# MANAGEMENT INFORMATION AND CONTROL SYSTEMS

## REVISION NOTES

*(To be used along with ICAI study material)*

Compiled by Rajeev NL

*e-mail: nlrajeev@gmail.com*

## TABLE OF CONTENTS

**Chapter 7 – System Development Process .....3**

**Chapter 8 – System Design.....8**

**Chapter 9 – System Acquisition, Software Development & Testing .....12**

**Chapter 10 – System Implementation & Maintenance .....16**

**Chapter 12 – Enterprise Resource Planning.....17**

**Chapter 15 – Detection of Computer Fraud .....20**

**Chapter 16 – Cyber Laws and IT Act, 2000.....24**

**Chapter 17 – Audit of Information Systems .....28**

**Chapter 18 – Information Security.....30**

**Chapter 1 – Basic Concept of System .....35**

**Chapter 2 – Transaction Processing System.....39**

**Chapter 3 – Basic Concepts of MIS.....40**

**Chapter 4 – System Approach and Decision Making.....43**

**Chapter 5 – Decision Support and EIS .....46**

**Chapter 6 – Enabling Technologies.....48**

# Chapter 7 – System Development Process

1. **System Development Life Cycle Consists of following Activities:** [M04, N04, N07] – *[to be written in the same order]* (ISD)[2]
    a. Preliminary **I**nvestigation
    b. Requirement analysis or **S**ystem analysis
    c. System **D**esign
    d. Acquisition or **D**evelopment of software
    e. **S**ystem Testing
    f. System **I**mplementation and Maintenance

2. **Why Organisation fail to achieve their system development objectives?** [N03] *[For each point answer why required, Consequence if not there]***(LSDN I ROLL)**
    a. Lack of Senior Management Support for and involvement in the information system development
    b. Shifting User Needs
    c. Development of Strategic Systems
    d. New Technologies
    e. Inadequate Testing and User Training
    f. Resistance to Change
    g. Overworked or Under-trained Development Staff
    h. Lack of User Participation
    i. Lack of Standard Project Management and System Development Methodology

3. **Approaches to System Development:**
    a. **Traditional Approach -** Phasewise Development, Activity in sequence, Proceed to next stage only after approval, more cost and time involved.
    b. **Prototyping approach** – [N02, M04, N07] – A Prototype is a system component that is built quickly and at lesser cost with an intention to modify or replace it by a full scale and fully operational system

    **Steps in Developing a Prototype:**
    - ✓ Identify Information System Requirements
    - ✓ Develop the initial Prototype
    - ✓ Test and Revise
    - ✓ Obtain User signoff of the approved prototype

**Advantages of Prototyping**

- ✓ Intensive involvement of system users.
- ✓ Development time is very short
- ✓ Error detection and elimination is at early stage of development process

**Disadvantages of Prototyping**

- ✓ Users not willing to spend time on development
- ✓ Sys Developers are tempted to minimize the testing and documentation process
- ✓ Causes behavioral problems with system users

c. **End User Approach** – End user responsible for system development. Risks involved are as follows:

- ✓ There will be a decline in standards and controls
- ✓ Inaccuracy of specification requirements
- ✓ Reduction in quality and system stability
- ✓ Increase in unrelated and incompatible system
- ✓ Difficulties in accessing

d. **Top Down Approach** – 1. Analyse the objectives and goals of organisation. 2. Based on objectives, identify the functions of org. 3. Based on functions, identify the activities, decisions and functions of the managers. 4. Based on activities and decisions, identify the models, nature and form of info required to help managerial decision making. 5. Prepare information processing programs in detail.

e. **Bottom Up approach** – 1. Identify Life Stream systems (LSS) i.e systems essential for day to day business. 2. For each LSS, identify Basic Transactions, Information file requirements and information processing programs. 3. Based on point 2, the information system is developed for each LSS. 4. The data files kept in each information system is integrated after thoroughly examining various application, files and records. This enhances shareablitiy and evolvability. 5. Decision models and planning models are added to support planning activities. 6. All these models are integrated to support higher management activities.

4. **Differences between Top-down and bottom up approach:** 1. Few people use-many people use. 2. Starts from Top mgmt – starts from mid and lower mgmt. 3. Org objects to transaction – Tran to Org objectives. 4. Developing time more- Developing time less. 5. Unstructured specification-structured specification. 6. e.g. EIS, MIS – e.g. TPS, AIS

5. **Reasons for Poor Project Management and IT project system failures [N06]: 1.** Under-estimation of Projects – (a) Time (b) Resources (c) Size and Scope. **2.** Inadequate a. Project Planning b. Project Control Mechanism. **3.** Changing System Specification. **4.** Senior mgmt not monitoring the project.

   **Following elements help proper Project management:**

   1.User Participation. 2. Assignment of staff and define their authorities and responsibilities 3. System's nature and scope. 4. Feasibility study. 5. System master plan, time and cost estimates. 5. Risk Management Program. 6. Dividing system in manageable process. 7. Approval at completion of each phase. 8. Quality Assurance plan.

6. **System development Methodology or SDLC:** formalized, standardized, documented set of activities used to manage a SDLC project. Characteristics are:
   a. Division of project into process. Division of process into several activities, one or more deliverables and magmt control points. Helps in project planning and control.
   b. The deliverables should be produced periodically to make system developers accountable for faithful execution of their tasks. Helps in documentation used for training purposes.
   c. Users, Managers and auditors should approve the completed parts at each control points. Helps maintain record that proper approval of development is obtained.
   d. System testing to be done before implementation
   e. Training plan to be developed for end users.
   f. Ensure security to prevent any changes to program codes.
   g. Post implementation review should be done to access the efficiency and effectiveness

7. **Preliminary Investigation – Objects of system analyst:** 1. First understand the project i.e. What is done now, what is required later and why, etc. 2. Determine the size of the project. Check if it a new project or modification of old system. 3. Determine technical and operational feasibility. 4. Conduct a cost-benefit analysis. 5. Report to the management whether the project can be taken up or not.
   a. **Methods of collecting data – Conducting investigation:**
      - ✓ Reviewing internal documents.
      - ✓ Conducting Interviews
   b. **Types of Project Feasibility: [TOESL]***(its like TOEFL)*
      - ✓ Technical Feasibility
      - ✓ Operational feasibility
      - ✓ Economic Feasibility
      - ✓ Schedule Feasibility
      - ✓ Legal Feasibility

c. **Estimating Costs and Benefits**

**Costs Include:**

- ✓ Development costs: salaries of designers and programmers, data conversion, data file preparation, buying computers, testing cost, documentation & training.
- ✓ Operating Costs: Rental charges of hardware and software, salaries to operators, system analysts, maintenance programmers, input data preparation, computer consumables, power, light, overheads, etc
- ✓ Intangible Costs

**Benefits Include:**

- ✓ Increase in sales, profits, efficiency, operational ability, productivity.
- ✓ Decrease in data processing costs, operating costs, required investments.
- ✓ Improved information availability, computation and analysis, customer service, employee morale, decision making, competitive position, etc.
- ✓ Intangible benefits

8. **Requirement analysis – Various Fact Finding Techniques [N05, N07]** – Documents, Questionnaires, Interviews, Observation

9. **Analysis of Present System – Areas to be studied: [M05, M08]***(Read this visualizing as if you are doing it, the steps are in specific order)(Remembering phrase: Analyse the model twice, to review 4 times b4 u undertake overall analysis – model can be anything u think☺)*
   a. Review Historical Aspects
   b. Analyse Inputs
   c. Analyse outputs
   d. Review Data files maintained
   e. Review methods, procedures and communications
   f. Review internal controls
   g. Model the existing physical system and logical system
   h. Undertake overall analysis of present system

10. **Major category of tools for system development**
    a. System Components and Flow – System Flow Chart, DFD's, System Component matrix.
    b. User Interface – Layout Forms and Screens, dialogue flow diagrams
    c. Data Attributes and Relationships – Data Dictionary, Layout forms and screens, Entity relationship diagrams.
    d. Detailed System Process – Decision Trees, Decision tables, Structure Charts.

