complex and costly to implement, management might want auditors to perform an independent evaluation of whether the design is likely to fulfill user needs.

System Efficiency Objectives

An efficient information system uses minimum resources to achieve its required objectives. Information systems

consume various resources: machine time, peripherals, system software, and labor. These resources are scarce, and different application systems usually compete for their use.

The question of whether an information system is efficient often has no clear-cut answer. The efficiency of any particular system cannot be considered in isolation from other systems. Problems of sub-optimization occur if one system is "optimized" at the expense of other system. For example, minimizing an application system's execution time might require dedication of some hardware resource (e.g., a printer) to that system. The system might not use the hardware fully, however, while it undertakes its work. The slack resource will not be available to other application system if it is dedicated to one system.

System efficiency becomes especially important when a computer no longer has excess capacity. The performance of individual application systems degrades (e.g., slower response times occur), and users can become increasingly frustrated Management must then decide whether efficiency can be improved or extra resources must be purchased. Because extra hardware and software is a cost issue, management needs to know whether available capacity has been exhausted because individual application systems are inefficient or because existing allocations of computer resources are causing bottlenecks. Because auditors are perceived to be independent, management might ask them to assist with or even perform this evaluation.

General objectives of System Auditing

The general information system auditing objectives are as follows:

- Validation of the organizational aspects and administration of the information service function.
- Validation of the controls of the system development life cycle.
- Validation of access controls to installations, terminals, libraries, etc.
- Automation of internal auditing activities.
- Internal training.
- Training members of the information service function department

Management should be primarily interested in information system audit auditing in order to prevent:

- Excessive time and development costs.
- Unrealistic or impossible objectives to comply with.
- Rigid systems when they become operational.
- Non-compliance with value added benefits.
- Costly methods and systems.

The lack of control involves many risks. Many systems fail because of some of the following reasons:

- Lack of management technical capacity.
- Lack of management support in system development.
- Inexperience of employees or lack of training.
- Unrealistic expectations with wrong orientations.

Information System Audit Plan

To approach an information system, a plan has to be developed, similar to the ones used in financial auditing. Some of the tasks involved are as follows:

- Definition of scope and objectives.

- Analysis and understanding of standard procedures.
- Evaluation of system and internal controls.
- Audit procedures and documentation of evidence.
- Analysis of facts encountered.
- Formation of opinion over the controls.
- Presentation of report and recommendations.

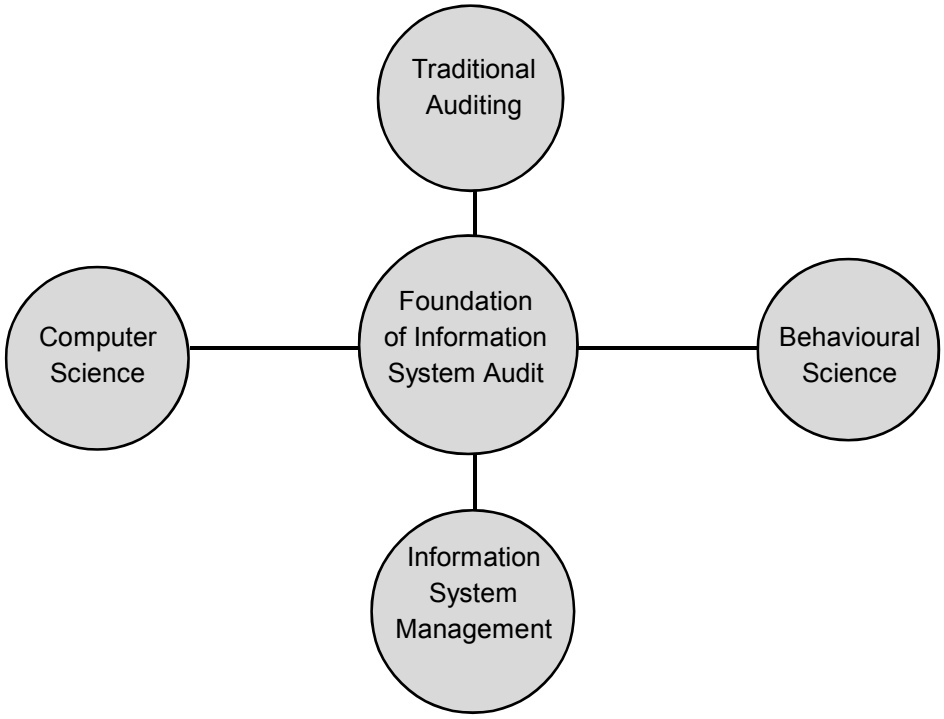
One of the most difficult things in drawing the information system audit plan is to determine the objectives and scope of the audit. As guidance, one can take into account the following variables to determine such scope:

- Extension and scope of the financial audit taking place.
- Duration and nature of the review, internal and external audit.
- Dimension of the installation and level of complexity.
- Level of both centralization and distribution of systems and integration of databases.
- Existence of procedures and norms for the development and production environment.

Foundations of Information Systems Auditing

Information systems auditing is not just a simple extension of traditional auditing. Recognition of the need for an information systems audit function comes from two directions. First, auditors realized that computers had affected their ability to perform the attest function. Second, both corporate and information systems management recognized that computers were valuable resources that needed controlling like any other key resource within an organization.

The discipline of information systems auditing has been shaped by knowledge obtained from four other disciplines which are described below



FOUNDATION OF INFORMATION SYSTEMS AUDITING

Traditional Auditing

Traditional auditing brought to information systems auditing a wealth of knowledge and experience with internal control techniques. This knowledge and experience has had an impact on the design of both the manual and machine components of an information system.

For example, in a computer system, clerical activities, such as data preparation activities, are often a critical component of the system. As with manual systems, these activities should be subject to internal control principles such as separating incompatible duties, having competent and trustworthy personnel, and establishing clear definitions of duties. By applying these principles, management seeks to ensure that the integrity of data is maintained before it is entered into the computer-based components of the information system.

Similarly traditional auditing concepts like control totals are also relevant to the update and maintenance of files by computer programs. Computer programs must ensure that all transactions data are processed and that they are processed correctly. Control totals have had long-standing use in information systems because these concerns also exist when humans (rather than programs) update and maintain files.

The general methodologies for evidence collection and evidence evaluation used by information system auditors are also based on traditional auditing methodologies. The long evolution of an extensive experience gained in traditional auditing highlight the critical importance of having objective, verifiable evidence and an independent evaluation of information systems.

Perhaps most important, traditional auditing brings to information systems auditing a control philosophy. It is difficult to articulate the nature of this philosophy. One can glean elements, however, by reading auditing literature or examining the work of auditors. The philosophy involves examining information systems with a critical mind, always with a view to questioning the capability of an information system to safeguard assets, maintain data integrity, and achieve its objectives effectively and efficiently.

Information Systems Management

The early history of computer-based information systems shows some spectacular disasters. Massive cost overruns occurred, and many systems failed to achieve their stated objectives. As a result, for many years researchers have been concerned with identifying better ways of managing the development and implementation of information systems.

Some important advances have been made. For example, techniques of project management have been carried across into the information systems area with considerable success. Documentation, standards, budgets, and variance investigation are now emphasized. Better ways of developing and implementing systems have been developed. For example, object-oriented analysis, design, and programming have enabled programmers to develop software faster, with fewer errors and easier maintenance characteristics. These advances affect information systems auditing because they ultimately affect asset safeguarding, data integrity, system effectiveness, and system efficiency objectives.

Behavioral Science

Computer systems sometimes fail because their designers do not appreciate the difficult human issues that are often associated with the development and implementation of a system. For example, behavioral resistance to an information system can seriously undermine efforts to meet asset safeguarding, data integrity, system effectiveness, and system efficiency objectives. Disgruntled users could try to sabotage the system or to circumvent controls. Similarly, designers and users could have difficulty communicating with one another because they have different conceptions of the meaning inherent in an application domain. Because of these difficulties, a system's requirements might be poorly formulated.

Auditors must understand the conditions that can lead to behavioral problems and, as a result, possible system failure. Behavioral scientists, especially organization theorists, have contributed much to our understanding of the "people problems" that can arise within organizations. For some time, several researchers have been applying the findings of organisation theory to information systems development and implementation. For example, some researchers now emphasize the need for systems designers to consider concurrently the impact of a computer system on task accomplishment (the technical system) and the quality of work life of persons (the social system) within the organization. Other emphasize the need for information systems designers to understand how users socially construct" the meaning of the domains in which they work.

Computer Science

Computer scientists also have been concerned with how asset safeguarding, data integrity, system effectiveness, and system efficiency objectives might be better achieved. For example, they have conducted research on how to prove the correctness of software formally, built fault-tolerant computer systems, design secure operating systems, and transmit data securely across a communications link.

The in-depth, technical knowledge that has been developed with the discipline of computer science provides both benefits and problems for auditors' work. On the one hand, they can now be less concerned about the reliability of certain components in a computer system. On the other hand, if this technical knowledge is used improperly, they might have difficulty detecting the abuse. For example, if a skilled systems programmer decides to perpetrate a fraud, it might be almost impossible for auditors to detect the fraud unless they have extensive knowledge of information systems technology.

NATURE, SIGNIFICANCE AND SCOPE OF SYSTEMS AUDIT

Nature of System Audit

It has been the practice in Industry to carry out Financial, Managerial and Technical audits. The oldest and most prevalent audit has been the Financial Audit. Traditionally, financial auditors have been going by the paper-based book of accounts. They have been focusing mainly on ensuring internal controls and compliances with the laws of the land, and thereby, good governance.

Managerial audit has been focusing on the basic Management policies and practices, with the aim of determining whether the enterprise is in good shape, has good processes and has a good feedback framework for managerial effectiveness and performance.

Technical audit has been focusing more on the shop floor details, such as, whether the manufacturing and maintenance functions are performing efficiently.

With the increasing use of computer-based systems in the enterprise, the complexity of systems and risk of errors, sabotage and fraud have increased manifold. In a network setup, a transaction is initiated in a physically different location, posted in the books elsewhere and the management information aggregated from the data viewed somewhere else. Because of the number of agencies involved and the increased risk exposure of mechanized systems, it is no longer sufficient to go by auditing of the book-based accounts. One has to see the vulnerability of the IT setup to external "crackers" and "hackers".

There is an example of a company which co hosted its server in the Data Center of a Service Provider. The necessary security precautions were not taken, as a result of which a cracker could get into the Mailing system and use the server to send unsolicited spam mail to tens of thousands of addressees all over the world. The identity of the server figured in the entire watchdog lists of the Internet. The result was, several sites blocked the server. Isolated from the rest of the world, the company was forced to request the service provider to give a new set of IP addresses. It had to hire experts on an emergent basis to reinstall the server after plugging the security loopholes. In the process it had to suffer a week of isolation from the outside world. After the reinstallation, it took

another 72 hours for all sites to remove the name of the site from their blacklist. Conventional audit would not normally be addressing such issues.

The nature of systems audit, unlike the other audits, is not restricted to audit of reported items only. It has to take into cognizance the choice, use and risk of Technology. It has to look at the realities of business processes and constantly changing legal framework.

Significance of System Audit

The significance of systems audit is sharply highlighted by the way businesses are changing. For any business (for profit or for nonprofit) to survive, it must have an adequate information security system in place. How to know that a system is secured is when an audit is carried out on the system.

In a nut shell, the world would be a worry free place if we have the assurance that are information (trade secrets, private information, personal identity, etc) are safe, hence, the importance of auditing an information system. The system audit is mainly getting importance for various reason but few of them are explained as below:

1. To Ensure the Security of Information

Information is a vital asset of any entity that needs to be seriously secured or face the consequence of not doing so. Information security has become so vital that many large organizations have full-fledged department that handles the inflow and outflow of information. Information security is not all about securing the data in your data warehouse, it goes beyond that. By information security audit, the activities of actors in the information domain need to be monitored more than ever. The advent of mobile computing and Smartphone created a new loophole in the business of handling information which the information audit must track down and proffer solution to.

2. To Filter out Noise in the System

Noise in any information system is a key factor that causes mistakes, misunderstandings and misrepresentation of facts which has proved to be fatal over the period of time. It is by auditing the system that carries the information flow that such noises are identified and corrective action taken to either remove or ameliorate their effects on the organization.

3. Building Confidence and Public Reputation

The general public would rather go with a secured system with lesser benefit than with an unsecured system with more benefits. This is more pronounced in the world of business and investment where investors seek the safety of their capital first before profit. This is a rational thing to do as the number one tenet of investing and financial management is to ensure the safety of your capital. The general idea behind any form of auditing of any kind is to render credibility to a piece of information

The role of information auditing also include improving the general standard of living in an economy. Through adequate information audit, treats to human lives and properties are identified and remove if possible. This will also go a long way in preventing these cycles of global financial crisis that we face these days

Scope of Information System Audit

The scope of systems audit covers the entire IS management process. The scope includes review of the entire design & development process, the review of technology choice, the processes employed to assess risks and losses that could accrue to the system, the possibility of computer frauds, the care taken in managing changes to the system, extent of testing and reliability of the system. It also cover Senior management involvement, review applicable minutes Network, workstation, Internet, disaster recovery, and other IT security policies, Overall security procedures, Segregation of IT duties, Internal quality and integrity controls, Data communication security, User identification authorization, User level of accessibility, Restricted transactions, Activity and exception reports, Backup procedures, Other operational security controls, Insurance coverage, Network security including the

internet, Internal auditing procedures, Contingency planning and disaster recovery, Internet security procedures, Vendor due diligence etc.

INFORMATION SYSTEM AUDIT PROCESS

IS Audit is an evaluation of adequacy of controls. In a computerised environment, controls can be classified as under, which are verified by the IS Auditor:

A. Management Controls

1. Security Policy and Standards
2. Constitution of Steering Committee
3. Business Continuity Planning
4. Systems Development Methodology

B. Operational Controls

1. Monitoring physical assets
2. Ensuring adequate environmental controls such as Air-conditioning (dust, temperature & humidity controls), Power Conditioning (Online UPS functioning all the time with backups, proper earthing)

C. Organizational Controls

1. Defining roles, responsibilities and duties of User Departments and IT Department
2. Defining roles, responsibilities and duties within IT Department – such as developers, operators and administrators

D. Application Controls

1. Each of the Computer Systems and subsystems must have its own set of controls for Inputs, Processing & Outputs. Processing controls should also ensure checks for legal compliance.
2. While performing the audit, each of the controls needs to be studied for its existence and adequacy.

AUDIT OF MANAGEMENT CONTROLS

1. Security Policy and Standards

The IS auditor should first verify whether the organization has a Security Policy. If it does not exist, the auditor needs to point this out, unless the management has a corporate IS Security policy and follows standard implementation of IS Security across all units and divisions.

If a security policy exists, it needs to be examined for currency and adequacy in proportion to the risk. The security policy has to be always dynamically updated.

2. Steering Committee for Security

The formulation and implementation of a sound security policy should not be the handiwork of just the IT Department. It should be a team effort, brought into effect by a committee in which there is at least one member of the Board of Directors apart from the CIO and User HoDs. The auditor should point out the absence of such a committee.

Without such a committee having regular planned meetings with agenda and action points, the implementation of security policy would be in jeopardy. The auditor needs to stress upon the possible benefits of a properly functioning steering committee or conversely, the disbenefits of not having such a committee. In recommending

the constitution and functioning of the committee, the auditor should be specific about composition, individual roles and responsibilities and monitoring/ escalating mechanism.

3. Business Continuity Planning

Business Continuity is a very important aspect of Information Systems. It encompasses all aspects that can result in usage discontinuity. As a simple example, let us say that a company has three servers connected to a single UPS. The UPS is not under Annual Maintenance Contract. Its batteries may be dying out. Since there is no mechanism to look into the health of the UPS, it can go down without a warning, resulting in a server tripping. All work halts till the UPS can be set right. If such a catastrophe occurs in a remote place, then the time to repair/ replace the UPS can be longer.

The IS Auditor should examine all such possibilities by which the availability of Computer Systems is threatened with temporary or permanent breakdown. In sensitive areas, even proofing against mob violence/terrorist strikes should be kept in view.

4. Systems Development Methodology

In most companies Systems Development is badly handled. And proper documentation is not maintained. The code is developed in great hurry and control aspects are given the go by. The accuracy of the processing and the legal compliance are left as open questions.

The IS auditor should verify whether following documents exist or not:

1. Functional requirement Specifications
2. Software requirement Specifications
3. Design Description
4. Software code
5. Test Plan
6. Unit test results
7. Integration test results
8. Acceptance test results

The documentation should be properly cross-indexed. The effect of a change made in the system should be well understood. It should not happen that, due to ignorance of the entirety of the business process and its ramifications, a change made in one area affects other areas, that too after a lapse of time.

Every time a change is made, a thorough testing should be done and documented.

The IS Auditor should get necessary evidence and comment on the lack of proper adherence to procedure.

AUDIT OF OPERATIONAL CONTROLS

The Auditor should observe the operations and comment on the drawbacks. Some of the possible scenarios are:

(a) Anybody walks into the server room and has access to documents/media/ machines.

(b) Backup media not labeled properly and kept under lock and key.

(c) One set of backup not regularly kept at another location

(d) No documented and organized change control process. Software and data are arbitrarily changed.

(e) Correction of errors not done by reversal of entry but by running dangerous script on the database backend.

(f) Administrator passwords freely floating around and used by developers, operations staff and administrators.

(g) Dirty network cabling with loose cables hanging around, hand crimped cables, cables not tagged for easy identification.

(h) Switches/hubs lying loose on tables/hanging on walls.

(i) Data controls not properly checked and filed.

(j) Preventive Maintenance of Servers not done.

(k) Machines working with covers kept off.

(l) Media not properly labeled and recorded in media register.

(m) Absence of gate pass culture: machines arbitrarily taken from/into computer rooms.

(n) Unknown and untrusted floppies directly used without checking for virus.

The above scenarios speak of a very casual IT setup. Such carelessness can result in serious downtime. Sensitive data can be pilfered from the servers. The IS auditor needs to highlight these flaws as serious lapses.

AUDIT OF ENVIRONMENTAL CONTROLS

The following environmental factors need to be checked and commented upon by the auditor:

(i) Online UPS not used; either line-interactive UPS or Offline UPS used, or CVT used.

(ii) Electrical cabling loose / points having loose contact.

(iii) No separate earth pit for the Computing equipment.

(iv) Switches/Hubs/Routers not fed UPS power.

(v) Server room door kept open.

(vi) AC not functioning properly, especially in summer.

(vii) In winter AC set at 29 Deg C instead of 22 Deg C.

(viii) No pest control measures taken.

(ix) Eatables taken into server room/ Smoking in the server room.

(x) Heavy duty printer kept inside server room: scope for dust.

(xi) UPS, AC, other electricals not under regular AMC.

(xii) No genset backup in case City power supply fails for long hours.

(xiii) No smoke detectors/fire alarms in server room area.

(xiv) Fire extinguishers not kept filled and ready.

(xv) No fire drill carried out to make people aware of dos and don’ts

The above are serious lapses that can seriously affect the functioning of the IT Setup and cause work stoppages.

AUDIT OF ORGANIZATIONAL CONTROLS

There needs to be an effective Organization Chart for the IT function. In some Organizations, IT is treated as a

technician's job. A very junior person is made the head of IT. He/she will be unable to hold his own when powerful functional heads as the Finance Head or the Production head keep breathing fire. It is best to have the IT function reporting to the CEO. The Head of IT is the Chief Information Officer or CIO.

The CIO should have three reportee managers – one for taking care of the development team, one for ensuring Information System / IT Center security and another for managing the facilities (i.e., operations and maintenance of hardware, OS, database administration, vendor management, service providers, etc.) It is advisable not to club IS security with operations or development.

The IS auditor should look for a succession plan for the IT Management team. The main concern here is that a few persons may be knowing the ins and outs of the software. They may be fixing problems because of their deep knowledge of the code. Other than in their minds, there is no documentation of what they know. Either because of their leaving the organization or their disgruntlement, they may not keep doing the good work. Such an event would compromise the functioning of the systems and emergent solution to the problem may be very expensive.

The IS Auditor should check for clear-cut definition of User role, IT Role so that there are no ambiguous overlaps. For example, it should be clear that the Wage Administration section would advise tax rate changes, etc. to the development and maintenance team member concerned. Under the formal authorization of the user HoD, such changes should be carried out. Deciding which data should be kept and which should not be kept is the responsibility of the User and not IT Department. Making a final pronouncement on the correctness of processing by software is again the concerned User Department responsibility.

There are companies in which there is no specific duty allocation to IT Staff members. This is not desirable, since everybody escapes accountability. One section of IT Department must take the responsibility for developing and maintaining the software. They should have nothing to do with the Hardware upkeep, System, Network and Database administration. This should be looked after by another set of people. Systems security was earlier the purview of the system administration staff. Given the increasing dependence on computer systems and the ever-increasing security risks, it is necessary to ensure that no person who has executive responsibility should have anything to do with an audit type of function. This is the reason why Security and Audit of systems should be the responsibility of a different section. This group needs to have a very good technical knowledge of IT and security risks. It would only audit and report findings to the management without getting into actual solution implementation. Any deviation in this regard needs to be pointed out by the IS Auditor, including an impact analysis.

STEPS INVOLVED IN CONDUCTING IS AUDIT

1. Purviewing the environment

The auditor must understand which applications are running on which machines, etc. S/he must meet the IT and Users to get a complete picture. S/he meets and discusses with the Development and maintenance staff as well as the facilities management people. In case the auditor decides to use any Audit software, s/he must decide whether the given environment would support it. S/he must also assess her/his own technical knowledge specific to the system and enhance it as necessary. The Auditor thus:

(a) Understands the audit objectives in specific terms such as areas covered in the past, areas to be revisited, etc.

(b) Defines the scope clearly

(c) Gathers necessary background information through interviewing the people concerned.

2. Understanding the Information Systems

The auditor should go through the system documentation to understand the overall framework and individual

subsystems. S/he should start with inputs originating in the user department and walk through the entire system to understand how it gets processed. Any deficiencies or hurdles faced – such as non-availability of the documentation – should be straightaway recorded. The auditor then makes her/his own short notes on the system functioning. Particular attention is given to the control aspects, such as assuring completeness of inputs, correctness of inputs, how correctness of processing is ensured and how completeness and correctness of reports, especially the infrequent but important ones. The job of understanding Application Systems can be made easier and faster by preparing a flow chart and verifying the same.

3. Identifying the Audit Risks

Risks in the context of Auditing Systems are of two kinds:

(a) Risk of loss, non-compliance with laws, etc. which arise from the system and its usage.

(b) Detection risks arising out of the inadequacies and problems in the audit process itself.

The first task before the Auditor is to assess the risks and prioritize the same. The commonly associated risks are:

(c) Unreasonable processing (e.g., system accepts a salary rate for a Peon higher than that of a General Manager).

(d) Repetition of errors – one error in the processing logic leads to a large volume of errors.

(e) Cascading of errors – in integrated systems, the output of one subsystem goes as input to another, and so on. Propagation of error from one subsystem can thus cascade into several errors in the linked subsystems.

(f) Incorrect data entry – while amounts and other numerical entries may be brought under the purview of control/hash totals and thus detected, entries such as Product type (which may determine the Excise duty, Sales Tax, etc.) can only be detected if the code is out of range or of a different type. If A and B are valid codes and B is entered for A, then the error could go unnoticed.

(g) Concentration of control responsibility – in manual systems, same transaction is seen by several persons, increasing the chances of detection of errors. In Information systems, since so much of integrated processing takes place, the error control has to be much more rigorous.

The next step is to see which of the risks can have serious adverse outcomes and assign higher priority to them. Some of the risks may be trivial and hence dropped from the list.

4. Identifying Audit Evidence

The IS Auditor has to make an exhaustive list of evidence to be gathered from the flow chart and the risk analysis.

The audit evidence is then documented in terms of the medium of data, data format and structure, database used, backup period, frequency of updates. etc.

This would enable the auditor to decide on the methodology to be used for verifying the veracity of the evidence.

5. Identify Key Control Points

Based on the risk prioritization, the auditor looks for those control points that control maximum risks. This is not an easy task, since there are very many technical and functional factors to be understood before the key control points can be pinned down. The risks range from human error to error in programming logic as well as intentional fraud.

6. Identify Control Weaknesses

It is quite possible that the controls may be leaving the door open for some loss to occur. For example, checking whether the amount field is numeric and below 999999 in value does not eliminate the possibility of 89 being entered as 98. Take an example where a clerk raises a requisition and the officer approves it. The Officer may be loaded with other work, so he gives his/her password to the clerk and asks the clerk to enter and approve the transaction. The clerk not being so knowledgeable can commit serious mistakes. The system assumes that the approver has seen all aspects of the transaction before approval and accepts the same.

7. Verifying veracity of computer files

Let us take an example: in a Fertilizer company, the price of Sulphur has been erroneously taken as price of DAP. The error goes unnoticed because the hash total also was based on the wrong price. The error is detected when the MIS report reveals lopsided costs. The error is manually corrected on the cost sheet but the system still carries the error. In short, the auditor has to start with the user output that was corrected and come back to the computer files. The auditor should also look out for corrections directly made on the database without correcting the transaction files.

8. Conduct Audit Tests

An auditor may conclude that there is a possibility that the controls do not detect a certain type of problem. In such cases, the auditor calculates the correct result for a correct data and passes the same through the system. Computer programs may also be used for this purpose. The results are compared and conclusions drawn.

9. Concluding the Audit

The tasks involved in concluding the audit are:

(a) Develop the findings highlighting facts, against which standards the findings have been made and impact analysis.

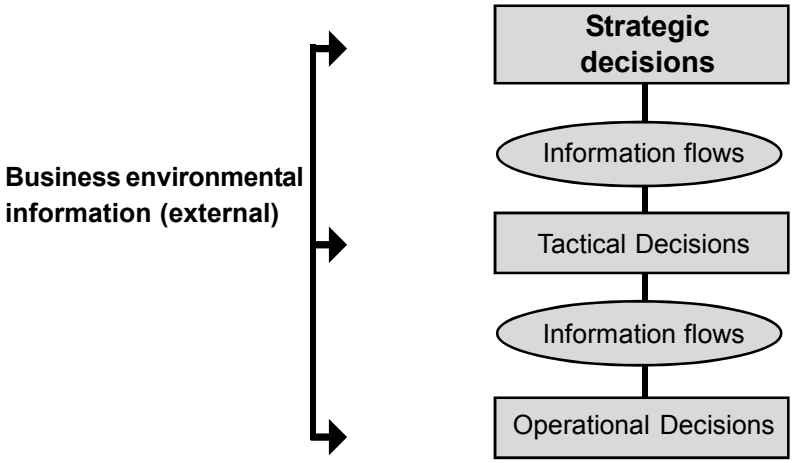
(b) Develop Audit Recommendations that would best mitigate the risks under existing circumstances.

(c) Write the Audit report highlighting the above.

The last step is to have a meeting with the Management representatives who have to implement the findings and record the action points for the next audit review.

SYSTEMS AUDIT & MANAGEMENT FUNCTIONS

If we look at the time-honored management pyramid,



We notice the major role information systems have to play in decision-making across the Management functions. Information systems usually focus inwards and are endoscopic in nature. Information gathering from the external business world is mostly manual or done through disjointed systems such as taking information out of the Internet, etc. The Strategic vision and direction are set based upon the top management's perception of opportunities. The information feedback from operations and operational decisions flow to help the middle management in its tactical management. The information flow from Tactical Decisions enable the Top Management to assess where the organization is, vis-à-vis its vision and strategic direction.

Systems Audit helps the management to be assured that its feedback loop is healthy and is not likely to miss out on vitally important details. Any deficiencies in the Information systems and in the creation, maintenance and usage of the information are pointed out by the systems audit function. In turn, this also reinforces the Stakeholders' faith in the basic management processes that are tracked by information flows.

All organizations suffer from fragmentation of knowledge across functions and across departments as well. Paretto's principle seems to apply well in that 20% of the people get to have 80% of the knowledge of their departmental/functional area. The challenge before all managements is, how to manage knowledge. Knowledge needs to be distributed instead of being hoarded, so that the activities of the company are at the optimal best.

In its primitive form, a Knowledge Management system today is a glorified form of document management system. The extent and granularity of indexing determine how closely relevant a piece of knowledge can be. Raw knowledge has to be validated to make sure that it is well supported by facts. Only then it can be used. Use of invalidated knowledge can be dangerous. Systems are evolving from information management to knowledge management. The traditional management function of planning, directing, coordinating, analyzing and staffing are deeply impacted by information and knowledge.

At a more mundane level, all functional managers need to cooperate with IS Audit so that the exposure of a weakness can be converted into a strength.

EFFECTS OF COMPUTERS ON AUDITING

When computer systems first appeared, many auditors were concerned that the fundamental nature of auditing might have to change to cope with the new technology. It is now clear this is not the case. Auditors must still provide a competent, independent evaluation as to whether a set of economic activities has been recorded and reported according to established standards or criteria.

Nevertheless, computer systems have affected how auditors carry out their two basic functions: evidence collection and evidence evaluation. We examine some of these changes in the following subsections.

Impact of Computers on Evidence Collection

Collecting evidence on the reliability of a computer system is often more complex than collecting evidence on the reliability of a manual system. Auditors confront a diverse and sometimes complex range of internal control technology that did not exist in manual systems. For example, accurate and complete operation of a disk drive requires a set of hardware controls not used in a manual system. Similarly, system development controls include procedures for testing programs that would not be found in the development of manual systems. Auditors must understand these controls if they are to be able to collect evidence competently on the reliability of the controls.

Unfortunately, understanding the control technology is not always easy. Hardware and software continue to evolve rapidly. Although some time lag occurs, the associated controls evolve rapidly also. For example, with increasing use of data communications for data transfer, substantial research continues to be undertaken on the development of cryptographic controls to protect the privacy of data. Auditors must keep up with these developments if they are to be able to evaluate the reliability of communications networks competently.

The continuing evolution of control technology also makes it more difficult for auditors to collect evidence on the reliability of controls. Indeed, in some cases auditors might be unable to collect audit evidence using manual

means. Thus, they need computer systems themselves if they are to be able to collect the necessary evidence. The development of generalized audit software occurred, for example, because auditors needed access to data maintained on magnetic media. Similarly, new audit tools might be required in due course if auditors are to be able to evaluate the reliability of controls in data communications networks competently. Unfortunately, the development of these audit tools usually lags the development of the technology that must be evaluated. In the meantime, auditors are often forced to compromise in some way when performing the evidence collection function.