**11. Few of the system development tools discussed:**

a. **Systems Flow Chart** – 1. It is a Graphic Diagramming tool. 2. Communicates the Flow of data media and information processing procedures in the information system. 3. Uses symbols and arrows.

b. **Data Flow Diagram (DFD)** – 1. It is a Graphic diagramming tool. 2. It describes the flow of data within an org. 3. Uses four elements (a) Data Sources and Destinations represented by ☐. (b) Data Flows represented by ↑. (c) Transformation Process represented by ○. (d) Data Stores represented by =. *(Write figure 3 of study material in the exam)*

c. **Layout Forms and Screens:** 1. Consists of electronic displays or preprinted forms. 2. Forms consists of titles, headings, data and information. 3. Used to design input and output screen displays. 4. Form designing requires 4GL packages and case tools.

d. **System Components Matrix:** 1. It views the information system as a matrix of components. 2. It highlights how control is established in inputs, process, output and storage. 3. Establishes how the use of hardware, software and human resource convert data into information products

e. **CASE Tools:** 1. CASE stands for Computer Aided Software Engineering. 2. These are used to generate System flow charts and data flow diagrams. 3. CASE refers to the automation of anything that humans do to develop systems. 4. Today, CASE products can support virtually all phases of traditional system development process.

f. **Data Dictionary [N02, M05, N07]:** The business information systems contains data items. The description of these data items are given in a computer file called data dictionary. DD contains the following:

- ✓ Codes *describing* the data item's length, data type, range - Description
- ✓ Identity of source document used to *create* the data item - Creation
- ✓ Names of computer files that *store* the data item - Storage
- ✓ Names of computer programs that modify the data item – Modification
- ✓ Details of permission to access the data item – Accessibility
- ✓ Details of persons not permitted to access – Non- Accessibility

**Uses:** 1. Serves as documentation aid to programmer. 2. Used in relation to file security by referring to the permissions. 3. Used by accountants and auditors. 4. Serves as aid in investigating or documenting internal control procedures.

# Chapter 8 – System Design

## 1. Designing System Outputs

### i. Important Factors in output Design [M04] [C TOM Full and Final]:

| | | |
|---|---|---|
| 1. Content | 2. Timeliness | 3.Output volume |
| 4. Media | 5. Format | 6.Form |

### ii. How to present the information?

#### i. Tabular Format

- Used when details dominate.
- Used when few narrative comment or explanations are needed.
- Details are presented in discrete categories, each labeled and totals are drawn or compared between components.
- Items to be included in tabular report are 1.Exception to normal expectations. 2.Major activities. 3.Summaries of major activities. 4.Unique Identification Information 5.Time dependent entities.

#### ii. Graphic Format

- They are superior to tabular format and information format of output display.
- Used mainly for management presentations
- Low cost powerful software's helps producing high quality charts and diagrams
- Used to improve effectiveness of output reporting, manage information volume, suit personal preferences.
- Comparisons can be made easily.
- Charts include pie charts, bar charts, etc.

**Standards in graphic design i.e what steps to be taken to design graphic output**

- System analysts should determine the purpose of the graph.
- The type of audience and the effect of graph on audience should be kept in mind.
- Graphic report should include title, date of preparation, page numbers, etc.
- Use of labels increases accuracy and readability. Abbreviations should not be used.
- Vertical and horizontal axes should be proportional.

iii. **Designing a printed output – guidelines in preparing layout form:**

- Readability from *left to right and from top to bottom*.
- Should enable the user to *find most important* items very easily.
- Should have *heading, title, page number, date of print, column headings*.
- There should be *heading for each data item*.
- There should be sufficient *margin*.
- There should be proper *page breaks and control breaks*
- Detail line for *variable data* should be defined.
- *Mock up reports* should be reviewed by users and programmers for usefulness, feasibility, readability, understandability, etc

iv. **Designing a visual display output – Layout of display screen** *(States that while designing the output on the screen, the following points to be kept in mind):*1.Physical dimensions of the screen. 2. Number of colors 3. Number of rows and columns. 4. Degree of resolution. 5. Methods of highlighting. 6. Methods of intensity control.

**2. Designing system inputs**

i. **Important factors in Input Design [C TIM Full]**

1. Content 2. Timeliness 3.Input volume
4. Media 5. Format

ii. **Form Design – Guidelines in form design**

i. Making forms easy to fill
   1. Form Flow
   2. Divide forms into logical sections
   3. Captioning
ii. Meeting the intended purpose
iii. Ensuring Accurate Completion
iv. Keeping forms attractive

iii. **Coding – Characteristics of good coding scheme [ M05] [I SPECS]**

i. Individuality – Uniqueness of the code
ii. Space – Should be brief than its description.
iii. Permanence – Should be used for ever, should not change with the circumstance
iv. Expandability – Flexible, future addition possible
v. Convenience - code to be short and simple
vi. Suggestiveness – Readily understandable

iv. **Coding – Types of coding schemes [N06][C**ash **F**low **S**tatement of **M**a**H**arashtra**]**

i. Classification Codes – Distinguishes one class from other like people, events, etc
ii. Function Codes – Codes based on activities or work
iii. Significant Digit Subset
iv. Mnemonic Codes
v. Hierarchical Classification

**3. Designing Efficient data entry :**

i. Quality Data input is required for quality data output hence efficient data entry is important
ii. Efficient data entry is achieved by attaining the following objectives: 1. Effective and efficient data capture 2. Effective coding 3. Appropriate data entry methods.

**4. Data Storage**

i. Data storage is an important decision in system design
ii. Two approaches in data storage – First, to store data in individual files i.e. one file for each application. Second, Store data in a database so that it can be used by many based on needs.
iii. First approach is conventional approach used where storage is application oriented. E.g.: Master files, table files, etc.
iv. Database approach is relevant where data needs to be entered, stored, retrieved, modified, etc.
v. Ways in which data can be organized in a storage medium under conventional approach: Sequential Organisation, random or direct organisation, indexed organisation, indexed-sequential organisation
vi. A database approach is used where data needs to support management decision making.
vii. System analysts should work with DBA to determine the storage, retrieval and conversion methods of data.

**5. System Manual – Contents of System Manual [NO03, M07]:** It is prepared together by analysts, designers, management, users, etc.(remember this dialogue: "**G**irl **F**riend, **O G**irl **F**riend, **I, I, L**oved **O**nly **O**nce, **M**arried, **L**eft **T**hen **S**earched **A**nother **G**irl")

i. General description of existing system
ii. Flow of existing system
iii. Output layout of existing system
iv. General description of new system
v. Flow of new system

vi. Input layout
vii. Input Responsibility
viii. List of files to be maintained
ix. Output Layout
x. Output Distribution
xi. Macro logic of the flow in the system
xii. List of Programs to be written
xiii. Timing estimates
xiv. System operation Controls
xv. Audit Trial
xvi. Glossary of terms used

6. **Reporting to management after finishing system design:** The report should include:
   i. *Description* of the application and *users source* that led to the system
   ii. A *summary* of the results of the requirement analysis
   iii. Design *recommendation*
   iv. Any *changes* made to cost benefit analysis of new system
   v. A *plan* for remaining system development activities

# Chapter 9 – System Acquisition, Software Development & Testing

1. **Considerations in procuring Computer System[M06]**
   a. Most Recent Computer, Latest Technology, Better performance, lower cost
   b. Speed and good capability of input, output and Storage facility.
   c. Consideration of name of the manufacturer and software compatibility with the system that needs to be procured.
   d. Decide as to the system should be a server or a backup device or a central processor. Whole model to be designed based on long range expansion plan and investment.
   e. Selection of system configuration and plan for its gradual expansion.

2. **Software Acquisition –Whether to Make or Buy software [M03]:** This decision is made after the following process:
   1. First finalise the input and output design. Then assess the nature of application software required for the input and output design.
   2. This helps to decide
      a. the type of application software to be used
      b. the degree of processing that the system needs to handle
      c. the type of system software to be procured for the application software
      d. the type of hardware to be procured for the application software.
   3. Then the system developers should determine whether the application software should be created in-house or acquired from vendor.

3. **Advantages of Pre-Written Application Packages** *(for each point compare the related merits or demerits if application packages were developed in-house)*
   1. Rapid Implementation
   2. Low Risk
   3. Quality
   4. Cost

4. **Sources of Packaged Software:** Computer manufacturers, large and small software houses and computer retail stores, user groups, association of users, etc.

5. **Steps in selecting a computer system: [N07]** Imagine you are given the task to select a computer system by your boss, you should proceed in the following manner:
   1. First prepare the design specification required
   2. Then prepare a RFP (Request for proposal) containing the specifications required and distribute it to selected vendors.
   3. Once you receive the proposal from vendors, compare and eliminate inferior vendors.
   4. Negotiate with the remaining vendors and ask them to present revised proposal.
   5. Conduct further analysis of proposal.

6. Contact present users of proposed system
7. Conduct equipment benchmark test to check if the configuration proposed by the vendor is reaching the required benchmark established by the company.
8. Select the Computer System.

**6. Points considered for validating a vendor's proposal [M05]** *(Physics Chemistry Maths Computer Science – PCMCS)*

1. The ***P****erformance* capability of each proposed system in relation to its costs
2. The ***C****osts and benefits* of each proposed system.
3. The ***M****aintainability* of each proposed system
4. The ***C****ompatibility* of each proposed system with existing system
5. Vendor ***S****upport*

**7. Methods of validating a vendor's proposal**

**A. Checklist:**

- ✓ It is the most simple and subjective method to validate a vendor's proposal.
- ✓ Various selection criteria are put in the form of questionnaire and response are validated.
- ✓ The vendor giving the best response is selected.

There are many types of checklist, two of which are as below:

i. **Software Validation Checklist** – This checklist is used to assess the capabilities of or evaluate the performance of packaged software. The following questions are to be answered in the checklist: **[3C-3D-FHL-4M-2O-P-3T]**

- ✓Cost
- ✓Control
- ✓Capacity
- ✓Design
- ✓Developed
- ✓Documentation
- ✓Formats
- ✓Hardware Compatibility
- ✓Language of software
- ✓Modification – Is it required?
- ✓ Modification – Can it be done
- ✓ Modification – Who will do it?
- ✓ Maintenance – Who will do it?
- ✓ Organisation of package
- ✓ Operation of package
- ✓ Processing time by software
- ✓ Techniques the software use
- ✓ Training required for software
- ✓ Transactions – how many processed

ii. **Vendor's Support Service Checklist- [**System Developments Hardware Software Maintenance Back's Up Conversion of Training into Performance with Proximity]

**B. Point Scoring Analysis [N03]**

a. Important tool to validate vendor's proposal.

b. A proposal evaluation committee prepares a set of software evaluation criteria.

c. The criteria's are analysed with the proposal sent by various vendors.

d. A fixed number of points are assigned to each evaluation criteria and on evaluation, the vendor is given points for each criteria based on how much he meets the required criteria.

e. The points given for all the criteria are totaled and the vendor scoring highest point is selected.

f. Many experts feel that this tool is more of art than a science involved in evaluation.

g. There are no absolute rules in selection process. Only guidelines for matching user needs with software capabilities are available.

**C. Public Evaluation Reports:** 1. Consultancy agencies do a Public Evaluation of various manufacturers in hardware and software and publish their reports. 2. Many buyers who has inadequate computer knowledge resort to this method. 3. This evaluation will only resolve particular criteria's of buyer. Other criteria have to be evaluated by other means of evaluation

**8. Bench Marking problems for vendors proposal [N06]**

a. These are *sample programs* designed to test *software and hardware consideration* of whether the computer offered by the vendor *meets the requirement of the job on hand* of the buyer.

b. Computers are required to be procured *based on the job mix* of the buyer. Thus, these programs are successful only if *job mix has been clearly specified*.

c. Bench marking problems include long jobs, short jobs, tape jobs, disk jobs, mathematical problems, etc in proportion to the job mix.

d. If the job is truly represented by selected benchmarking problems, these programs can provide realistic and tangible basis for comparing vendors.

e. The disadvantage is that it takes considerable time and effort to select problems representative of job mix. It also requires operational hardware, software and service of systems.

f. This approach is very as it can test the functioning of vendor's proposal.

**9. Steps or stages in In-house software development [N05, M07]**

1. *Program Analysis* – Ascertaining outputs required, inputs available, processing aspects.
2. *Program Design* – Deciding on programs structure, input and output layout, file layout, etc.
3. *Program Coding* – Drawing up the program logic and syntax. Syntax means vocabulary, punctuation and grammatical rules available in the language manuals. Coding is written in special sheets. Programmers should meet 3 objectives in coding: Simplicity, efficient utilization of storage space, least processing time. Programs to be flexible future modification.

4. *Debug the Program*-Debugging means correcting the program syntax and errors. Has 4 steps: Inputting source program to complier, Letting compiler find errors in the program, correcting lines of code that are in error, resubmitting the corrected code to the complier.
   - ✓ Use Structured Walkthrough
   - ✓ Test the program
   - ✓ Review the program code for adherence to standards
5. Program documentation
6. Program Maintenance

**10. Program Design Tools [M04, N07]**

1. Program Flow Chart-Graphical representation of program logic
2. Pseudo Code – It presents program logic in English like statements.
3. Structure Chart – Organises each of program tasks into well defined modules.
4. 4GL Tools – Ensures completion of program design in short time, maintains consistency in program logic.
5. Object oriented programming and design tools – Used for enhancing programming productivity and to reduce application backlogs in many organisation. Object oriented design is often taken from a DFD.

**11. System Testing**

a. Conducted prior to installation of information system
b. It involves the following:
   i. *Preparing* realistic test data in accordance with the system plan.
   ii. *Processing* test data in the new equipment
   iii. *Checking* the results of test data after processing is done.
   iv. *Reviewing* the results with future users, operators and support personnel.
c. *System level testing* is done by conducting parallel processing with existing system and the results given by both the system is anlysed.
d. If the system is a *interactive processing system*, testing is done by having several input terminals connected on line and operated by the supervisory personnel backed up by the personnel operating the old system. The output is checked for compatibility and appropriate corrections are made to online computer programs.
e. *Those responsible for comparing* the old and new systems should establish that the remaining deficiencies are caused by the old system. A poor checking job can result in complaints from top management and other users of the system.

# Chapter 10 – System Implementation & Maintenance

1. **Activities involved in equipment installation**
   a. Site Preparation – Space, temperature, lighting, electric lines, air conditioning, etc.
   b. Equipment Installation – Equipment is Physically installed, connected to power, etc.
   c. Equipment Checkout – Equipment is turned on and tested, diagnostic and extensive tests.

2. **Training Personnel [M03, N06] -**
   a. Training system operators
   b. Training System Users
3. **Conversion or Changeover from Manual to Computer System [M03, N03, N06]**
   a. **Conversion Strategies**
      i. Direct Changeover
      ii. Parallel Conversion
      iii. Gradual Conversion
      iv. Modular prototype conversion
      v. Distributed Conversion
   b. **Activities involved in conversion [M05, N07}**
      i. Procedure Conversion
      ii. File Conversion
      iii. System Conversion
      iv. Scheduling personnel and equipment
      v. Alternative plans in case of equipment failure

4. **Evaluation of New System [N04]**
   a. *Development Evaluation* – Checking if development was within Time Schedule & Budget.
   b. *Operational Evaluation* – Timely processing, accuracy, ease of use, response time, reports, storage capacity
   c. *Information Evaluation* – Quantitative and qualitative – Decision system, meet the information need of usual decision makers. Measure user satisfaction thru interviews, questionnaire, etc.