Impact of Computers on Evidence Evaluation

Given the increased complexity of computer systems and internal control technology, it is also more difficult to evaluate the consequences of control strengths and weaknesses for the overall reliability of systems. First, auditors must understand when a control is acting reliably or malfunctioning. Next, they must be able to trace the consequences of the control strength or weakness through the system. In a shared data environment, for example, this task might be difficult. A single input transaction could update multiple data items that are used by diverse, physically disparate users. Somehow auditors must be able to trace the consequences of an error in the transaction input for all users.

In some ways, auditors are also under greater stress when they perform the evidence evaluation function for computer systems. As noted earlier, the consequences of errors in a computer system can be more serious than the consequences of errors in a manual system. Errors in manual systems tend to occur stochastically; for example, periodically a clerk prices an inventory item incorrectly. Errors in computer systems tend to be deterministic; for example, an erroneous program always will execute incorrectly. Moreover, errors are generated at high speed and the cost to correct and rerun programs can be high. Whereas fast feed-back can be provided to clerks if they make errors in computer programs can involve extensive redesign and reprogramming. Thus, internal controls that ensure that high-quality computer systems are designed, implemented, operated, and maintained are critical. The onus is on auditors to ensure that these controls are sufficient to maintain asset safeguarding, data integrity, system effectiveness, and system efficiency and that they are in place and working reliably.

SYSTEMS AUDIT OF COMPUTERIZED SECRETARIAL FUNCTIONS

The following describes the role of the CS and his/her functions:

> "A Company secretary is a person intended to ensure compliance of laws affecting the working of a company for formalizing the business transactions. S/he is, therefore required to possess specialized knowledge of the various corporate laws and rules made there under. Apart from the shareholders and directors, normally, the company communicates with the outside world through its company secretary. Broadly, a company secretary is required to work in a three-fold fashion. A Company Secretary –
>
> 1. is a vital link between the company and its Board of Directors, shareholders, government and regulatory authorities and all other stakeholders?
> 2. ensures that Board procedures are followed and regularly reviewed and provides guidance to Chairman and the Directors on their responsibilities under various laws.
> 3. Commands high position in the value chain and acts conscience seeker of the company.

A Company Secretary being multidisciplinary professional render services in varied areas. In actual practice it can be seen that the Company Secretary's functions require substantial summary information from all the existing systems. For instance, compliance with the laws of the land does not only involve compliance with the Company Law. There are also other legal aspects such as Labor Laws, Pollution Control laws, Industrial Safety, FEMA, MRTP, etc. Since the Company Secretary represents the Board of Directors, s/he has to have a wide angled view through information received from several systems – whether computerized or not.

System Audit of Computerised Secretarial Function

The procedure to be followed for performing a Systems Audit remains the same irrespective of functionality. The testing of application controls alone vary. Systems audit consists of evaluating the following:

- Management Controls
- Environmental Controls
- Organizational Controls and
- Application Controls

Now in the present era, most of the secretarial processes of a company are either computerised or handled by a specialized agency i.e. Depositories, STA etc. In this scenario, a company secretary has a wider role to play. To get an ease about the system operations, he verifies the presence of necessary control in the system and procedures.

For verifying the presence of necessary controls in the system and processes, first the auditor needs to review the system development methodology adopted. The Systems Development Methodology adopted in developing the system and processes for Secretarial function would have to be verified for the following:

1. Are the best practices being followed for the development of the program and whether the Librarian is having records for the various versions of the program? For example, we need to verify the version number of the Dividend Warrant preparation program. The purpose of verifying the version number is to ensure that in a live environment only the correct latest version of the program is used. Also verifying the procedures for Change Management will assure us that change to programs are made only under the specific authorization of the user endorsed by appropriate authority within the Computer Department.
2. Verifying the procedures becomes all the more important if Dividend Warrant processing is given to third parties.
3. The control practices followed by the third party Service Provider should be verified. Having verified the Management Controls, Environmental Controls and Organizational Controls, the further steps to be followed for performing the Systems Audit of dividend preparation applications would be the following:

Verification of Input Controls

After verifying the system development methodology, the secretarial audit should verify the input controls in the systems and procedures developed for computerized secretarial function.

The input will consist of the details of the various shareholders. The Master Data would contain the name, address, nominee, or joint account holding details, as also income-tax status. Before the Dividend Warrant application program could be run in a live environment the steps that would be taken would be to ensure all master records have been corrected, upto and including Share Transfers as approved by the last Share Transfer Meeting, and also all correspondence received regarding change of address, income-tax status etc.

The first and initial input control would be to run the data file of the shareholders and obtain the total of the shareholding to ensure that it is equal to the subscribed share capital. An error at this stage would indicate that some wrong corrections have been made to the Master Data like the transferee details would have been included and the transferors details might not have been deleted or when a transferor has effected a part transfer, suitable corrections might not have been effected.

Generally, every time after the Share transfer Meeting, the Master file of the Shareholders would be modified to take into account the latest changes in shareholdings. General practice that could be followed would be that at every point of time it would be ensured that the Master File contains the correct total figure of shareholdings. When modifications have to be made because of the authorized share transfers, there would be a separate

verification program to ensure that the number of shares transferred by the transferors is equal to the number of shares transferred to the transferees. So, when performing the Systems Audit, one must verify these records to ensure whether all these procedures have been followed. It is not uncommon to hear of stray incidents when transferor and transferee might have received dividend warrants or the transferor receiving the dividend warrant and not the transferee! In those circumstances, while the computer is conveniently blamed, the real culprits are the individuals who are not following the procedures correctly. In a manual environment, before the procedure of computing dividend warrants is commenced, it is manually ensured that all of the transfers as per the list as authorized by the Directors have been correctly posted. The same procedure needs to be verified in a computerized environment. As we would not be verifying the manual posting, a computer program is run to ensure the integrity of the Master file of the shareholders.

Providing Parameters

The program needs to be provided with certain parameter details like percentage of dividend being declared, income-tax to be deducted for the various types of Shareholders, e.g. Corporate Body, Non-Resident individuals, individuals.

Checking Exemption from Tax Deducted at Source (Form 15-H)

In cases like individuals not being liable to tax, whether Form 15-H has been provided and the fact that it is provided is correctly entered in the machine. For this purpose, the computer listing of all of the cases where Form 15-H is purportedly have been provided should be printed out and this list should be physically verified with a hard copy of the 15-H forms. This would ensure two things.

1. The individuals, who would have had to pay tax, would have tax deducted.
2. Only those who have provided Form 15-H would be enjoying the privilege of not having the tax deducted.

If this verification is not done, it is not unusual to find the computer doing the tax deductions wrongly (Note – The procedure of tax on Dividend would be changing with each budget and hence care should be taken to see that the procedure that is being followed is in line with the latest Finance Act)

Verifying the above ensures that input is correct as far as the

(a) Shareholding is concerned;

(b) Names and addresses; and

(c) Tax status

The application program/preparation of Dividend Warrants should be tested for these purposes.

USE OF TEST PACK

The use of test packs is the application of auditors test data (live or dummy) to client's application programs. A small sample of data is processed through the computer and output is compared with manually generated output using the same data. This audit approach requires little computer expertise but designing of test data which will represent all the possible combinations is a time consuming and difficult process. Use of test data generators can overcome this disadvantage.

The Systems Auditor should request for the appropriate computer program to be loaded on a separate computer. He should prepare an exhaustive Test Pack. The Test Pack will consist of a comprehensive data so that the logic of the program is extensively checked.

Illustrative Test Pack

Shareholder	Shares held	Income Tax Status
No 1	nil	Individual
No 2	500	No income-tax status
No 3	1,000	Individual taxable
No 4	1,000	Non-Resident Indian
No 5	10,000	Indian Company
No 6	10,000	Foreign Company

The contents of the Test pack are left to the imagination and innovativeness of the Systems Auditor. The Test Pack would have to be developed in such a way that all of the possibilities envisaged in the Program logic would be tested. As a matter of fact, the program should even be tested for negative holding. The program should be expected to come out with error messages whenever there are apparent or otherwise mistakes in the data or values. For example,

1. There should be no shareholder who has got nil shares.
2. A shareholder is a minor.
3. A shareholder has negative value of shares (say-10).
4. Total Number of shareholders under each of the categories does not tally with the control total for the respective category.

If a shareholder has got negative holding, it means more shares than what he holds, have been transferred wrongly. These sort of mistakes will not arise normally in a manual environment as the individual is looking at the data and applying his mind for its correctness or otherwise. In a computerized environment, the processes become mechanical and hence the program has to provide for the type of checking which we would do if the system were manual.

Hence, while creating the test pack, we should bear in mind that it should not only be illustrative, but also comprehensive and exhaustive.

The program would now need to be tested. The computer, which has got a copy of the program loaded, would need to be utilized for loading this Test Data. The loading of Test data is done by creating a file of shareholders as envisaged in the Test Pack. After loading of the Test Pack, the necessary commands for commencing the processing should be given (this procedure can easily be picked up by discussing with the regular users of the Computer). Once the program commences processing, it would be processing one record at a time, as each of the records (details of the shareholder) would need to be verified for its correctness and completeness. If the first record in the Test Data is processed, the computer should come out with an error message to say “No Shareholding”.

1. For the second record, the message should say “minor but no guardian”
2. The Shareholder has no valid income-tax status.
3. The shareholding is negative
4. Control totals do not tally – Control total*.

Note: The contents of the error messages would also require to be fed into the program so that appropriate message as programmed would be picked up.

If for any reason, the results are not in line with the results as expected if the program were to function properly, we need to perform the following steps.

1. Ensure the Test Data has been entered into the Machine correctly. (This can be done by taking out a print out of the test pack and compare it with what was envisaged to be fed into the computer).
2. Note down the type of malfunctioning of the computer Program, for example, if record number 1 is processed without giving an error message, the program is not testing for nil balance of the shareholder, i.e. the Master file contains details of Shareholders who have ceased to be shareholders as they have sold out all their holdings.

At the end of the testing of the program and after evaluating the results, the Systems Auditor is able to conclude as to what types of "bugs" are in the program. Bugs, as we know are mistakes in the program. For instance, the list of bugs, which would have been discovered by using the above Test Pack, could be:

– The program does not check for "Nil" holding.

– Existence of Income tax status is not being verified.

– The holding of shares by a member is not being verified to ensure that it is positive.

– There is no built in control to verify the integrity of the file. If totals are not built and verified, if data is unreliable, it will go unchecked.

The auditor should discuss this with the User Department. If the Secretarial Department itself is performing the System Audit, it should discuss it with the developers of the program. Till such time as the program bugs are removed, that version of the program cannot be used, as it is not bug free. It is at this juncture that the Secretarial Department would inform the Computer Department of the corrections to be effected and after correcting the program, the new version of the program would be created and the Librarian will take note of it. The Systems Auditor in the meantime would be preparing a report.

NORMS AND PROCEDURES FOR COMPUTERIZATION

Systems are developed to meet the organization's business objectives. Application systems should be developed and implemented to ensure organization's business objectives. The systems may be developed in-house or acquired from outside.

Whether developed in-house or bought out from third parties as readymade packages it is an accepted fact that the user needs would change and so the systems would need to be modified. It is essential that from the point of ensuring that the systems are reliable, well-accepted best practices should be followed for systems development. Whether bought from a third party or developed in house, the change procedures should conform to expected best practices. This alone would ensure that software is not only developed properly but also maintained well thereafter. A need for a new system to be developed may arise under any one of the following conditions:

(i) A new opportunity relating to an existing business process.

(ii) A problem which relates to an actual business process.

(iii) A new technology that will enable an organization to take advantage of the technological developments.

(iv) A problem associated with the technology currently in house.

More common applications that could be envisaged from the company secretary's point of view could be

(a) Fixed Deposit System

(c) Preparation of dividend warrants/interest warrants

(d) Fresh issue of capital

(e) Issue of bonus shares.

If as a Company Secretary we are associated with a mutual fund company or as a Company Secretary in practice, we have to verify the processing procedures to ensure that all regulatory procedures are complied with. The following process would have to be considered:

A company acting as a registrar for a mutual fund is entirely relied upon for information in connection with opening balance of investments, purchases less sales to arrive at the closing balance and thus declare the net asset value at the end of the day. While the above list is only illustrative, we need to understand that the areas where computers could be utilized is only dependent on the capabilities of the concerned management to utilize the technology. The major components in software development are as follows:

(i) Feasibility study

(ii) Requirements definition

(iii) If developed in-house, development, programming, alpha testing

(iv) If readymade package is acquired, acquisition of software and modification thereafter.

(v) Beta testing, approval, implementation and post implementation.

1. Feasibility study

The feasibility study would consider the technical feasibility as also the financial feasibility. The factors, which would be considered while performing a feasibility study, would be

(a) Decide whether computerization is desired

(b) Decide if an existing system can be modified or improved upon

(c) The time frame which is required of a new system is developed

(d) Determine the associated costs.

Considering the above-mentioned factors weighing the advantages and disadvantages and considering whether the proposed system would really meet the objectives, a decision would be taken.

The factors which would be considered for taking a decision as to whether a system should be developed in house or bought as a readymade package would be

(a) Cost – buying versus cost of developing

(b) Time factor

(c) Resources required by way of availability of staff and their capability to develop a new system

(d) If a package is bought from an outsider, whether it can be used as a test or whether any customization i.e. changes to be made to meet the requirements of the organization will required to be made should be considered.

(e) If purchased from a third party, the source code would not be provided. The source code is the original programming code used while developing a program. Any time a program has to be changed source code will require to be modified. If the source code is not available it would be impossible to modify a program. The vendors would be providing only an executable program i.e. a program code created by a compilation process of the source code. An executable program (also called object code) cannot be altered.

If a readymade program is being purchased from the outsider, it should be robust and have a good proven record and the vendors should have financial stability, has to be in business and continue to exist to provide maintenance assistance for the software packages to be maintained.

2. Requirements Definition

The user groups should clearly specify the business requirements. For example the secretarial department should explain clearly their expectations regarding the functionality of the proposed system. If it were a share application system, the requirements would broadly cover the following aspects:

There would be a master data of existing shareholders with their names and addresses and shareholding would need to be created. Subsequently, share transfers would require to be effected between existing members or between existing members and new members who are acquiring the shares. The system has to provide for members selling part of their holding. The master data should have details regarding not only the income tax status of resident, non-resident, etc. but also their liability to income tax.

After every transfer of shares meeting, the following facts should be verified:

(a) Whether the numbers of shares transferred by the transferor is equal to the number of shares acquired by the transferees?

(b) Total of share holding should be obtained after the transfer to ensure that there is no alteration to the total issued share capital.

(c) It may be necessary to file a number of returns to the regulatory bodies like the Company Law Department, Income tax Department etc. When it is proposed to computerize share accounting of all the above would be mentioned as requirements definition at the minimum level.

As a matter of fact, the details which would be required to be provided would be far more in as much as the details would have to be provided as to the likely shareholder number, folio number, name of the shareholder, address and other details like husband's name, father's name, guardian in case of minor etc. Apart from those details, the user should specify access controls and management information needs. Access controls should specifically mention what restrictions should be placed, on what information and who needs to be authorized to access what information. In a manual environment, the shareholders register is under the secured control of the senior officer as also the share certificates. So when a system is being computerized, a Company Secretary or a senior officer of the Company Secretary's department should specify the requirements for the controls that are necessary so that when the system is developed, the adequate and appropriate controls will be built into the system to the extent possible and where not possible compensating controls would be envisaged and recommended.

If these controls are not implemented situations like share capital not tallying, transferor continuing to be a shareholder in the book even after transfer has been effected or the transferee acquiring more shares than he paid for etc. would arise.

3. Software Acquisition

After requirements definition has been provided the next phase will be to consider whether the system needs to be developed in house or a readymade system being supplied by a third party could be used.

It is not uncommon to find readymade packages being utilized, as the major factors in the functionality of share capital are more or less similar.

The requirements as defined in the earlier phase would be provided to various vendors of software packages. A decision would be taken from the proposals made by the different vendors taking into consideration the following factors:

(i) Are the vendors reliable?

(ii) Who are their current customers and what is the feed back from them?

(iii) What is the financial position of the vendor?

(iv) Is he well established and likely to continue to be in business so that he should be relied upon for any modifications to the existing systems to customize to their requirements and also be in a position to maintain the software in the future and such a need arise.

Once a decision is taken to acquire a software package from a third party and after negotiations have been completed regarding the price and service levels a formal contract needs to be entered into. The contract should broadly cover the following aspects:

Specific descriptions of deliverables i.e. what would be the various outputs from the system?

What would be the cost?

What would be the data at which the deliverables would be available?

What would be the kind of support that would be provided while the system is being installed?

Make it very clear that the contract should be final only after users have performed acceptance testing and given a clearance regarding the functionality as also the controls. To what extent can changes be made?

What would be the documentation standards expected for changes to be made?

What would be the documentation support provided by the vendor?

The further phases when system is to be developed in-house after requirements definition are as under:-

(a) Detailed design

(b) Programming

(c) Debugging the programming

(d) Testing the programs

(e) Implementation and

(f) Post-implementation.

4. Detailed design of System

Based on the user specifications as mentioned in the requirements definition phase, the system personnel would develop a detailed design. At this stage, screen designs would be presented. Systems flow charts would be developed. This would provide details as to how information will flow through the system. This would also include details of converting data from a manual system or from an existing computerized system. There would be interactions with the users to ensure that user requirements and systems deliverables match. A system will consist of several modules. For example a shares system may consist of the following modules:

Master creation module

Transfer registration module

Dividend warrant preparation module

Modules for preparing various statements in connection with regulatory requirements

Modules for providing management information system.

5. Programming

Programming is the process of giving instructions to the computer so that from the given input required output will be obtained. The process of writing the program is called coding. Individuals who get trained in programming would be assigned the job of doing the coding.

There are certain programming standards to be followed. The rationale for programming standards to be followed is that it is not dependent on any one individual who did the original coding to explain the basis. Once the standards are adhered to, any trained programmer would be able to understand how the program has been written. Main problem area in programming is that documentation standards are not adhered to and as a matter of fact, documentation may be totally absent also. The emphasis from the systems and programmers angle is to get the system going. Also it is not uncommon to find users and management pressuring the systems development team to develop a system and make it go live with an unreasonably short time span. Whatever be the reason, it is not uncommon to find documentation standards being given the go by. Minimum documentation standards should be adhered to. Lack of documentation is sometimes attributed to the fact that the staff turnover is high. But from the point of view of adhering to best practices the reason that it is likely that there would be a staff turnover should be a deciding factor for maintaining good standards of documentation.

6. Debugging a Program

Programs are written with the objective of giving instructions to the computer so that from the given input required output would be obtained. However, instructions to the computer may not be conveyed properly. In such circumstances, the program would be defective and technically it is called that the programs has got “bugs” i.e. defects. It is the responsibility of the programmer to ensure that these defects or bugs are removed and the instructions are conveyed properly. This process of removing the bugs is called debugging. It is the responsibility of the programmer to debug the programs he has written. He should ensure that the functionality of a program is in order and also that the built in controls function as expected. There are various methods of debugging a program. By adopting these methods, a programmer would be able to locate the errors he has committed. He would rectify the error and test the program again and again till such time the program functioning is as expected. The process of debugging a program is also called the testing of a program. For testing a program, an illustrative but exhaustive test data would be created i.e. a set of dummy data would be created so that all the logical paths in the program would be tested. Effectiveness of testing a program is very much dependent in creating an exhaustive test data. There are various types of testing. The programmers perform some tests. Some performed by the system analysts, some by the users. We discuss below a few of the types of the tests and also as to who does it and when.

Pilot testing: This is a preliminary test and it has a limited evaluation of the system. The programmer generally performs this.

Unit testing: This test is performed on individual modules of a program. This would not only verify the functionality but also the controls structure. A successful unit test would ensure that the internal operation of the program is in line with the specification provided.

Interface testing: In the individual module, this is only a part of the total system and so it is necessary that after all of the individual testing of the modules are over all of them should be tested together to ensure that the interfacing between them is as per expectations.

System testing: A systems analyst who has higher responsibility than a programmer generally performs this. Systems analyst has to ensure that the system as a whole would work properly. In this process he would verify

(a) Systems ability to recover after a software or hardware failure

(b) Systems ability to process high volumes expected during peak times.

7. Regression Testing

This is an important test to be performed any time a program has been modified. When business needs change or the systems department decides to make a change to improve the performance of the program the existing system would require to be modified. However, in this connection, it must be ensured that the performance of the existing system is not in any manner affected due to the changes being incorporated subsequent to the system having been originally tested and found to be in order.

When a modification is effected, first it will be ensured to see whether the modification has been incorporated in the program so that the changed program caters to the changed condition subsequently incorporated. At the same time, it should be ensured that the balance of the system and programs should not be affected either in the functionality or controls. To achieve this objective, a comprehensive test of the system would be taken to verify whether the modification effected works properly and it has had no adverse impact on the already proved system. The existing system should continue to perform properly and only take on the modifications. Regression testing is a test methodology by which this is ensured. It is necessary that any time a change is effected regression testing should, without fail, be performed.

8. Parallel Testing

The system team also performs the parallel testing. The system is tested and a copy of the live data e.g. share transfers effected during the last 6 months, the results of the share transfers are already available in the live environment as either a manual system or another computer system is in existence. When the same data is fed into the new system, the results obtained should be compared to ensure accuracy. As the same data is run on two systems one new and another existing, it is called parallel testing.

9. Acceptance Testing

The systems personnel after having satisfied themselves that the new system will meet the requirements of the user, the system would be handed over to the user for their testing. This test is called acceptance testing and as its name indicates this is a test conducted before actually accepting the system. As the system has to be accepted by the user, the user and not the systems developer perform acceptance testing. The user would test the system for whatever condition he would like to and satisfy that the functionality is as expected and that the expected controls are also effective within the system. After the user is satisfied that the system given to them by the systems personnel is acceptable to them, they convey the same by means of "User sign off". User Sign off is an acceptance by the end user. Only after obtaining the user sign off the system that would be with the developers is deemed to be ready for implementation. The systems would all along have been in an environment, which is called a test environment. The user departments' environment is called a live environment or production environment. After successful acceptance testing, the system would migrate from the test environment to the production environment

10. Implementation

Upon successful completion of testing, the program is converted into an executable mode in the computer department and only the copy of the executable program is transferred to the production environment. The corresponding source code would be/should be maintained safely in the computer department, with the Librarian.

11. Post implementation review

After successful implementation of the new system, it is recommended that the system is verified to ensure the correctness of the design, appropriate test of the controls and generally the other objectives of the system. At the post implementation review, the following features would be assessed:

- Does the system meet user requirements?
- Have access controls been properly implemented?

On completion of the assessment any observation regarding inadequacies, deficiencies and plan for implementing this should be recorded. This should be conveyed by the manager of the user department to the manager of the IT department or through a Steering Committee so that necessary steps could be taken to implement changes. Developing a system, making changes wherever necessary, developing it again and again making request for changes has a iterative process. It is important that whether it is original development or a modification all of the best practices to be followed in the various phases should be strictly adhered. The phases also should be sequentially followed even in the case of change management.

CHANGE MANAGEMENT

The most important aspect of software lifecycle is change. Change has several dimensions:

- Changes can be driven by external factors over which the organization has no control: for example, when SEBI or Company Law authorities bring about a change in disclosure formats or manner of accounting, the organization has no choice but to adopt the changed method of functioning.
- Changes can be driven by internal factors: for example, after the recent incidents involving Tata Finance, the company has resorted to tightening of internal controls.

There is an important angle involved in managing change – the human angle. A change involves a different way of working. There is a general resistance to change. Taking ownership for change is again a major issue with many Indian companies. Change also involves many departments – thus requiring coordination and ensuring unified approach. The speed of change is another matter.

The foregoing goes to show that there needs to be a formal process for making changes, particularly to information systems. We have seen how rigorous the SDLC process needs to be from the perspective of Systems Audit.

We know that some of the business rules will change every year. For example, Income Tax, Corporate Tax, Excise Duty laws, Sales tax laws and other laws pertaining to other levies such as Octroi, etc., change with each budget in the Central Government and several State Governments. Sometimes, the incorporation of new rules necessitates altering the structure of the database tables and the associated programs.

The following questions crop up:

1. Is the new requirement fully understood? Who are all to be involved and whose views should be finally to be taken as that of the "final authority"?
2. Has it been studied from various angles such as Accounting, legal compliances, implementability, implications, etc.? Has the final authority taken a total view and decided on the course of action?
3. The System developers need to be given accurate specifications of the new requirements: who will do it?
4. Controls have to be built in to ensure that the processing is complete, correct and accurate. Who will check it and how?
5. If the changes are temporary (such as the "Earthquake Surcharge" on Income Tax valid for one year) they have to be rolled back. Is the System Development team taking care of this? How will this be ensured?
6. At some point of time the system may become so altered with changes that it might no longer be efficient, or, running the software may be risky in the sense that it could terminate abnormally and destroy data. Is there a process to judge the health of the systems and take specific maintenance action?

It needs to be understood that the Computerized Applications, with their underlying hardware, networking elements, Operating System, Database and Application programs are the joint intellectual property of the Management, the user departments and IT Department. Each of the entities mentioned above has contributed to the existence of the Application for a specific business purpose. The concerned entities depend upon the Application for carrying out their tasks. It should therefore be protected from accidental or intentional tampering that can seriously affect the corporate interests.

Organizations need to have proper change management processes in place. The framework consists of:

1. Setting up a change control authority in the organization with a constitution that can do justice to the subject

2. Setting up Change Initiation, Change Review and Change Authorization mechanism
3. Setting up change implementation process
4. Setting up a Documentation Standard that permits complete and correct capture of the proceedings of the entire change management process
5. Setting up Technology renewal process.

Let us address these one-by-ones.

1. Change Control Authority

An Organization may have several Application Systems & subsystems. These systems are interrelated. For example, a new plant may be set up on the Production floor. It has been set up to augment production. It uses the same raw materials such as the existing plant. The finished product may be the same or varying in specific technical details. The Materials Manager wants to keep track of the indents plantwise. Since the vendor is not interested in knowing which plant he is supplying to, so far as the material is the same, the Purchase Order is consolidated for both plants. Let us say that both the plants have separate stores attached to themselves. The material is to be delivered to the plants as specified. Each plant will carry out its Inward Quality Check (IQC) and take into stock the material that passes the IQC. Let us stop at this stage and note the change – earlier it was one plant, one store. Now there are two plants, each with its own head. For control reasons, breakup is required as stated above and this requirement is emanating from the Materials Manager. The obvious question that arises is, what are the financial implications? First of all, is the procedure correct? Is the change really required? Cannot one store and one purchase section handle the needs of both plants? The affected departments are Purchase, Stores, Finance & IT, which has to carry out the change. The Top Management would like the affected users – who also have the requisite domain knowledge and competence to go into the issues involved – to arrive at a joint solution to the problem. The onset of change always results in creating some extra tasks, those who have to carry out these extra tasks may either want extra resources, or may not want to take on the extra load. This is where a decision is to be taken and the change implemented.

It is therefore prudent to constitute a Change Control Board consisting of Heads of Functions headed by a Functional Director as the chairperson. Internal Audit should also be a member of the Change Control Board to deliberate on the control and security issues involved. The change initiation takes place when a detailed written request is raised by an affected entity. Let us say that in the above example, the Purchase Supervisor was the one to feel the need for change. The document comes to the Materials head for review. He has to consult the Stores Supervisor and Accounts Department also. After thrashing out the first level issues, the request is firmed up and sent to the coordinator of the Change Control Board. Here the change request is reviewed in all its aspects. Some of the points may be agreed to, some may not be agreed to. There may be some fundamental unsolved problems that might arise in the deliberations. At this stage, the request may be routed to a task force consisting of internal or external experts. The change request is also commented upon by the IT Department, as they may require extra resources to implement the change.

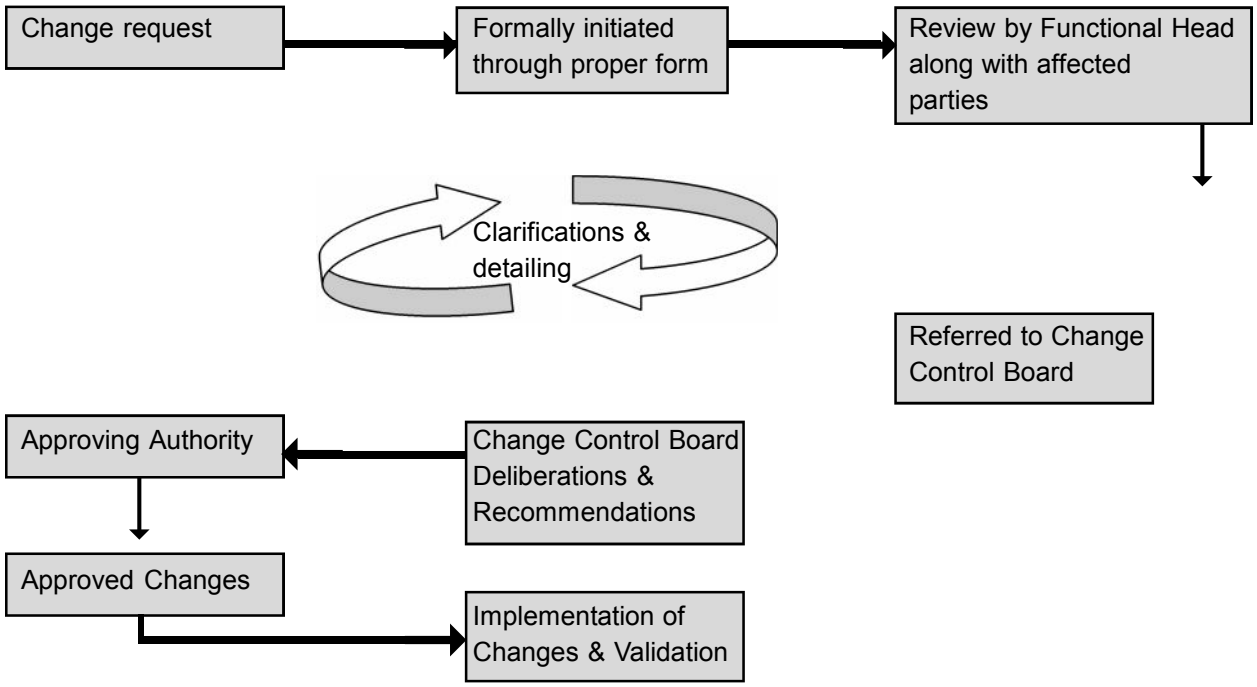
The functional director heading the Change Control Board then puts up the change request as approved, to the Top Management team headed by the CMD if the change is a major one.