5. **System Maintenance [N02, N05, M07]** – 1. This starts after the new system is being used. 2. This is required to meet the changing organizational needs. 3. It involves adding new data elements, modifying reports, adding new reports, changing calculations, etc. 4. Two ways of maintenance:
   a. Scheduled Maintenance – Anticipated and planned for.
   b. Rescue maintenance – refers to undetected malfunctions that are unanticipated.

# Chapter 12 – Enterprise Resource Planning

**A. ERP – Definition – [N02, N03, N07]** – It is a fully integrated business management system covering functional areas of an enterprise like logistics, production, finance, HR, etc. It organizes and integrates operation processes and information flows to make optimum use of resources such as men, material, mone and machine. It is a global, tightly integrated closed loop business solution package and is multifaceted.

**B. ERP – Evolution** –

1. *Factors leading to evolution*: industry wants like cost control, cost analysis, revenue analysis, flexibility to respond to changing business needs, decision making.
2. *Stages of Evolution*: Material Requirement Planning (MRP) systems -> Manufacturing Requirement Planning (MRP II) –> ERP.
3. ERP as the name indicates is the integration of enterprise resources.

**C. ERP – Characteristics [M05]**

1. Flexible
2. Modular
3. Comprehensive
4. Beyond the company
5. Best business practice

**D. ERP – Features [M05]**

1. Has *Multiplatform, multi-facility, multi mode manufacturing, multi currency, multi lingual* facility.
2. Has end to end *supply chain management*
3. Supports and integrates *strategic, operational and business planning* activities.
4. Supports Better *Project Management*
5. Provides for automatic introduction of *latest technology.*
6. Provides intelligent business tools like DSS, EIS, data mining, etc.
7. Provides *Company-wide integrated functional system* covering all functions like finance, stock, etc
8. Provides *integrated functional systems* across companies.
9. *Bridges information gap* across organisations.
10. Performs *core activities* and increases customer services
11. Eliminates most *business problems* like material shortage, cash management, cust service, etc

**E. ERP – Benefits**

1. Improves Control, reporting standards, accuracy, presentation, cost control, efficient cash collection, flexibility to business changes, supply-demand linkage across branches in countries, information access.

2. Reduces paper work
3. Timeliness, faster customer response and follow up, better monitoring, quick solutions to queries, achieve competitive advantage, unified customer database, supports variety of tax structures

**F. Business Process Reengineering[N04] –** The following is involved:

1. A business process in the organisation is taken up and studied.
2. After study, the process is divided into necessary and unnecessary process.
3. All unnecessary processes are eliminated.
4. This is called Business Process Reengineering wherein you redesign/reengineer the existing process.
5. BPR can be defined as the fundamental rethinking and radical redesign of processes to achieve dramatic improvement in critical, contemporary measures of performance such as quality, services, etc.
6. It needs complete rethinking and eliminates unnecessary process to improve quality, time, and customer satisfaction.
7. This can be achieved through optimal cost, quick deliveries and eliminating paper based communications.

**G. Methodology used in implementation of ERP:**

1. Identifying the needs for implementing the ERP package.
2. Evaluating the "as is" situation of the business.
3. Deciding the "would be" situation of the business.
4. Reengineering the existing business process to achieve the desired results.
5. Evaluate various ERP packages available in the market to assess suitability.
6. Finalise the best ERP package for implementation.
7. Install the required hardware and networks for the selected ERP package.
8. Finalise the consultants who will assist in ERP implementation.
9. Implement the ERP package.

**H. Guidelines in implementation of ERP** – Check for the following *before implementing* ERP to structure the ERP accordingly:

1. Corporate Needs and culture.
2. Business Process Redesign exercise
3. Efficient, Strong and effective leadership
4. Efficient and capable project manager
5. Good Team of implementation consultants
6. Good Communication network across organisation
7. Good Implementation Methodology
8. Training end users – after implementation

9. Adapting new system and making required changes.

**I. Post Implementation**

1. *Expectations from ERP*: Improved Process, Increased productivity, total automation and less manual intervention, improved key performance indicators, no manual records, real time information systems, total operation integration. *(This is same as benefits of ERP)*
2. *Fear in ERP*:
   i. Individual fear - Job redundancy, change in job profile, loss of importance, increased stress due to more transparency,
   ii. Organisational fear – Loss of control and authorisation.

**J. Realities that organisation should consider before ERP implementation:**

1. Changing organisation involves 3 leavers – strategic, business process and change and consequential organisation change.
2. Changing organisation requires mindset change.
3. Process related KPI is not measured in most companies in India.
4. The genetic nature of ERP packages is such that there would be processes peculiar to some sectors and organisations which may be kept out of such processes.
5. Some of the processes can be done better manually

**K. Life after Implementation** – Tasks to be performed after implementation are as follows:

1. New job description and organisation structure
2. Determine skill gap between existing and envisioned jobs
3. Assess training requirements and create and implement the training plan.
4. Develop and amend HR, financial and operational policies to suit the ERP environment.
5. Develop a plan for workforce logistics adjustment.

**L. Sample List of ERP vendors**

1. BAAN (The Baan Company)
2. BPCS
3. Mapics XA – Marcam corporation
4. MFG/Pro - QAD
5. Oracle Applications – Oracle corporation
6. Prism - Marcam Corporation
7. R/3 – SAP
8. System 21 - JBA

# Chapter 15 – Detection of Computer Fraud

**A. Computer Fraud – Definition and Inclusions** – it is defined as "using a computer to cause prejudice, in the sense of financial and/or reputational damage to a business". It includes the following:

1. Clearly Recognisable Frauds – Investment frauds, secret market fauds, pyramid schemes
2. Hacking
3. Manipulation of Computer Systems to obtain money from an employer or a third party.
4. Theft or destruction of confidential information
5. Abuse of computer systems by employees
6. Software Piracy

**B. Why should business take Computer Fraud seriously and assess security needs? [N03, M05]**

1. No Computers, no business.
2. No computer networks, no usage of recent trends like e-payment, e-order booking, etc
3. Growth in e-Commerce leads to more internet business and thus more hacking risk
4. Growth in e-Cash leads to loss, theft or destruction of e-receipts at the time of transmission.
5. Computer Fraud is far dangerous than conventional Fraud because:
    a. It can be easily hidden and is hard to detect
    b. Collection of evidence of fraud is not easy and even if collected is difficult to produce in the court.
    c. Fraud is committed in many ways that:
        i. it involves manipulation of invisible data
        ii. it may involve only few key stokes
        iii. computers used in business can be accessed from remote regions
        iv. Huge business data can be copied and taken away in CD, Flash Drives, etc.

**C. Computer Fraud – Internal Threats [M04, N06, N07]-[I DOM**inate **PC]**

1. Input – Collusive Frauds, Disbursement Frauds, Payroll Frauds, Cash Receipts Fraud.
2. Data
3. Output
4. Malicious alterations of e-mail
5. Processors
6. Computer Instructions

**D. Computer Fraud – External Threats**

1. Removal of Information
2. Destruction of System Integrity

3. Interference with web pages
4. Transmission of viruses by emails
5. Interception of emails
6. Interception of electronic payments

**E. Internet Frauds – Characteristics of internet that attracts fraud to be committed:**

1. Internet site – no regulation for Setting up, no license fee payable to government.
2. Internet Site – set up anywhere in the world and at low cost.
3. Internet Site – Impressive sites having links to big companies trap innocent customers.
4. The credibility gained by the site will influence prudent investors to commit fraud.
5. The victim of fraud and the committer of fraud stay at different legal jurisdictions.

**F. Reasons for increase in Computer Fraud**

1. Not everyone agrees of what is a computer fraud
2. Fraud goes undetected
3. Even if detected, it goes unreported.
4. Even if reported, it is difficult to prove it.
5. Low level of security
6. Internet itself contains information as to how to commit fraud
7. Cyber crime department is not able to cope up with the increase in computer fraud.

**G. Computer Fraud and Abuse Techniques**

Please refer to ICAI Study material.

**H. Measures to be taken to prevent computer frauds**

1. Make fraud less likely to occur
2. Use proper hiring and firing practices
3. Manage disgruntled employees
4. Train employees in security and fraud prevention measures as follows:
   a. Security Measures
   b. Telephone Disclosures
   c. Fraud Awareness
   d. Ethical Considerations
   e. Punishment for unethical behaviour
   f. Educating employees
   g. Manage and Track software license
   h. Have signed confidentiality agreements

**I. How to increase the difficulty of committing fraud? [DERRS PC PC]**

1. *Develop* a strong system of internal control
2. *Encrypt* data and programs
3. *Require* Vacation and rotation of duties
4. *Restrict* access to computer equipment and data files
5. *Segregate* Duties
6. *Protect* Telephone Lines
7. *Protect* System from Viruses
8. *Control* Sensitive data
9. *Control* Laptop Computers

**J. Steps or Methods to detect computer frauds**

1. Conduct frequent audits
2. Use a computer security officer
3. Use computer consultants
4. Monitor System Activities
5. Use Fraud detection software

**K. Reducing losses caused by Frauds**

1. Insurance
2. Backup of programs and data
3. Contingency plans
4. Special fraud prevention software's

**L. Disk Imaging and Analysis Technique (DIAT) [M03, N05]**

1. Used by fraud investigator to collect evidence of fraud committed by the perpetrator has thought are inaccessible.
2. Example of such evidence may be a word document showing stagewise creation of blackmail letter, forged invoice, confidential e-mails or passwords sent, etc.
3. The stages involved in DIAT is as follows:
   a. *Duplication of Hard disk:*
      i. Investigator uses special hardware and software resources to take a copy of hard disk.
      ii. The imaging hardware is attached to parallel port of the computer. Then using imaging software an exact copy of hard disk is taken without using the computers operating system.
      iii. No clue of this activity is left in the system thereby not alerting the fraudster.
   b. *Recovery of file from disk image:*
      i. When files are deleted, they are not actually removed from the hard disk. Only the reference to that file is removed from the file allocation table.

ii. Any new program saved is overwritten on the space for which file allocation is removed.

iii. So the part of files on which space the programs are not written is recovered by the special processing software.

c. *Analysis of the processed image:*

i. Search software is used to analyse the processed image to find references to suspect transactions.

ii. The search is across all text on the disk so that the files, which the suspect thinks have been destroyed and data which he may well have no idea was being retained, are searched.

**M. From where the information stored can be recovered under DIAT?** *(Fixed Deposit LIST)*

1. **F**ree Space
2. **D**eleted files
3. **L**ost Chains
4. **I**nternet Cache files or temporary internet files
5. **S**lack Space
6. **T**he contents of windows SWAP file

# Chapter 16 – Cyber Laws and IT Act, 2000

## A. Objectives of the Act [M05, N07]

1. to grant Legal Recognition to *Transactions* carried on by means of *EDI and e-commerce*
2. to grant Legal Recognition to *Digital Signatures* for authentication of Information
3. to grant Legal Recognition to *Books of accounts of bankers* kept in electronic form.
4. to grant Legal Recognition to *Electronic Fund Transfers* between banks and FI's.
5. to facilitate *e-Filing* of documents with government departments
6. to facilitate *e-Storage* of data
7. to amend *Indian Penal Code, Indian evidence Act, 1872, The Banker's Book evidence Act, 1891 and Reserve Bank of India Act, 1934.*

## B. Non-Applicability of the Act [M03]

1. Negotiable Instrument – Negotiable Instruments Act, 1881
2. Power of Attorney – Powers of Attorney Act, 1882
3. Trust – Indian Trust Act, 1882
4. Will – Indian Succession Act, 19225
5. Contract for sale of Immovable Property or any interest in such property
6. Others as specified in Official Gazettee

## C. Definitions

Please refer to ICAI study material for the definitions

## D. How Digital Signature is affixed to Electronic Records? (Sec 3) [N02]

1. It takes 2 steps to create a Digital Signature:
   *Step 1*: e-Record is converted to a *message digest* using *hash function* which is a mathematical function. Hash Function digitally freezes the data to maintain data integrity. Any tampering with data would immediately invalidate digital signature.
   *Step 2*: A private key, which is used to identify the person affixing the digital signature, attaches itself to the message digest. The identity of the person is verified by others using a public key and also to ensure that the e-Record in not tampered.
2. Hash Function is an algorithm mapping i.e translation of one sequence of bits into another smaller set known as Hash Result such that the e-Record gives the same Hash Result when hash function is executed. Hash function thus helps in the following:
   a. The original record can't be derived from the hash result produced by hash function.
   b. No two e-Records can produce the same Hash Result.

**E. Note on e-Governance:** e-Governance deals with the fact as to how the documents can be filed electronically.

1. Sec 4 – Legal Recognition to *e-Record maintenance*
2. Sec 5 – Legal recognition to *authenticate e-Records* using digital signatures
3. Sec 6 – Legal recognition to *e-Transactions* like filing of forms, applications. Creation, retention or preservation, grant, etc of records, licenses, etc in electronic form.
4. Sec 7 – Legal recognition to retain documents in electronic form on certain conditions.
5. Sec 8 – Legal recognition to publish govt documents like rules, regulations, etc in e-form.

**F. Power of Central Government to make rules:** w.r.t digital signature the govt can specify:

1. Type of DS
2. Manner and format of affixing DS
3. Manner and Procedure for identification of person affixing DS.
4. Controls, process and procedure for integrity, security and confidentiality of e-Records.
5. Any other matter

**G. Duties of Certifying Authorities [N02, N05, N07]**

1. With respect to digital signatures:
   a. Secure hardware, software and procedures from intrusion and misuse.
   b. Reliability in services
   c. Adhere to security procedures.
   d. Observe rules and regulations.
2. Ensure that his employees comply with the provisions of the act, rule and regulations.
3. Display his license at conspicuous places.
4. Disclose his digital signature certificate.

**H. Issuance and suspension of Digital Signature Certificate (Sec 35 to 40)**

1. **Issuance:** Application in Prescribed form. Fees not exceeding Rs.25,000. Fee paid to central govt. Conditions for granting DSC: 1. Private key is corresponding to public key which is listed in DSC. 2. Private key can create a DS. 3. Public Key can be used to verify DS.
2. **Suspension:** 1. Done only in public interest. 2. Opportunity of being heard is given. 3. Suspension should not to exceed 15 days. 4. Certifying authority to publish notice of suspension.

**I. Damage to computer, Computer System or network:** It includes the following

1. Securing Access
2. Introducing computer contaminant or virus
3. Downloading or extracting
4. Damaging
5. Disrupting
6. Denying access to authorised
7. Providing assistance to unauthorised access
8. Charging Services availed by one to the account of another.

Refer study material for the definitions of Computer Contaminant, computer database, computer virus and damage.

**J. Cyber Regulation Appellate Tribunal - CRAT**

1. CRAT has appellate powers in respect of orders passed by any adjudicating officer.
2. It consists of a presiding officer appointed by notification by the central govt.
   a. *Qualification*: High court Judge or member of Indian Legal Service in the post in Grade I for at least 3 years.
   b. *Term*: 5 years or 65 years age which ever earlier.

**K. Powers and procedures of Appellate Tribunal [M06, N06]**

***Powers***

1. Summoning and enforcing attendance of person and examining him on oath.
2. Production of documents
3. Receiving evidence on affidavits
4. Reviewing its decisions
5. Issuing commissions for examination of witness, etc

***Procedures***

1. The appellant can appear in person or thru legal representative to present his case.
2. The appeals should be filed within the prescribed time.
3. An officer can take up only cases which are in his jurisdiction.

**L. Power of Central Government to make rules [M04]:** The CG can exercise their powers in the following:

1. Manner in which a *document can be authenticated* by digital signature
2. Manner and Format of *filing e-records*.
3. Manner and Format and Type of *digital signature*.
4. Period of *license validity*.
5. *Security Procedure* for creating e-records and digital signature.