Let us say that an organization was having a legacy system that was developed in-house. In course of time the system became obsolete, as several pieces of the system got deactivated and replaced with manual working. At this stage, all users are dissatisfied and want to go in, for, say, an ERP package. This is a major decision impacting the entire organization. The cost implications might necessitate a Board level decision. This is an example where the decision cannot be taken within the ambits of the Change Control Board.

The IS Auditor needs to look into the entire change control process. Otherwise the rigor with which the system was introduced can be diluted and the control aspects rendered ineffective.

2. Change Initiation, Change Review & Change Authorization mechanism

The change control process is shown diagrammatically below:



It is to be noted that upon approval the change control board is intimated by the approving authority, which passes back to the initiator through the Functional Head. The details of Approved Changes are given to the IT Department along with copies to affected departments for implementation.

3. The Change Implementation Process

The implementation process has to be initiated with a Project Plan. For better ownership and involvement, it is desirable that the Project manager role should be assumed by the Initiating Functional Manager, working closely with the CIO (head of IT) and other Departments. The project plan has to be in detail, with roles, responsibilities, tasks, task durations, interdependencies and work-arounds in case the existing system needs to be brought down for some time. It should also address issues of whether the change would be carried out in-house or outsourced. Internal Audit & IS Audit have to be involved in ensuring that the system controls are foolproof and the changes are thoroughly tested before rolling out. There also needs to be a mechanism for troubleshooting. This is because, despite the best of care, computer systems can have bugs and they have to be properly tracked and eliminated. The recommended testing methodology needs to be rigorously followed. If necessary, users have to be retrained in the use of the Application. When the users are spread over multiple locations, it becomes necessary to plan training and rollouts appropriately.

DOCUMENTATION STANDARDS

Every Organization needs to evolve its own Documentation Standards for the various types of documents. Textbooks on Software Engineering are replete with various templates for Standards. While a rigorous and elaborate treatment may be really necessary for software houses producing highly complicated and integrated software, user organizations also need to document their systems so that compliance with requirements and controls may be maintained.

In the absence of documentation, knowledge of the System and software remain in the minds of some individuals.

In the event of attrition, their knowledge goes away with them. It is therefore necessary to capture this knowledge in a written-down form.

The first standard an Organization needs is a standard for Documentation. This standard stipulates the getup, layout, font, pagination, style, paragraph numbering and indentation, etc. All documents follow the style and template of the Document Standard.

The next important document is the Functional Requirements Specification Document that lays down the Business functionality required. This document does not address itself to any hardware/software platform but merely describes Inputs, Processes & Outputs required in various functional areas.

The Functional Requirements have to be translated into a Software Framework. For this purpose, an analysis is carried out and interrelationship between different functional areas is defined in terms of information flows. At this stage, details of multi-location operations, volumes, frequencies and duration for keeping online records (such as last three years financial data, etc.) are noted. In a sense the Software Requirements Specification (SRS) implicitly assumes a design framework but this is restricted to interfaces only.

Although decision on the platform, etc. can be correctly taken after Design Phase, it needs to be remembered that there is a lead time of 4-6 weeks in getting the hardware and system software. For this reason, from the type of requirements, a platform is generically decided and the SRS developed assuming this backdrop. In case one is selecting a packaged application, then the choice of platform becomes automatically one in which the package runs best.

The Design Phase, in which the "How" aspect of the system is fleshed out, carries all the important factors on which the System foundation would rest. The Software Design Description document records these points under the heads of Inputs, Processes & Outputs. Where Object Orientation is used, this is the document that describes the Object Hierarchy and interrelationship. This document must be updated with every change and so should the SRS document be.

The Program code follows the detailed Design Description that goes to the level of specifying programming logic. There are standards for coding in the various languages. These standards are based on easy readability, understandability and efficiency of the code. Conventions are adopted for giving names to variables, indenting conditional statements and writing comment lines which will be of use to a programmer reading the code and which will be ignored by the computer.

There are also standards for Software Testing and documenting test plans and results. It will be out of place to get into further details. But the IS Auditor needs to look at documents such as the IEEE Standards and Guidelines for Software Engineering and get familiar with the standards. S/he then needs to compare the in-house documentation with the standards and comment upon the completeness, clarity and veracity of the documents.

It is very important to check whether the change in documentation is done every time a change is implemented in the system. Absence of documentation and rigorous testing should not be accepted.

Technology Renewal

An important aspect is that there is a high rate of obsolescence in IT. The Change Control Board also needs to concern itself with issues of Technology Renewal. Because of the depth of technology knowledge required, many Managements do not appreciate the warnings sounded by the IT Department. In non-IT organizations, it is common to have a junior manager heading IT. S/he in turn, reports to some functional manager such as Chief of Finance, Chief of Production, etc. The Head of IT has a lot of convincing to do before the organization wakes up to the reality of technology obsolescence. An IS Auditor needs to be vary of this aspect. One should keep abreast of the technology currency and comment upon the need to eliminate obsolescence if any.

COMPUTERS, CONTROLS & SECURITY

With increasing dependence on computers, the risk of breach of System security is also increasing. The rising stakes often tempt people to defraud organizations and get away with criminal gains.

If there is no control on printing of Dividend Warrants in the system, an investor could walk away with multiple dividends for the same amount invested. A vendor could get away with multiple payments for goods delivered once. Customer dues can be conveniently whitewashed. Insiders in collusion with external elements perpetrate most of the frauds and share the spoils.

The first principle of control lies in controlling access to the computer system. Nobody should be allowed direct access to the servers other than authorized administrators. Access to the server room can be controlled through swipe-card, fingerprint and other biometric devices. In sensitive data centers, there are movement-sensing cameras that constantly carry out surveillance. Security officers watch the displays in each zone and act when suspicious activity occurs. The key areas are network control area, server bay, power supply, air-conditioning and security control room. Each zone has remote-lockable doors acting as “man-traps”. An intruder can be restrained in the forbidden zone till security officers can nab the person. Modern data centers are also built with flood-proofing, fireproofing and earthquake-proofing measures to ensure that even accidentally through acts of God, the crucial systems are unaffected.

Logical access should be limited to the role played by the user. For example, a data entry clerk need not have access to the Payroll Database. S/he needs only a Read-Write-Update access to the raw data files that can be tracked to the operator. An Accounts clerk need not have access to production data logs.

In order to ensure that the access rights are properly followed, we have the system of passwords. The System Administrator assigns access rights to the users as required by their work. The user protects his/her access through passwords. Ideally, passwords should be minimum 12 characters long, having a combination of letters and numerical digits. Where permitted one can use special characters also. There are cases where users cannot remember their passwords. So they write the password on Post its and paste the same on their machines. Or else they use easy to guess words such as their own names or name of wife/child/pet. Such words are usually small and can easily be broken into.

The computer system remembers our passwords by storing them in internal, encrypted files. An expert cracker can retrieve the password if the Operating System has not been set up for the highest security levels.

For example, let us say that a security breach occurs in Microsoft Windows 2000 Operating System. This is reported to Microsoft and they issue an immediate “hotfix” or patch to the OS software that prevents the security hole from being misused. Later on, Microsoft collects similar corrections and bug fixes into a “Service Pack”. Details of such Hotfixes and Service Packs are available in Microsoft’s web site. Users can download such patches and correct their OS. Similarly there are other resources for correcting Unix bugs. When such patches are applied and the recommended security steps are taken care of at the time of the operating system installation, we say that the OS has been “hardened”.

Another class of insecurity comes in through Viruses. Computer Viruses are malicious programs capable of replicating themselves and destroy data or annoy users with meaningless messages. There are malicious codes known as Trojans that can seep into the system through electronic mail attachments. They can remain in the server and copy critical and secret information such as email addresses of others, passwords, credit card numbers, etc. and transmit the information to their creators. In turn the creators can indulge in frauds or cause trouble by changing the password, etc.

Internet web sites are attacked by different methods. The Denial–of-Service (DoS) attacks essentially flood the web server by sending thousands of high priority system messages. The server is rendered too busy responding to such spurious messages than attending to productive work.

In "spoofing" attacks, the user is deluded to get into some unwanted site by overriding the Domain Name Service entries. It needs to be remembered that information travels in packets that have the destination IP address. All computers in the network receive all the packets though they respond only to packets destined for them. A hacker or cracker can use this information to recraft the information content in the packet.

Modern information systems are used to connect external agencies such as service providers, customers and suppliers to the internal network through the medium of Internet. This is where the major risk lies.

Networks are protected from attackers by using:

- Appliances or software called "Firewalls" which restrict entry to outsiders based on security policy.
- Content Inspection & Intrusion Detection Systems, which monitor incoming packets and look for known or suspicious attack patterns. When they encounter suspicious code, they block the packets containing the same and thus protect the server.
- Antivirus software that is kept up-to-date with latest viral identities so that infected files can be identified and quarantined if not cured.

Organizations require security experts to keep a constant watch on network security as attack patterns are dynamically changing. Recent studies by the FBI have shown that most of frauds and damages have been done with insider collusion. Hence one needs to watch activities within and without.

Security of Information in transit over the network is taken care of by encryption, secure tunnels and tracking.

Encryption basically consists of transforming the information from an intelligible form to a non-intelligible form while sending. While receiving, the received information is transformed back to the original form. Modern encryption uses a pair of keys, one called "public" which is downloaded to the sender on initiation of the session. The sender's machine uses a mathematical algorithm to encrypt the information. This encrypted information can only be decrypted with the "private" key, which the receiver has, on his/her machine. Thus even if a cracker traps the information, s/he cannot decrypt it. It is no use trying to decrypt by permutation because not even the fastest of computers can crack the encryption in years of continuous working!

Secure tunnels are established by a combination of encryption and authentication by a special signature. Tracking tools are available to monitor the entire path taken by the transmitted information. In the event of suspicious activity, the offending machine can be identified and reported.

A major concern in carrying out commercial activities over the Internet or any public network is "repudiation". For instance, a person A buys some goods online and feeds his/her credit card number. When the card company presents the bill, A can refute it, saying that the purchase was not ordered by him/her and that it is the case of misuse. Modern technology offers methods by which the sender can be uniquely identified and it can be established that the order was, indeed, placed by A. This is known as "non-repudiation".

Computer Security is a very technical and complex subject. An IS Auditor needs to be aware of the type of attacks. S/he should know the various risks and consequences. S/he should verify whether there is a security policy in the organization and whether there is a mechanism to keep it up-to-date.

The IS Auditor should also verify whether passwords are being properly constructed and kept safe. The Systems Administrator should be aware of the security risks and their mitigation. This is what can be commented upon by the IS Auditor if s/he sees a gap.

DOCUMENTATION STANDARDS, POLICIES, PROCEDURES AND AUDIT APPROACH

Documentation of the system

Systems documentation normally takes the form of narrative descriptions, flowcharts or a combination of the two.

Narrative Descriptions

A narrative description helps to give a complete picture of the system. It provides a detailed record of the system under audit and, taken together with other forms of system records, it should cover:

1. System objectives and targets;
2. Links and interfaces with other systems;
3. The environment in which the system operates;
4. The allocation of authority and responsibility;
5. All key controls and systems processes;
6. Exceptional situations or cases that may need to be dealt with by the system;
7. Ad hoc controls such as management reviews.

Narratives may cover detailed descriptions of transaction flows but in some cases these can be better recorded through flowcharts. It is often useful to use a combination of narratives and flowcharts – using flowcharts to describe more complex parts of the system. If flowcharts are used as well they and the narrative descriptions should be cross-referenced to each other.

Narrative descriptions may be usefully divided into:

– A summary overview of the system; and

– Separate detailed descriptions of the main constituent parts of the system.

Full use should be made of headings and they should be organised in a logical way in order to give a clear picture and make handling and updating easier. Wherever possible the source of the information and the names and titles of people interviewed should be recorded. A clear concise record of the system should be prepared.

Flowcharts

Flowcharting is a diagrammatic method of recording and describing a system, which shows the flow of documents or information and the related internal controls within a system.

Flowcharts can help:

1. To obtain a perspective on the whole system;
2. Gain an understanding of the auditee's objectives;
3. Identify segregation of duties;
4. Help the person supervising the audit to identify areas which are not being covered by the audit.

Flowcharting is likely to be most effective if a logical, top-down approach is taken by starting with an overview or summary flowchart, followed by detailed flowcharts of specific processes if necessary.

There are various methods of, and symbols for, flowcharting.

When preparing flowcharts remember:

(a) Flowcharts are primarily designed to show document flows rather than operations – although other operations can be explained by means of narrative notes if necessary;

(b) Try to avoid mixing up the 'regular' process and exceptional processes (two or three transactions per period) on the same flowchart. Prepare separate charts for the regular and the exceptional processes;

(c) To consider whether it is better to record the system by preparing one or more basic flowcharts which show the main flows in the system - supplemented by narrative description where necessary;

(d) To flowchart the actual system. In some cases it may be necessary to record the 'official' system , and in those cases the charts must be labeled clearly to show whether it is the official (prescribed) or the actual (real functioning) system;

(e) To work in pencil. This will save time redrawing the flowchart when you make a mistake;

(f) That each flowchart should have a title, the date of creation and of any amendments to it and the name of the person who drafted it;

(g) To make sure that all documents (and every copy of each document) on the flowchart are fully dealt with;

(h) To think carefully before preparing a flowchart. Ask yourself whether it's really necessary or whether narrative description will be just as effective and less time-consuming.

Flowcharting can be a very effective way of recording document flows in a system.

Advantages of flowcharting are:

- Information can be easily communicated and assimilated;
- Flowcharts highlight the relationship between different parts of the system;
- The auditor can see the whole flow of documents: potential bottlenecks can be identified easily;
- Flowcharts offer a consistent method of recording;
- The auditor has to obtain a clear understanding of information flow in order to draw up a flowchart of a complex system;
- Cross-referencing between systems is made easier.

There are a number of disadvantages to using flowcharts. The most important is the time they can take to prepare. It is very easy for auditors to spend a lot of time preparing a flowchart when it would have been more efficient and useful to do a narrative description instead. Other disadvantages are:

- They are limited in scope and may not identify managerial and organizational controls;
- The technique and conventions have to be learned and practised;
- Complex flowcharts may confuse rather than clarify;
- The auditor usually needs some training and experience to be fluent in preparing them.

Organisation Charts

The organisational structure relating to the system under audit should be recorded. A copy of an existing organisation chart will suffice, as long as it is accurate and up to date.

An up-to-date organisation chart will show details of the information flow, relationships in the organization and responsibilities. It is also useful in identifying staff and deciding where audit testing needs to be done. The date the chart was prepared should be recorded.

The chart may include:

- Main department/units with a description of their functions;
- Job titles, grades and names of staff together with lines of responsibility;
- All reporting lines.

Minimum Contents of System Documentation

Whichever method is used for documenting the procedures in each system there are certain items, which should be included on every system file. These are:

- Examples of documents describing their purpose and use. These documents and reports should be filed in the order in which they are used in the system, and cross-referenced to the narrative note or flowchart.
- Examples of reports (whether computerised or manually prepared) describing their purpose and use;
- Details of the number of transactions passing through the system. These are essential to a full understanding of the context of the system in relation to the overall activities of the entity. It is therefore necessary to summarise data such as:
  (a) Number of transactions;
  (b) Value of transactions;
  (c) Seasonal fluctuations.
  (d) Forms used to evaluate the system.

It may also be useful for the auditor to know the number of employees or a stratification of the transactions by value or age to assist in the evaluation of risk when a weakness is highlighted.