6. *Controller* - Qualification, experience and terms of service.
7. *Adjudicating Officer* - Qualification, experience and terms of service.
8. *Presiding Officer* – Salary, allowances and terms of service

**M. Offences under the Act**

| Sec | Offence | Penalty/Jail/Both |
|---|---|---|
| 65 | Tampering Source Documents | 2 Lakhs/3 Yrs / Both |
| 66 | Hacking | |
| 68 | Controller ordering to cease business activities | |
| 69 | Controller ordering to intercept | |
| 67 | Publishing obscene information: 1st Time<br>2nd Time | 1 Lakh / 5 yrs /Both<br>2 Lakhs / 10 yrs / Both |
| 70 | Unauthorised access of secure computer systems | 10 Years |
| 71 | Misrepresentation | 1 Lakh / 2yrs /Both |
| 72 | Breach of confidentiality | |
| 73 | Publishing false digital certificate | |
| 74 | Fraudulent publication | |

**N. Power of Controller to make regulations [M07]:** The regulations include the following:

1. *Maintenance of data base* containing the disclosure record of every certifying authority.
2. Conditions subject to which the controller may *recognise foreign certifying authority*.
3. Conditions and terms subject to which *license is granted* to certifying authority.
4. *Standards* to be observed by Certifying Authority.
5. *Manner of disclosures* to be made by Certifying Authority.
6. *Particulars* to be submitted along with application by the Certifying Authority.
7. Manner in which the *subscriber* should *communicate the compromise of private key* to the certifying authority.

**O. Matters not considered by Information Technology Act**

1. Protection of *domain names*
2. Infringement of *copyright* laws
3. *Jurisdiction* aspect of e-Contracts
4. *Stamp Duty* aspect of e-Contracts
5. *Taxation* of goods and services traded through e-Commerce

# Chapter 17 – Audit of Information Systems

**A. Functions of a Information Sys auditor/Auditing Concerns: (APTECH CS CABADI)[M03]**

1. Audit Trial
2. Performance
3. Training
4. Evaluation Criteria
5. Controls
6. Handling exceptions & Rejections
7. Control over changes
8. Security
9. Compatibility
10. Accounting and data integrity
11. Backup and Recovery
12. Authorisation
13. DB design and control
14. Implementation

**B. Manual Audits prove ineffective in many IS audits because of following (TEAR New)[N05]**

1. Terminology
2. Electronic evidence
3. Automated Processes
4. Reliance on controls
5. New Risks and Controls

**C. Scope and Objectives of IS audit [N03, N05, N07]** ***(C MICS)***

1. Computerised systems and applications
2. Management of Information systems
3. Information Processing Facilities
4. Client Server, Telecommunication and Intranet
5. Systems Development

**D. Objectives/Role of an IS auditor [N03, N05, N07]**

1. Unauthorised access, modification, etc – Security Provision
2. Program development and acquisition – Management authorisation
3. Program modification – Management authorisation
4. Processing of Transactions, files, reports – accurate and complete
5. Computer data files - accurate and complete and confidential
6. Inaccurate source data – handled properly

**E. Computer Security shows the following:**

1. Types of security errors and frauds faced by the company
2. Control Procedures to minimise security errors and fraud
3. Systems Review audit procedure
4. Test of Control audit procedures
5. Compensating Controls

**F. Concurrent Audit Techniques – Meaning and types:** These are the techniques used by IS auditor to continuously monitor the system and collect audit evidence while live data is processed. They are as follows:

1. Integrated Test Facility
2. Snapshot Technique
3. SCARF
4. Audit Hooks
5. Continuous and intermittent simulation

**G. Software Programs used to analyse the program logic:** Using the following you can analyse the logic written in a program:

1. Automated Flowcharting Program
2. Automated Decision Table Program
3. Scanning Routines
4. Mapping Programs
5. Program Tracing

**H. For all framework, refer to the study material.**

# Chapter 18 – Information Security

**A. Importance of Information Security (M04, N07)**

1. Information which is accurate, complete, valid and timely is always required for the organisations growth. Loss of information to the competitor would endanger the very existence of business. Thus there are certain risks associated with information due to:
   a. Reach of Technology
   b. Growth of technology
   c. System interconnectivity
   d. Elimination of constraints in time distance and space
   e. Devolution of management and control
   f. Electronic attacks over the system
   g. External factors like statutory and regulatory requirements
2. Security failures results in financial and other losses like disclosure of competitive price sensitive information
3. Threats can be intentional, non-intentional, internal, external, technical lapse, natural disasters, etc
4. Hence securing the information is important for any organisation.

**B. Meaning of Information Security [M04, N07]**

1. Security means protection of valuable assets from loss, disclosure and damage.
2. Such valuable assets should be secured by way of locks, perimeter fences and insurance.
3. In case of information, security should also include logical and technical safeguards like passwords, firewalls, etc
4. Even after such safeguards, if there is a security breach, the security policies and procedures should be reassessed.
5. Security objective is met when there is:
   i. Information availability
   ii. Confidentiality
   iii. Integrity

**C. Sensitive Information:** You can find sensitive information in the following:

1. Strategic Plans – Business plans, R&D, marketing decision, , etc.
2. Business Operations – Competition, pricing, quality, production, etc.
3. Finances – Financial statements, salaries, product costs, etc.

**D. Protecting the critical information is crucial. Why?**

1. Not all data has the same value
2. Know where the critical data resides
3. Develop an access control methodology
4. Protect Information Stored on media
5. Review hardcopy output

**E. Principles of Information Security [N02, N03, M05] (MICS RAAT) or (AMIT'S CA$^2$R)**

1. Multidisciplinary–Security requirement must consider both technical and non technical issues
2. Integration – Security must be coordinated and integrated
3. Cost effectiveness – Security must be cost effective
4. Societal factors – Ethics must be promoted by respecting the rights and interests of others
5. Reassessment – Security must be reassessed periodically
6. Accountability – Accountability and responsibility should be explicit
7. Awareness – Awareness of risks and security initiatives must be disseminated
8. Timeliness – Security procedures must provide for monitoring and timely response

**F. Ground Rules for Protection of Computer held information**

*Rule # 1* – We need to know what the information is and where is it located?

*Rule # 2* – We need to know the value of information held and how difficult it would be to recreate if it is damaged or lost

*Rule # 3* – We need to know who is authorised to access the information and what they are permitted to do with the information.

*Rule # 4* – We need to know how quickly information needs to be made available in case of loss or modification of the same.

**Types of information protection**

**A. Preventative Information Protection**

a. Preventive information protection is a method whereby security controls are installed to protect information.

b. Security control may be logical (passwords, file permissions, access control lists, power protection programs) , physical (access control doors, security guards, disk locks, paper shredders, etc) or administrative controls (Security Awareness, Security policies, etc)

c. These control are made mandatory thru Company's security polices and standards.

**B. Restorative Information Protection [N06]:**

a. There are certain events which lead to loss of valuable and sensitive information.

b. If the information is not recovered in time, the entity may go out of business.

c. Restorative information protection helps to retrieve or recover such lost information.

d. This is achieved by timely and effective planning of backup and recovery system.

e. It should not only cover information backup, but also the system backup because there may be no use of information without the system.

f. Restorative information protection should answer the following questions:

i. Has the recovery process been tested recently?

ii. How long did it take?

iii. How much productivity was lost?

iv. Did everything go according to the plan?

v. How much extra time was needed to input the data changes since the last backup?

**C. Holistic Protection [M07]:**

a. It is not an easy task to protect the information.

b. Protection should be done on a holistically keeping the mind the acceptability of cost involved in such protection.

c. The protection program should be ready for the unknown, expect the unexpected and should recover very fast from such disasters.

**G. Contents of Information Security Policy [M06, N07]:** In relation to the information security policy, the statement should contain; *(C BRASIL VISA SP 4 Security )*

1. Communication security
2. Business continuity plan
3. Reporting responsibilities and procedures.
4. Asset classification
5. System development and maintenance life cycle requirements

6. Its Importance
7. Legal, regulatory and contractual requirements
8. Violation enforcement provision
9. Issue specific areas
10. Statement on Information security from CEO
11. Accountabilities and Responsibilities
12. Standards and Compliance requirements
13. Physical, logical and administrative security
14. Security of data
15. Security of person
16. Security awareness, training and education
17. Security breach detection and reporting requirements

**H. Roles and Responsibilities to include the following**

1. Executive Management
2. IS Security Professionals
3. Data Owners
4. Process Owners
5. Technology Providers
6. Users
7. IS Auditors

**I. Implementation:** On implementation the security standards, measures, practices etc should include the following: **(MLC IS BCAP)**

1. Managerial Controls
2. Logical access controls
3. Cryptography
4. Identification and authentication controls
5. SDLC Process controls
6. Business continuity planning controls
7. Computer support and operations controls
8. Accountability controls
9. Physical and environmental controls

**J. Monitoring :**

Actions that result from monitoring process:

1. disciplinary or corrective action
2. minimisation and recovery of losses
3. refinement of security levels
4. changes to policy or standards
5. changes to design and implementation of security
6. initiation of re-assessment programs including root cause and pattern analysis
7. initiation of intelligent monitoring systems with interactive feedback

Issues that need to be addressed ***for effective monitoring*** include the following*:*

1. Appointment of responsible managers with adequate tools and resources
2. Independent and objective assessment of security controls like security audits
3. Clear and expedient investigative procedures
4. Examination of management audit trial information
5. Timeliness of escalation processes
6. Dynamic and ever changing business environment

**K. Awareness, Training and Education:** *Security awareness is communicated* in the following ways

1. Security policies on notice board
2. Security policies in freqtly visited areas
3. Training the staff
4. Non-disclosure statements
5. Company newsletter
6. Visible enforcement of security rules
7. Periodic audits
8. Conduct fake security incident.

**L. Role of security Administrator [M03]**

1. Information safety from threats
2. Sets policy
3. Investigates, monitors, advices, etc
4. Responsible for minimal security requirements
5. Guides and trains other security administrator
6. Investigates company's security violations
7. Advises
8. Consults
9. Periodic review
10. Considers list of possible threats to organisation

# Chapter 1 – Basic Concept of System

**A. What is a system?**

1. System is defined as a set of *inter related* elements that *operate together* to accomplish *common purpose*.
2. Thus a system can be described by specifying the elements, the way in with the elements are related and goals which they are expected to achieve.
3. A business system comprises of economic resources like manpower, money, material, etc
4. A Computer Information system comprises of resources like hardware, software, data, etc.
5. A system can be abstract or physical. An abstract system is an orderly arrangement of interdependent ideas.

**B. System environment**

1. *Environment* like system is a collection of elements.
2. These elements surround the system and often interact with it.
3. The feature that define and delineate a system form its *boundary*. The system is inside the boundary and that which is outside the boundary is the environment in which the system is present.
4. A system in an environment can be a subsystem or a supra system. The interconnection and the interaction between the subsystems is termed as *interfaces.*
5. A *subsystem* is a part of larger system. Each system comprises of subsystems and each subsystem further comprises of many more subsystems which are separated from other through boundaries.
6. A *supra system* refers to the entity formed by a system and other equivalent systems with which it interacts.

**C. Deterministic and probabilistic system**

1. Deterministic: Predictable, Certainty of interaction between elements, no errors, example-Computer Program.
2. Probabilistic System: Unpredictable, uncertain, errors may occur. Example-Inventory system.

***D.*** **Open and closed systems** ***(also write the figure given in the study material)***

1. Closed system is self contained and isolated from environment. No interaction with the environment. A relatively closed system may accept defined inputs. Closed systems do not get the feedback from environment to sustain them. They to deteriorate over a period of time.
2. Open system is not self contained and actively interact with environment. They exchange resources, information, material or energy with the environment. They get feedback from

environment and thus adopt to changes to sustain and grow. They sustain for longer period generating surplus out of process.

**E. Decomposition or factoring of systems** *(Write the diagram given in the study material)*

1. A complex system cannot be studied easily. Hence, decomposition is adopted wherein the system is decomposed into subsystems. The system is decomposed until the smallest subsystems are of manageable size. (Business (system) is decomposed into finance, sales, administration, etc (subsystems). Finance is broken down into Accounting, legal, budgeting, etc.(smaller subsystems))
2. The boundaries and interfaces are defined to identify each subsystems and the system as a whole.
3. Decomposition in a subsystem is used to analyse an existing system and to design and implement a new system.
4. The general principle in decomposition which assumes that system objectives dictate the process is functional cohesion. Components are considered to be part of the same subsystem if they perform or are related to the same function.

**F. Simplification**

1. Once the system is decomposed into subsystems, the complexity increases. Hence the process of simplification is adopted.
2. Simplification is a process of organising subsystems so as to reduce the number of inter-connections.

**G. System entropy**

1. System entropy refers to a state where the system at one stage becomes disordered or decayed or disorganised.
2. System entropy can be prevented by regular repair, maintenance and replenishment of system. This task is termed as negative entropy.
3. Open systems require more negative entropy than closed systems because they interact freely with the environment and hence are more prone to entropy.

**H. System stress and system change [N05]**

1. **Meaning:** Any system has to undergo stress. A stress may be defined as *a force transmitted* by the systems supra-system that causes a *system to change* to achieve its goals.
2. **Types:** Stress brings in two basic types of changes in the system as follows:
   a. A change in goals of the system. This can be creation of new goals or elimination of old goals.

b. A change in achievement levels required for existing goals that can be either increased or decreased.

3. **Consequence of Stress**: Due to stress, the system can either adopt itself to the change or may decay or terminate.
4. **Adoption to change**: Due to stress, the system may adopt itself through a structural change or through change in its process. Example – A computer system under stress for more shareablitiy of data may be changed by the installation of terminals in remote locations – Structural Change. Demands for greater efficiency may be met by changing the way it sorts the data – Process change.

**I. Information – Meaning and characteristics [M06, M07]**: A raw data put into meaningful and useful context constitute information. Data and information are sometimes used interchangeably. Data is raw information and information is processed data. The following are the characteristic features of useful and effective information: (*Remember like this:* **TP MRR FCR CVQ** – *Costing* i-e Transfer Pricing, Marginal Rate of Return, Fixed Cost Recovery, Cost-Volume-Quantity)

1. Timeliness
2. Purpose
3. Mode and format
4. Redundancy
5. Rate
6. Frequency
7. Completeness
8. Reliability
9. Cost Benefit analysis
10. Validity
11. Quality

**J. Business Information System [N07]**

1. A business is also a system. However, a business system depends on an abstract entity called information system. Thus combination of business and information forms BIS.
2. Thus BIS helps in data flows between persons, departments and can encompass everything from inter office mails and telephone links to computer systems that generate periodic reports to various users.
3. It links the elements of business with an object of achieving a common goal.
4. The purpose of BIS is to process the inputs, maintain data files and to produce information, reports and other outputs.
5. BIS consists of subsystems like hardware, software, data storage, etc.

**K. Categories of Information system**

1. **Transaction Processing System:** 1. It is aimed at improving routine business activities of the organisation. 2. This is done by inserting Standard Operating Procedures in computer programs that control data entry, processing of details and search and presentation of data and information. 3. Computerised TPS provides speed and accuracy and can be programmed to follow routines without any variances. 4. TPS are operation oriented unlike MIS which is management decision oriented

2. **Management Information System** – Ref Chapter 3
3. **Decision Support System** – Refer Chapter 5
4. **Executive Information System** – Refer Chapter 5
5. **Expert Systems:**
   a. They are designed to *replace* the need for *human expert* where expertise is scarce.
   b. It's a software that expresses knowledge in terms of *facts and rules in specific areas*.
   c. Expert systems have arisen largely from academic research into *artificial intelligence*.
   d. It can change or *add rules* by itself
   e. It is developed by using software by name *PROLOG*.
   f. It is of greater use in *tactical and strategic level* of management.