The Documentation Standards have been touched upon in the section on Change Management. Documentation guidelines are decided by policies.

In the Audit Approach, an IS Auditor goes through the documentation to understand the system and the controls provided for. The IS Auditor may get clues from other audits such as Financial audits to focus on areas that need attention. S/he then prepares specific test cases, which are passed through the Computer system. Deviations are noted down and covered in the report.

Importantly, the IS Auditor looks at the standard of documentation. Is it clear? Is it Current? Is it complete? An example of Documentation Standards for the Data Model approach is given as *Annexure A.*

Annexure A

Title Page: It should contain a general description of the System, the areas it covers and the areas it does not cover.

Documentation:

1. Requirements Documentation: The purpose of the requirement section of the documentation is to define the problem so that the solution can be planned.

1.1 Name – Short title is given

- Problem statement – State what needs to be done, e.g. Share Capital needs to be updated after each transfer meeting.
- Problem Illustration – Complete and detailed specification of the problem should be given. Any assumptions made regarding the problem should be stated. This should provide a real world description of the problem, its input, its output and its processing.

1.2 Input Information

1.2.1 Input Files (to repeat for each input file)

- Name
- Description – how is the file used?
- What is the purpose?
- Format – How are the data organized and formatted?
- Size – What is the expected number of lines (or records or items)
  – Is the number fixed or variable? If variable, is there a minimum or maximum?
- Sample – provide a sample of properly formatted input.

1.2.2 Input Items: Repeat for each data element or program input

- Description – What does the input or data element mean?
- Type – What is its logical data type (e.g. integer, alpha- numeric etc.)
- Range of acceptable values – What is the acceptable range for this program (e.g. 0 – 30,000)

1.3 Output Information

1.3.1 Output files (repeat for each file or stream)

- Name
- Description – How is it used? What is its purpose?
- Format – How are the data organized and formatted in the output file
- Size – How many number of lines (records or items) are accepted
- Is the number fixed or variable? If variable, is there a minimum or maximum.
- Sample – provide a sample of properly formatted output.

1.3.2 Output items: Repeat for each program output

- Name

- Description – What does the output element mean? What is it used for?
- Type – What is its logical data type (integer, alphanumeric)
- Range of Acceptable Values – What is the acceptable range for this program.

1.4 User Interface Information

- Description – How will the user interact with the program?
- Types of user interfaces include menu selection, Form Fields, command language etc.
- Sample – include illustrations of screens.

1.5 Specifications: Description of functionality

2. The purpose of section of the documentation is to describe the plan for the solution of the problem. The software system consists of all components of the software product. The components are a collection of related items (sub-routines, constant etc.)

2.1 System Description: This section includes a list of each system component.

2.2 Component Information: A solution will include several types of system components. It consists of:

- Data abstraction
- Functional abstraction.

Module Information (repeat for each module)

- Module Name – Name of the Data abstraction
- Descriptions – briefly describe the task it performs. Specify accepting inputs and outputs

Data Abstraction Attributes — repeat for each attribute.

- Name
- Description
- Type
- Range of acceptable values.

Data Abstraction operations –

- Name – Name of the operation
- Description – briefly describe the task it performs.
- Specify accepting inputs and the outputs.

Functional Abstraction Components: Functional abstraction components consist of collection of sub routines that work together to carry out a portion of the requirements of the overall system. All sub-routines other than the main routine and those listed in the section on audit abstraction components should be covered in this section.

Sub Routine Information:

- Name
- Brief description of its function
- Input parameter – Name, type and purpose for each parameter

– Output parameter – Name, type and purpose for each parameter.

Design diagrams: Diagrams should be used to illustrate the design.

Structure chart is a true diagram of the sub-routine in a program. It indicates the interconnection among the sub-routines.

Pseudo Code — This section should describe in an easily readable and modular form how the software system will solve the given problem. Using simple Standard English terms, there should be a description of the problem and how exactly the solution is obtained.

III. Implementation Document: The purpose of this documentation is to give details of how the system has been implemented.

Physical Organization of System Components: Different components of the System. The architecture will appear in different compilation.

Comments: The program design information should be explained. It should broadly cover System Documentation, Problem Statement, Problem Specification, System Architecture.

Programming style: Programming style refers to those conventions that enhance the readability of the program.

IV. Verification and Validation Documents: The purpose of the verification and Validation documents is to demonstrate the operation of the program, describe how it is run on the machine and present evidence of program verification and validation.

IV.1 Planning

– Approach – What is the approach which has been adopted to ensure system software works correctly.

– Test Cases and Test Audit include a list of input data that test thoroughly the logic of the program and demonstrates that the program satisfies its requirements. If each of the test data explain the requirements it will exercise.

IV.2 Outcome of Verification and Validation

Summary of verification and validation results: Give a brief description of the results from your verification and validation activities.

Verification and Validation Process: Provide a description of the procedure followed and any changes made.

IV.3 Operating Directions: The name and version number of the compiler used

– Name and location of the version program file, executable file, and any data files used.

– Names and locations of different files which are needed to be compiled to execute this program.

IV.4 If the program has any bugs that needs to be indicated. Explain what parts of the program work and also any caution that needs to be exercised to avoid problems.

V. Version History

– Revision I

– Revision II

– Original Version

LESSON ROUND-UP

- Information systems auditing or systems audit is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently.
- The objectives of information system audit include verifying safeguarding of assets, data integrity, system effectiveness and system efficiency.
- To start system audit, a plan has to be developed, covering scope and objectives, key strategies for Analysis and understanding of standard procedures, Evaluation of system and internal controls. Audit procedures and documentation of evidence etc.
- Information systems auditing is not just a simple extension of traditional auditing. The discipline of information systems auditing has been shaped by knowledge obtained from four other disciplines i.e. traditional auditing, computer science, behavioural science and information system management.
- The nature of systems audit, unlike the other audits, is not restricted to audit of reported items only. It has to take into cognizance the choice, use and risk of Technology. It has to look at the realities of business processes and constantly changing legal framework
- The scope of systems audit covers the entire IS management process. The scope includes review of the entire design & development process, the review of technology choice, the processes employed to assess risks and losses that could accrue to the system, the possibility of computer frauds, the care taken in managing changes to the system, extent of testing and reliability of the system. \
- IS Audit is an evaluation of adequacy of Management controls, Operational Controls, Organisation controls and application controls.
- Steps involved in conducting IS audit includes, purviewing of the environment, Understanding the Information Systems, Identification of the Audit Risks, Audit Evidence, Key Control Points and Identify Control Weaknesses, Verifying veracity of computer files, Conduct Audit Tests, Concluding the Audit
- Collecting evidence on the reliability of a computer system is often more complex than collecting evidence on the reliability of a manual system. Auditors confront a diverse and sometimes complex range of internal control technology that did not exist in manual systems. Auditors must understand these controls if they are to be able to collect evidence competently on the reliability of the controls.
- Given the increased complexity of computer systems and internal control technology, it is also more difficult to evaluate the consequences of control strengths and weaknesses for the overall reliability of systems. First, auditors must understand when a control is acting reliably or malfunctioning. Next, they must be able to trace the consequences of the control strength or weakness through the system.
- For doing the system Audit of Computerised Secretarial Function, the auditor should note that the procedure to be followed for performing a Systems Audit remains the same irrespective of functionality. The testing of application controls alone vary. Systems audit consists of evaluating the Management Controls, Environmental Controls, Organizational Controls and Application Controls
- The use of test packs is the application of auditors test data (live or dummy) to client's application programs. A small sample of data is processed through the computer and output is compared with manually generated output using the same data. This audit approach requires little computer expertise but designing of test data which will represent all the possible combinations is a time consuming and difficult process. Use of test data generators can overcome this disadvantage.

SELF-TEST QUESTIONS

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. Discuss nature and significance and scope of systems audit. Also mentions various steps involved in conducting in information system audit.
2. Discuss system audit of computerised secretarial functions.
3. Write short notes on:
   (a) Norms and procedures for computerisation
   (b) Computer control and security
   (c) Testing of computer system
   (d) Objectives of Information Systems Auditing
4. Discuss the Foundations of Information Systems Auditing.
5. What do you mean by operation control? Describe in details
6. What do you mean by test pack? State the use of test pack in IS Audit.
7. What is the meaning of documentation standards? Explain its importance.
8. State the relationship of Systems audit and various management functions.

GLOSSARY

Algorithm	In computing, a finite set of well defined rules for the solution of a problem in a finite number of steps.
Applet	A small *Java program* that can be embedded in an *HTML* page. Applets differ from full-fledged Java applications in that they are supposed to be restricted to provide some security to the user.
Application	A *system* that has been developed to serve a specified purpose, for example to pay suppliers' invoices, place orders with suppliers and maintain stock records. An application incorporates both clerical and computerised procedures; *controls* over *transaction* input, processing and output; and *file* management. It should also maintain an *audit trail* (see also *system software*; *program*).
ASCII	American Standard Code for Information Interchange. ASCII was developed to *standardise* data transmission among disparate hardware and *software* systems, and is built into most mini and personal computers. It is a coding scheme using 7 or 8 *bits* that assigns numeric values to up to 256 characters. These include letters, numerals, punctuation marks, control characters and other symbols. ASCII text is often referred to as a "plain text"
Asymmetric encryption	A cryptographic *algorithm* that employs a *public key* for *encryption* and a *private key* (see *secret key*) for *decryption*; or in *authentication*, a private key for signing and a public key for signature verification. Public and private *keys* are related and form an asymmetric key set.
Audit trail	A chronological set of *records* that collectively provide documentary evidence of processing, sufficient to enable reconstruction, review and examination of an activity.
Authenticity	The attribute of genuineness. For evidence to be authentic it must be all that it purports to be.
Authentication	(1) The act of determining that a *message* has not been changed since leaving its point of origin. **(**2) A process that verifies the claimed identity of an individual.
Availability	The ability to access and use a *system*, resource or *file*, where and when required.
Backup	A duplicate copy (e.g. of a *program*, of an entire disc or of *data*) made either for archiving purposes or for safeguarding valuable *files* from loss should the active copy be damaged or destroyed. A backup is an "insurance" copy.
Bandwidth	A measurement of how much *data* can be sent across a communications circuit at the same time. It is usually measured in *bits* per second (BPS).

Biometrics	In *access control*, automated methods of verifying or recognising a person based upon behavioural or physical characteristics (e.g. fingerprints, handwriting, and facial or retina geometry).
BIOS	Basic Input/Output System. The set of essential *software* routines that test hardware at start-up, start the *operating system* and support the transfer of *data* among hardware *devices*. On PC-compatible computers, the BIOS is stored in read-only memory (*ROM*) so that it can be executed when the computer is turned on. Although critical to performance, the BIOS is usually invisible to computer users.
Bit	Shortened term for binary digit. It is the smallest unit of *information* handled by a computer. One bit expresses a 1 or a 0 in a binary numeral, or a true or false logical condition, and is represented physically by an element such as a high or low voltage at one point in a circuit or a small spot on a disk magnetised one way or the other. A single bit conveys little information a human would consider meaningful. A group of 8 bits, however, makes up a *byte*, which can be used to represent many types of information, such as a letter of the alphabet, a decimal digit or other character.
Black box testing	Testing that involves no knowledge of the internal structure or logic of a *system*.
Boot	The process of starting or resetting a computer. When first turned on (cold boot) or reset (warm boot), the computer executes important *software* that loads and starts the computer's *operating system* and prepares it for use. Thus, the computer can be said to pull itself up by its own "bootstraps".
Browsing	Searching through storage to locate or acquire *information*, without necessarily knowing of the existence or the format of the *data* being sought.
Buffer	(1) In computing, an area of storage that is temporarily reserved for use in performing an input/output operation, into which *data* is read or from which it is written. (2) In data communications, a storage area used to compensate for differences in the rate of flow of data, or time of occurrence of events, when transferring data from one *device* to another.
Bug	An error in *programming code* that produces an undesirable variation from design performance in a *program* during execution.
Business continuity	A formal plan, or integrated set of plans, designed to enable key business processes to continue in operation following a major system failure or disaster. Essential ingredients include the identification of key business *processes*, adequate system *backups* and a workable continuity *strategy*.
Byte	A unit of *data* generally comprising 8 *bits*. A byte can represent a single character, such as a letter, a digit or a punctuation mark. Because a byte represents only a small amount of *information*, amounts of computer memory and storage are usually given in kilobytes (1,024 bytes), megabytes (1,048,576 bytes), or gigabytes (1,073,741,824 bytes).

Call centre	A central point where customer and other telephone calls are handled by an organisation, usually assisted by some amount of computer automation. Typically, a call centre has the ability to handle a considerable volume of calls at the same time, to classify calls and forward them to someone qualified to handle them, and to record calls. Call centres commonly handle such activities as customer services, order entry, reservations, *help desk* facilities, dispatch systems, telesales and collections. Telephone banking, insurance and share dealing are among financial applications.
CASE	Computer Aided Systems Engineering. *Software* tools that support *systems* analysis, design and construction.
Central Processing Unit	(CPU) computer hardware that houses the electronic circuits that control/ direct all a computer's operations.
Certification authority	In cryptography, an authority trusted by all users to create and assign *digital certificates*.
Change Control	In *project management*, uncontrolled changes are one of the most common causes of delay and failure. Change Control is the process of implementing procedures which ensure that proposed changes are properly assessed and, if approved, incorporated into the project plan.
Change management	IN IT service management, the *process* of *controlling* and managing requests to change an *IT Infrastructure* or *IT service*, and then controlling and managing the implementation of the changes that are subsequently approved.
Channel	In data communications, a path along which signals can be sent. The term may also refer to a mechanism by which the path is effected.
Ciphertext	In *cryptography*, unintelligible text produced through the use of *encryption*.
Classification	The process of formally identifying *incidents, problems* and *known errors* by origin, symptoms and cause.
Client	(1) A computer that interacts with another computer, usually referred to as the *server*, using a client *program*. E-mail is an example - an e-mail client connects to an e-mail server to send and receive *messages*. (2) A term sometimes used by auditors to refer to an audited organisation.
Code	*Program* instructions written by a programmer in a programming language.
Confidentiality	In *information security*, the property that *information* is not made available or disclosed to unauthorised individuals, entities or processes.
Controls	In *information security*, *policies*, *procedures* and mechanisms designed to ensure that activities achieve their authorised objectives. Controls can be preventive (e.g. a 'no smoking' policy is enforced), detective (e.g. a smoke detector), corrective (e.g. a sprinkler system) or restorative in character (e.g. a disaster recovery plan).

Cryptography	The discipline that embodies principles, means and methods for the transformation of *data* in order to hide its *information* contents, prevent its undetected modification, and/or prevent its unauthorised use.
Data	In computing, (1) a representation of facts, concepts, *information*, or instructions in a manner that is suitable for processing by an *information system*. (2) The building blocks of information.
Data dictionary	In *databases*, a centralised repository of *information* about the stored *data*, providing details of its meaning, relationship (to other data), origin, usage and format.
Data file	A *file* consisting of *data* in the form of text, numbers or graphics, as distinct from a *program* file containing commands and instructions. Data files may also be called documents or spreadsheets.
Database	An extensive and comprehensive set of *records* collected and organised in a meaningful manner to serve a particular purpose.
DBMS	Database Management System. *Software* that handles *database* access requests from *application* processes. Essentially a DBMS handles storage, access, *data* sharing among multiple users, and database administration tasks (e.g. controlling what data an application *user* can view and update).
Decrypt	In *cryptography*, to convert by use of the appropriate *key*, *encrypted* text (see cipher text) into its equivalent plaintext.
Device	A generic term for printers, scanners, mice, keyboards, serial ports, video adapters, disk drives and other computer subsystems. Such devices frequently require their own controlling *software*, called *device drivers*.
Digital certificate	In *cryptography*, a message that guarantees the authenticity of the data contained within it. In *public key cryptography* it is important that anyone using a public key can be sure about its *authenticity*. Such a guarantee may be issued by a *Certification Authority* trusted by the users, and based on assurances obtained from applicants for digital certificates. A certificate generally contains the public key owner's identity, the public key itself and its expiry date. A user supplies the certificate and the recipient *decrypts* it using the certification authority's public key (often performed automatically by the recipient's *browser*/e-mail software). The recipient gains assurance that a trusted authority has signed the user identity and corresponding public key.
Digital signature	A *data* block appended to a *file* or *message* (or a complete *encrypted* file or message) such that the recipient can *authenticate* the file or message contents and/or prove that it could only have originated with the purported sender.
Document	*Information* in readable form. The medium on which the document is held (e.g. paper, fiche, film and magnetic disk) is not important.

EBCDIC	Extended Binary Coded Decimal Interchange Code. Developed by IBM, and mostly used by *mainframe* systems, EBCDIC is a standard way of representing text symbols using binary numbers
EDI	Electronic Data Interchange. In computing and communications, the transmission of documents from one computer to another over a *network*. Although EDI is sometimes carried out over direct links between trading partners (and increasingly the *Internet*), it is more usual to involve a value added supplier to operate an electronic mailbox through which documents are exchanged on a store and collect basis, similar to e-mail. The ability of communicating computer systems to exchange and process *information* in this way can significantly speed up processing and reduce manual transcription errors.
EFT	Electronic Funds transfer. *Systems* designed to move funds between banks using electronic communications rather than paper media. Common EFT systems include BACS (Bankers' Automated Clearing Services) and CHAPS (Clearing House Payment System).
Electronic business	Using an electronic *network* to simplify and speed up all stages of the business process including such as activities as design and manufacturing; buying, selling and delivering; and transacting government business.
Electronic commerce	Using an electronic *network* to simplify and speed up the process of buying, selling and delivering.
Electronic government	Using an electronic *network* to deliver government *information* to, and transact government business with other departments of state, citizens and businesses, and other governments.
Encryption	(Also encipher). The process of transforming *information* into an unintelligible form in such a way that the original information cannot be obtained ("one-way" encryption) or cannot be obtained without using the inverse *decryption* process ("two-way" encryption).
Encryption algorithm	A set of mathematically expressed rules implemented in either *firmware* or *software*, and used in conjunction with a *secret key* for *encrypting* plaintext and decrypting *cipher text*.
ETHERNET	A common *LAN* technology that employs CSMA/CD (carrier sense multiple access with collision detection) over either coaxial cable or twisted pair wiring. CSMA/CD allows computers to transmit when the *network* is free.
File	A complete, named and collection of *information*. (1) In computing, a *file* can contain program *code*, *data* (e.g. *transactions* to be processed by a *program*), or user-created data (e.g. a word processor file). Most commonly, however, the term refers to data (numbers, words, or images) that a user has created and then saved for subsequent retrieval, editing or printing. (2) In *information systems*, a collection of *documents*. The medium on which the documents are stored (e.g. paper, fiche, microfilm, magnetic disks) is not important.

File server	In a local area *network* (*LAN*), a computer that provides access to *files* for *workstations* that are connected to the network.
Firewall	A security system used to prevent unauthorised access between networks (both internal/internal, and internal/external) by examining and filtering IP data *packets*. A firewall will allow only approved traffic in and/or out by filtering packets based on source/destination *IP address*, source/destination port. The firewall inspects the identification information associated with all communication attempts and compares it to a rule-set consistent with the organisation's security policy. Its decision to accept or deny the communication is then recorded in an electronic log.
Firmware	Programming that is inserted into Programmable Read-Only Memory (PROM), thus becoming a permanent part of a computing *device*. Firmware is created and tested like other *software*. It can also be distributed like other software and installed in the PROM by the user. Firmware is sometimes distributed for printers, *modems* and other computer *devices*.
	Fourth Generation Language Any programming language that uses English terminology and allows rapid *software* development. With 4GLs the user specifies what is required and the programming language works out what actions are needed to carry out the required task. *Structured Query Language* (SQL) is a commonly used 4GL.
FTP	File Transfer Protocol. In communications, a *protocol* that ensures the error-free transmission of *program* and *data files* via a data communications link.
Function Point Analysis	In planning and estimating, a technique used to determine the size of a development task. It entails breaking a *project* down into function points (factors such as inputs, outputs, enquiries, logical internal sites, etc.), which are then classified by degree of complexity. Factors are then applied from which time estimates may be developed.
Gateway	A computer or other *device* that links two *networks*, routing and often converting *protocols* or *messages* from one network to the other. The term can also refer to a system capability that provides direct access to other remote networks or *services*.
GANTT Chart	A bar chart plotting the phases or *activities* of a *project* against a predefined timeline to completion.
Gigabyte	(GB) 1,024 megabytes (2^{30} *bytes*). Often interpreted, though, as approximately one million *bytes*.
Hash total	A figure obtained by some operations upon all the items in a collection of *data* and used for control purposes. A recalculation of the hash total, and comparison with a previously computed value, provides a check on the loss or corruption of the data.

Host	A computer connected to a *network* that offers services to one or more users.
HTML	Hypertext Markup Language. The programming language used for *web pages*. It is called a "mark-up" language because it is used to describe the formatting to be used to display the document. The html file contains both the text and *code* (called tags). It is read by a web browser, which interprets the code and displays the web pages in the format specified by the HTML.
HTTP	Hypertext Transfer Protocol is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the *World Wide Web*. By comparison with the *TCP/IP* suite of *protocols*, which forms the basis of *information* exchange across the *Internet*, HTTP is an *application* protocol.
Hub	A *device* that connects several devices (terminals, printers, etc.) to a *network*.
ICT	Information and Communications Technology. The acquisition, processing, storage and dissemination of *information* using a combination of computer and telecommunications technologies.
Information	Knowledge that was unknown to the recipient prior to its receipt. Information is derived from *data*, which to be of value needs to be valid (e.g. not duplicated or fraudulent), complete, accurate, relevant and timely.
Information security	The result of any system of policies and procedures for identifying, controlling and protecting *information* against unauthorised disclosure, manipulation, modification; unavailability and destruction. Unauthorised disclosure refers to information that is, for example, commercially sensitive, nationally classified or subject to *data protection* legislation. Manipulation is concerned with changing some attribute of the *data*, such as *file* ownership, security classification, destination, etc. Modification involves unauthorised alteration of the data itself, which can take place without leaving any trace. Unavailability refers to an inability to access and process the data (e.g. due to computer or communications failure). Data can be destroyed quickly and efficiently in electronic or magnetic storage *devices* (e.g. by degaussing, powering down *volatile* storage and overwriting).
Information security policy	A formal statement that defines top management intentions on *information security*, and provides general direction for protecting the *confidentiality, integrity and availability* of corporate *information*.
Information system	The means for organising, collecting, processing, transmitting, and disseminating *information* in accordance with defined *policies* and *procedures*, whether by automated or manual means.
Input controls	Techniques and procedures used to verify, validate and edit *data* to ensure that only correct data is entered into a computer *system*.

Integrity	In *information security*, the property that *information* is valid, complete and accurate.
Internet	A worldwide system of linked computer *networks* that enables data communication *services* (based on *TCP/IP*) such as remote logon, file transfer, electronic mail, and newsgroups. The Internet is not a discrete computer network, but rather a way of connecting existing computer networks that greatly extends the reach of each participating system. It is not single service, has no real central hub, and is not owned by any one group (see also IETF).
Intranet	A private *network* inside an organisation that uses the same kinds of *software* and *protocols* found on the *Internet*. Intranets may or may not be connected to the Internet.
IP	Internet Protocol. A *protocol* that defines and routes data across the *Internet*. It uses *packet switching* and makes a best effort to deliver its *packets* (see also *TCP/IP*).
IP address	Every computer on the *Internet* is assigned a unique number so it can be identified. *IP* addresses are 4 dot-separated numbers (for example, 205.243.76.2) that specify both the *network* the computer is connected to and the *host*.
ISDN	Integrated Services Digital Network. A medium speed, digital connection. It provides up to 128kbps *bandwidth* over two *channels*. Like normal phone lines, it has a number that can be dialled into and it can dial out to any other ISDN number, unlike leased lines which are strictly point-to-point. Like leased lines, ISDN provides a reliable digital *service* that is not normally affected by line noise and other ailments that modems can experience.
IS Steering Committee	The top management group responsible for the overall direction of *information systems* (IS). The ISSC owns, commissions, directs and agrees their organisation's *IS Strategy*.
IS Strategy	An organisation's master plan for directing, developing, installing and operating the *information systems* necessary to satisfy its business needs. An IS strategy should be supported by a business case to provide purpose and economic justification for what is proposed. It should also include measurable performance targets and deadlines against which its success can be monitored. Due to the delay generally involved in bringing new *IT infrastructure* into operation, an IS strategy usually covers a three to five year planning period. It should, however, be monitored and updated frequently to ensure that it continues to represent an effective and workable plan. See *IS Steering Committee*.
Key	In *cryptography*, a symbol or sequence of symbols that controls the operations of *encryption* and *decryption*. It is essential that keys are protected against unauthorised disclosure.

LAN	Local Area Network. A *network* that connects PCs and other computers within a limited geographic area by high-performance cables so that users can exchange information, share expensive peripherals, and draw on the resources of a massive secondary storage unit, call a *file server*.
Logical	In computing, conceptual or virtual (i.e. within the computer; in *cyberspace*), as compared with physical or actual (i.e. outside the computer; real world).
Logical access	The act of gaining access to computer *data*. Access may be limited to "read only", but more extensive access rights include the ability to amend data, create new *records*, and delete existing records (see also *physical access).*
Login	The act of connecting to a computer and being *authenticated* as a legitimate user. The usual requirements are a valid user name (or user ID) and password, but in higher *risk* scenarios a user may also have to insert a physical token (e.g. a *smartcard*) and/or provide *biometric* proof of identity.
Mainframe	A high-level computer designed for the most intensive computational tasks. Mainframe computers are often shared by multiple *users* connected to the computer by terminals.
Macro	A macro is a list of actions to be performed that is saved under a short key code or name. *Software* can then carry out the macro's instructions whenever the user calls it by typing its short key code or specifying the macro name.
Media	The physical material, such as paper, disc and tape, used for storing computer-based *information*.
Memory	Memory generally refers to the fast semiconductor storage (Random Access memory, or *RAM*) directly connected to the *processor* that is dependent on electrical power for activation. Memory is often differentiated from computer storage (e.g., hard disks, floppy disks, CD-*ROM* disks) that is not dependent on electricity and is therefore a more permanent means for holding *data*.
Memory chip	Or "chip", is an integrated circuit devoted to memory storage. The memory storage can be *volatile* and hold *data* temporarily, such as *RAM*, or non-volatile and hold data permanently, such as *ROM*, EPROM, EEPROM or PROM.
Message	In data communications, an electronic communication containing one or more *transactions* or one or more items of related *information*.
MICR	Magnetic Ink Character Recognition. A technique for the identification of characters printed with ink that contains particles of a magnetic material. Used widely in the banking industry to capture sort codes and account numbers on cheques.

Microprocessor	A central processing unit (*CPU*) on a single microchip. A microprocessor is designed to perform arithmetic and logic operations that make use of small number-holding areas called *registers*. Typical microprocessor operations include adding, subtracting, comparing two numbers, and moving numbers from one area to another. These operations are the result of a set of instructions that are part of the microprocessor design. A modern microprocessor can have more than one million transistors in an integrated-circuit package that is roughly one inch square. Microprocessors are at the heart of all computers, from *mainframes* down to *smartcards*.
Middleware	*Software* that is neither part of the *operating system*, nor an *application*. It occupies a layer between the two, providing applications with an interface for receiving services. Common examples are communications *programs* and *transaction* processing monitors.
Modem	A communications *device* that enables a computer to transmit *information* over a standard telephone line. Because a computer is digital (it works with discrete electrical signals representing binary numbers 1 and 0) and a telephone line is analogue (carries a signal that can have any of a large number of variations), modems are needed to convert digital to analogue and vice versa. The term is short for Modulator/Demodulator.
Multiplexor	Equipment that takes one or more *data channels* and combines the signals into one common channel for transmission. At the receiving end a demultiplexor extracts each of the original signals.
Network (1)	In data communications, a computer-based communications and data exchange *system* created by physically connecting two or more computers. The smallest *networks*, called local area networks (*LAN*'s), may connect just two or three computers so that they can share an expensive peripheral, such as a laser printer, but some LAN's connect hundreds of computers. Larger networks, call wide area networks (*WAN*s), employ telephone lines or other long-distance communications media to link computers.
Network (2)	A diagram that shows the logical relationships between *activities*.
Objective	A desired goal, or end result.
OCR	Optical Character Recognition. Techniques and equipment for reading printed, and possibly hand-written, characters on a *document* and converting them to digital code (e.g. *ASCII*) for input to a computer.
Off-the-shelf	A packaged item ready for sale. The term can refer to hardware, *software* or both.
On-line	Generally describes a computer that is connected to a *network* and is thereby ready for operation or interaction over the network. It may also refer to the ability to connect to the *Internet* by virtue of having an Internet account.

Operations bridge	The combination in one physical location of computer operations, *network* control and the *Help Desk*.
Operating system	In computing, a collection of *software* designed to directly control the hardware of a computer (e.g. input/output requests, resource allocation, data management), and on which all other *programs* (including *application programs*) running on the computer generally depend.
Output controls	*Controls* whose objectives are to ensure that computer outputs are complete and accurate, are securely held until distribution (they may include financial instruments), and are distributed to the intended recipient(s) in a timely manner.
Outsource	The use of an external contractor to provide (1) both the IT *systems* and the personnel required to run them (see also *facilities management*). (2) support *services*, such as hardware maintenance.
Packet	(Sometimes referred to as a 'frame') in communications, a packet comprises a well-defined block of bytes consisting of 'header', *'data'* and 'trailer'. Packets can be transmitted across *networks* or over telephone lines. The format of a packet depends on the *protocol* that created it. Various communications *standards* and *protocols* use special purpose packets to monitor and control a communications session.
Packet switching	A transmission method in which *packets* are sent across a shared medium from source to destination. The transmission may use any available path or circuit, and the circuit is available as soon as the packet has been sent. The next packet in the transmission may take a different path, and packets may not arrive at the destination in the order in which they were sent.
Password	In *Access Control*, confidential *authentication information* usually composed of a string of characters, that may be used to control access to physical areas and to *data*.
Physical access	In *access control*, gaining access to physical areas and entities (see *logical access*).
Platform	The computer hardware, and the associated *operating systems software* necessary for its operation, on which *applications software* is run.
Port	an interface between the CPU and a peripheral *device*.
Procedure	A set of instructions for performing a task. Procedures should be consistent with *policy* requirements.
Process	In IT Service Management, a sequence of operations that are intended to achieve a defined objective. Processes require *policy*, people, procedures and *IT infrastructure*.
Processing controls	*Controls* whose objectives are to ensure that only valid *data* is processed, and that processing is both complete and accurate.

Program	In computing, a series of instructions that conform to the syntax of a computer language, that when executed (or "run") on a computer will perform a given task.
Protocol	A set of rules that must be followed for any data communications to be made. Protocols enable totally different *platforms* (e.g. computers connected to the *Internet*) to communicate with each other. For one computer to communicate with another, both must adhere to the same *protocol(s)*.
Public key	In *cryptography*, the *key*, in an *asymmetric* encryption system, of a user's key set that is known to other users.
Query	In computing, a specific set of instructions for extracting particular *data* from a *database*.
RAM	Random Access Memory. Semiconductor-based memory that can be read and written by the central processing unit (CPU) or other hardware *devices*. The term is generally understood to refer to volatile memory that does not permanently hold *data* or *programs*.
Record	(1) In computing, a collection of related *data* treated as a unit. A record is the main unit of storage within a *file*. (2) In record management, anything that provides permanent evidence of, or *information* about past events. Although the term *document* includes records, records are particular types of document that are not subject to amendment, and for which there is often a legal or contractual requirement.
Risk management	The total process involved in reducing identified *risks* to a level that is acceptable to an organisation's top management.
ROM	Read-Only Memory. A semiconductor circuit into which *code* or *data* is permanently installed by the manufacturing process. ROM contains instructions or data that can be read or executed, but not modified.
Script	A simple *program* consisting of a set of instructions that are designed to perform or automate a task or function.
Secret key	In *cryptography*, the *key* of a user's key set in an *asymmetric* or *public key* cryptographic system, which may be known only to that user.
Server	A computing unit or *node* in a *network* that provides specific *services* to network *users*, e.g. a printer server provides printing facilities to the network, and a *file* server stores users' files.
Service Level Agreement	Or SLA, is a written agreement between a user and an IT service provider that documents the agreed service levels for an IT service (e.g. hours of operation, maximum downtimes, transaction throughput, terminal response times, security, contingency). An SLA is not normally a contract in itself, but it may form part of a contract.

Smartcard	A plastic card (of identical dimensions to a credit card) that has electronic logic embedded in it in the case of a *stored data card*, or a *microprocessor* in the case of cards with processing ability. Smartcards are commonly used to perform *digital signatures*, *authenticate* users for *access control* purposes, and *encrypt* or *decrypt messages*.
SMTP	Simple Mail Transport Protocol. The *protocol* that is used to move e-mail and any attachments between mail *servers*.
Software	Instructions for the computer. A series of instructions that performs a particular task is called a *program*. The two main types of software are *system software* (*operating system*), which controls the workings of the computer and *application programs*, which perform the tasks for which people use computers. A common misconception is that software is *data*. It is not. Software tells the hardware how to process the data. Software is "run" (or "executed"), whereas data is "processed."
Software package	A *software program* or *application* sold to the public, ready to run, and containing all necessary components and documentation. Also called "shrink wrapped" or "off-the-shelf" software.
Software maintenance	Any modification to a *software* product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a changed environment.
Specification	A detailed description of the requirements for a product or *service*.
Spoofing	In *Information Security*, (1) assuming the characteristics of another computer system for purposes of deception. (2) Malicious *code* that masquerades as the *operating system*, presenting a *login* screen and tricking the user into revealing their *password*.
SQL	Structured Query Language, the traditional language for accessing *data* stored in a relational *database*.
Strategy	A detailed and systematic plan of action.
Superuser	A user with unrestricted access to user *files* and system *utilities*. For reasons of security, this level of access should only be granted to the minimum number of staff necessary to perform system administration duties.
Symmetric encryption	A form of *data encryption algorithm* that employs the same value of *key* for both encryption and *decryption* processes.
System	Any collection of components that work together to perform a task. Examples are a hardware system consisting of a *microprocessor*, its allied chips and circuitry, input and output *devices*, and peripheral devices; an *operating system* consisting of a set of *programs* and data *files*; a *database management system* used to process specific kinds of *information*; or an *application system* used to perform a particular business function.

System Development Life Cycle	(SDLC). is the process of developing *information systems* through investigation, analysis, design, implementation, and maintenance.
System software	*Software* primarily concerned with co-ordinating and controlling hardware and communication resources, access to *files* and *records*, and the control and scheduling of *applications* (see also *operating system*).
TCP/IP	**T**ransmission Control Protocol/Internet Protocol. A set of *protocols* that make *Internet* services (Telnet, FTP, e-mail, etc.) possible among computers that don't belong to the same *network*.
Test environment	A computer system or part of a computer system (made up of hardware and *system software*), which is used to run, and sometimes to build, software *releases* for acceptance testing.
Test data	In computing, *data* prepared solely to test the accuracy of the *programming* and logic of a *system*. It is used to prove each branch and combination of branches (within feasible limits) of a system and should, therefore, be as comprehensive as possible.
Threat	In *Information Security*, actions and events that may jeopardise a *system's* objectives.
Transaction	A discrete activity within a computer *system*, such as an entry of a customer order or an update of an inventory item. Transactions are usually associated with *applications*.
Trapdoor	A hidden hardware or *software* mechanism that permits *access controls* to be bypassed. Trapdoors often inserted by system developers as a convenient means of testing computer *programs* and diagnosing *bugs*.
Trojan Horse	In *Information Security*, an apparently useful *program* that performs unauthorised functions by taking advantage of an innocent user's access rights in order to copy, misuse or destroy *data*. For example, a Trojan Horse hidden in a text editor might covertly copy sensitive *information* contained in a *file* being edited to another file that is accessible by the attacker
UNIX	A highly portable, general purpose, multi-user *operating system*, generally used on small and mid-range computers (versions are also available for PCs). There is many common features between the numerous commercial versions of UNIX. UNIX provides facilities for sharing resources (disc space, CPU time, etc.) and for protecting *users' files*. For each file users can allocate individual read, write and execute privileges to themselves, members of groups and all other users. The operating system is also multitasking, which allows users to relegate *programs* that require no interaction to background processing whilst working interactively on other tasks.
URL	Uniform Resource Locator. A uniform method where a *host* can be accessed at a specific address using a specific *protocol.* An example is http://www.Icsi.edu/, the URL for ICSI.

UPS	In *business continuity* an acronym for Uninterruptible Power Supply. A *device*, connected between a computer (or other electronic equipment) and a power source, that ensures that the computer's power supply is not interrupted. In most cases it also protects the computer against potentially damaging events, such as power surges and brownouts. All UPS units are equipped with a battery and a loss-of-power sensor; if the sensor detects a loss of power, it switches over to the battery so that the user has time to close down the computer in a controlled manner, thus avoiding *data* loss.
Utility program	*Software* designed to perform maintenance work on a system or on system components (e.g., backing up data; disk and *file* recovery; editing; sorting and merging; file and memory *dumps*)
Virus	A computer *program* designed to carry out unwanted and often damaging operations. It replicates itself by attaching to a host, which depending on the type of virus, may be a program, *macro* file or magnetic disc. In common with a human virus, the effects of a computer virus may not be detectable for a period of days or weeks during which time the virus will attempt to spread to other systems by infecting files and discs. Eventually, the effects manifest themselves when a date or sequence of events triggers the virus.
Virtual Private Network	A VPN is a private data *network*, but one that uses the public telecommunication infrastructure, such as the Internet. It is similar in concept to a system of owned or leased lines, but provides comparable capabilities at much lower cost by using shared rather than private infrastructure. Using a virtual private network involves *encrypting data* before sending it through the public network and *decrypting* it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. VPN software is typically installed as part of the organisation's *firewall* server.
Volatile	In *data* storage, a term used to describe any *device* that needs to be powered on in order to function. Most microchip storage technologies are volatile, compared with optical and magnetic storage devices which are non-volatile (although considerably slower to access).
Vulnerability	In *Information Security*, a weakness or flaw (in location, physical layout, organisation, management, procedures, personnel, hardware or software) that may be exploited by a *threat* to cause an *impact*.
Web browser	Or web client, is *software* designed to navigate the *WWW*, view its *information* resources and, when used interactively, exchange information. Netscape Navigator and Internet Explorer , Mozilla, Firebox are widely used examples of web browsers.
Web server	An *Internet host* computer that stores *web pages* and responds to requests to see them. Web servers talk to *web browsers* by using a language named *HTTP*.

Web site	A location on the World Wide Web (*WWW*). It is synonymous with *web page* and *web server*.
Web page	The basic building block of the World Wide Web (*WWW*). *Information* displayed on a web page can include highly sophisticated graphics, audio and video, the locus of contemporary creativity. Web pages are linked together to form the WWW.
Wide Area Network	(WAN) - a telecommunications *network* that is dispersed over a wide geographic area – possible world wide - as distinct from a local area network (*LAN*) that is generally confined to a confined geographic area, such as a building. A wide area network may be privately owned or rented; either way it usually requires the use of public (shared user) networks (e.g. the *Internet*) and/or leased communication circuits. See also VPN.
Work Breakdown Structure	A tree diagram that breaks a *project* down in increasing levels of detail. The lowest level of a work breakdown structure comprises *activities*.
Workstation	This term tends to have different meanings in different contexts. Generally it refers to a high-powered microcomputer, typically single-user but very powerful machines.
Worm	(1) In communications, a malicious *program* which, unlike a *virus*, is free-standing (i.e. it does not require a host). Worms replicate themselves across *networks*, cause both traffic congestion and can cause network failure. (2) In computing, Write Once Read Many (WORM). A data storage *device* to which *code* or *data* can be written but not altered or erased. They are generally implemented on non-rewritable optical discs, although pseudo-WORM magnetic tape devices are becoming available.
WWW	World Wide Web. Refers to the *information* resources of the *Internet* that are accessible via *web pages* using a *web browser*. Technically speaking, the WWW refers to the abstract cyberspace of information whereas the Internet is the physical side of the *network*, i.e. the computers and communications that link computers throughout the World.
XML	Extensible Markup Language, is a set of tags and declarations used as a complement to *HTML* in the construction of *web pages*.

PROFESSIONAL PROGRAMME

INFORMATION TECHNOLOGY AND SYSTEMS AUDIT

PP-IT&SA

TEST PAPERS

A Guide to CS Students

To enable the students in achieving their goal to become successful professionals, Institute has prepared a booklet 'A Guide to CS Students" providing the subject specific guidance on different papers and subjects contained in the ICSI curriculum. The booklet is available on ICSI website and students may down load from *http://www.icsi.edu/Portals/0/AGUIDETOCSSTUDENTS.pdf*

WARNING

It is brought to the notice of all students that use of any malpractice in Examination is misconduct as provided in the explanation to Regulation 27 and accordingly the registration of such students is liable to be cancelled or terminated. The text of regulation 27 is reproduced below for information:

"27. Suspension and cancellation of examination results or registration

In the event of any misconduct by a registered student or a candidate enrolled for any examination conducted by the Institute, the Council or the Committee concerned may suo motu or on receipt of a complaint, if it is satisfied that, the misconduct is proved after such investigation as it may deem necessary and after giving such student or candidate an opportunity to state his case, suspend or debar the person from appearing in any one or more examinations, cancel his examination result, or studentship registration, or debar him from future registration as a student, as the case may be.

Explanation - Misconduct for the purpose of this regulation shall mean and include behaviour in a disorderly manner in relation to the Institute or in or near an Examination premises/centre, breach of any regulation, condition, guideline or direction laid down by the Institute, malpractices with regard to postal or oral tuition or resorting to or attempting to resort to unfair means in connection with the writing of any examination conducted by the Institute".

PROFESSIONAL PROGRAMME

INFORMATION TECHNOLOGY AND SYSTEMS AUDIT

TEST PAPER 1

(This Test Paper is for recapitulate and practice for the students. Students need not to submit responses/answers to this test paper to the Institute.)

Time Allowed : 3 Hours *Maximum Marks : 100*

Question No 1 is compulsory and attempt 5 questions out of 6.

1. Ram is a Company Secretary and he has been working under the umbrella of Ram & Associates LLP with 10 other associates. The firm has got large information contained with all partners in a distributed way and in many cases, the partners faces the problem of extracting the correct information timely. The firm consulted an Information Management Consultant and it suggested them various ways i.e. Implementing Networking of Computers, segregation of data, digitizing all documents etc for managing the information. After implementing the measures, as suggested by the consultant, the firm observed remarkable improvement in information management. Now on the basis of above, answer following questions

   (a) What is the importance of Information for an organisation and what are the necessary attributes of information?

   (b) Why timely and proper extraction of information is necessary for the management?

   (c) Is information management a need or luxury? What are the ways other than explained above for information system management? *20 Marks*

2. (a) What do you mean by Decision support system? Is decision support system as same to executive information system? If no explain the difference *8 Marks*

   (b) What do you mean by data mining? Explain the various features of data mining *8 Marks*

3. (a) What do you mean by flow chart? Explain various symbols used in the preparation of Flow chart. *8 Marks*

   (b) Is the information requirement at all levels of management same? Explain in detail *8 Marks*

4. (a) What do you mean by Operating System? Explain its functions in detail. *8 Marks*

   (b) What do you mean by Programming? What are the different stages of programming? *8 Marks*

5. (a) Write a short note on Information technology Act, 2000 and its scope. *8 Marks*

   (b) Describe the composition and powers of Cyber appellate tribunal. 8 marks

6. What is database or database management systems (DBMS)? What's the difference between file and database? Can files qualify as a database? *16 Marks*

7. Who are the major players in ERP implementation? Explain two of them in detail. *16 Marks*

TEST PAPER 2

(This Test Paper is for recapitulate and practice for the students. Students need not to submit responses/answers to this test paper to the Institute.)

Time Allowed : 3 Hours *Maximum Marks : 100*

1. (a) ABC Limited has got its bank Account with XYZ Bank. ABC Limited wrote a letter to the bank and instructed the bank to transfer 5 crore rupees in the account of its one customer. Bank denied to transfer the money and asked ABC limited to transfer the amount via NEFT/RTGS/Cheque. On the basis of above, state whether XYZ limited is correct in denying the transfer of money on the basis of email instructions? If yes then why? (*10 marks*)

   (b) Who do you think is the controller of Certifying Authority? State his functions. (*10 marks*)

2. (a) What do you understand by a database? What are the characteristics of a database system? (*8 marks*)

   (b) State various functions of a database administrator (*8 marks*)

OR

2A. (a) What do you mean by E-governance? Explain various measures being taken by Indian government for promoting e-governance. (*8 marks*)

   (b) What do you mean by National Service Delivery Gateway (NSDG)? Explain its objectives. (*8 marks*)

3. (a) What do you mean by the term “CRM’? Explain the basic objectives of implementing CRM. (*8 marks*)

   (b) What do you mean by assembler and compiler? Differentiate between assembler, compiler and interpreter. (*8 marks*)

OR

3A. (a) What do you mean by e-commerce? State its various features. (*8 marks*)

   (b) What do you mean by Super computers? Explain the difference between Super computers and main frame computers. (*8 marks*)

4. (a) Explain the process of information gathering? Also explain the different characteristics of information. (*8 marks*)

   (b) Explain different functions of Management Information System in an organisation. (*8 marks*)

5. (a) what do you mean by term ‘Algorithm’? Explain the main characteristics of a good algorithm. (*8 marks*)

   (b) Explain the program development cycle in detail? (*8 marks*)

6. Write short note on the following:

   (a) Bluetooth Technology

   (b) Intranet

   (c) Flow Chart Symbols

   (d) Common service Centre (*4 marks each*)