# Chapter 2 – Transaction Processing System

**A. Transaction Processing Cycle** – Common cycles of business activity

1. Revenue Cycle
2. Expenditure Cycle
3. Production Cycle
4. Finance Cycle

**B. Components or elements of TPS**

1. Inputs
2. Storage
3. Processing
4. Outputs
5. Computer Storage
6. Computer Processing
7. Reference or table file

# Chapter 3 – Basic Concepts of MIS

**A. What is MIS and what does it consists of?**

1. MIS deals with the system that is critical for the success of a business.
2. It is mainly used by business managers for better management and scientific decision making.
3. The contents of MIS is:
   i. Management
   ii. Information
   iii. System

**B. Characteristics of a effective MIS** ***(2 Management, 2 Common, HIS Computer)***

1. Management Oriented
2. Management Directed
3. Common Database
4. Common Dataflow
5. Heavy Planning Element
6. Integrated
7. Subsystem Concept
8. Computerised

**C. Misconceptions or Myths about MIS:** People have some wrong notions of MIS. They think:

1. Study of MIS is about the use of computers
2. More data in reports means more information for managers
3. Accuracy in reporting is of vital importance

**D. Pre-requisites / Pillars of an effective MIS**

1. Database
2. Qualified systems and management staff
3. Support of Top Management
4. Control and maintenance of MIS
5. Evaluation of MIS

**E. Constraints in operating an MIS** *(For each problem also write the solutions)*

1. Non availability of experts
2. High turnover of experts
3. Experts usually face the problem of selecting the sub system

4. Non-standardised approach of experts due to varied business objectives
5. Non availability of co-operation from the staff
6. Difficulty in quantifying the benefits of MIS.

**F. Effects of using computer for MIS**

1. Speed of processing and retrieval of data increases
2. Scope of use of information system has expanded
3. Scope of analysis widened
4. Complexity of system design and operation increased
5. Integrates the working of different information subsystem
6. Increases the effectiveness of information system
7. More comprehensive information

**G. Limitation of MIS**

1. *Output quality* depends on input quantity
2. Not a substitute for *managerial decisions*.
3. Does not have requisite *flexibility.*
4. Cannot provide *tailor made information packages* for making decisions.
5. Ignores *non quantitative factors* like morale and attitude of members, etc
6. Less useful for *non-programmed decisions*
7. Effectiveness of MIS decreases where *information is collected but not shared*.
8. Effectiveness of MIS decreases where *frequent changes to top management* are made.

**H. Planning information requirements of executives can be categorised as**

a. *Environmental Information* – government policies, factors of production, Technological environment, economic trends.
b. *Competitive Information* – Industry Demand, Firm demand, Competitive data
c. *Internal Information* – Sales forecast, financial budget, supply factors, policies, etc.

**I. Factors on which information requirements depend**

a. **Operational function** – The fact of what information is required depends on various functions of sub-systems. Eg: Business information varies for marketing, finance, etc.
b. **Types of decision making**
   i. *Programmed Decisions* – 1. For pre-determined problems 2. Systematic 3. Structural 4. Formal 5. Procedural.
   *ii.* *Non Programmed decisions* – Need to use our skill and knowledge to achieve the objective. Unstructured, unscientific, no procedure, unanticipated

c. **Level of Management activities**

i. *Strategic Level* – Unstructured information, Top level decisions, vital impact on direction and functioning of the organisation.

ii. *Tactical Level* - Top level decisions are split into many small levels. Each level is done by tactical level of management.

iii. *Supervisory Level* – Information required for specific tasks.

**J. Level of Management Activity:** *(Also refer to the table in the study material the end of the chapter)*

a. **Top level(Strategic Level)**–*External* (Competitive Activities, Customer Preferences, style, changes, economic trends, technological changes), *Internal* ( historical sales, costs, profits, cash flow, divisional income, sales, expenses, financial ratios, interests)

b. **Middle Level (Tactical Level)** – *External* (Price Changes, shortages, demand or supply, credit conditions), *Internal* (current performance indicators, over-under budgets, etc)

c. **Supervisory Level** – *External* (changes to material supplies and sales), internal (Unit sales and expenses, current performances, shortages and bottle necks, etc)

# Chapter 4 – System Approach and Decision Making

**A. Systems approach in problem solving involves the following 6 steps:** (Write the diagram given in the study material)

a. Defining the problem –
b. Gathering and analysing the data concerning the problem
c. Identification of alternative solutions
d. Evaluation of alternative solutions
e. Selection of best alternative solution
f. Implementation of the selected solution.

**B. Classification of decision**

a. Programmed and non programmed decisions – Refer chapter 3
b. Strategic and Tactical Decisions – Refer chapter 3
c. Individual and group decisions

**C. Financial decisions taken with financial Statements include the following:** *(Visualise the budget, balance sheet and profit and loss account – Budget, share capital, fixed assets, working capital, current assets, PAT, tax)*

a. Estimation of requirement of funds
b. Capital Structure Decisions
c. Capital budgeting decisions
d. Working Capital Management
e. Current Asset Management
f. Profit Planning
g. Tax Management

**D. Marketing System:**

a. The main objective of marketing management systems is to develop, promote, distribute, sell and service the products of the organisation and return a profit that is enough to justify its existence.
b. It bridges the gap between business firms and its customers.
c. Marketing system consists of the following:
    i. Sales: Sales Support and Sales Analysis
    ii. Market research and intelligence
    iii. Advertising and promotion
    iv. Product development and planning

v. Product Pricing System
vi. Customer Service

**E. Information required by a marketing system**

a. ***Environment Information*:** Political and governmental considerations, demographic and social trends, economic trends.
b. ***Competitive Information*** – Business operations of competitive firms, individual firm's product demand and supply.
c. ***Internal Information*** – Sales forecast, financial plan, supply factors, policies.

**F. Production Decision:**

a. **Consists of:** production planning, product engineering, scheduling production facilities, quality control and production control
b. **Depends on:** pending sales orders, expected sales, consumer grievances, etc.
c. **Objectives:** Monitoring of work in process, daily stock balancing, correction of any deviation, meet the product demand, etc.

**G. Production Planning:** It consists of the following

a. First break the job into various division. Break divisions into sub-divisions. Thus make a list of operations to be carried out.
b. Make a drawing of how the production process is carried on.
c. Draw Bill of materials for each operation and also schedule the dates on which various materials is required.
d. List out the tools required for production process.
e. Once the above all are ready, have a trial run and rectify the problems.
f. Conduct routing where all tools, materials time, labour, etc required for a particular operation is charted out.
g. Draw up a detailed time table for entire activity to be completed
h. The dispatch-issue instructions for each operations should be carried out properly.

**H. Production Control**: It includes inventory control, time control, cost control, quality control.

**I. Basic information requirements of production planning and control systems:** Firm's Policy, Sales related details, inventory details, labour related details, cost related details, time schedule, job schedule, resources availability details. *(Imagine product cost sheet)*

**J. Objectives of Production Scheduling:** When your boss gives you the task of drafting a production schedule ensure that it meets the following objectives:

a. Production Stages should be in sequential and rational order
b. The idle time of operators and equipments are minimum
c. Be clear on to what extent we have to depend on the outside parties.
d. Ensure that required production is met on the target date
e. Study alternative methods of performing the activities so that time taken to perform can be further reduced.

**K. Benefits of MRP System**

a. ↓ Inventory level
b. ↓ Inventory carrying cost
c. ↑ Production
d. Better and reliable customer service
e. Grater responsiveness to change
f. Closer coordination

**L. What are the sub systems of Personnel system?**

a. Recruitment
b. Placement
c. Training and development
d. Compensation
e. Maintenance
f. Health and Safety

**M. Sources of personnel information**

a. Accounting Information System
b. Payroll Processing

# Chapter 5 – Decision Support and EIS

## A. What is a DSS?

a. A DSS can be defined as a systematic structure that helps the manager in developing semi structured and unstructured decisions. It supports human decision making process rather than replacing it.

b. DSS is a class of subsystems of MIS which support analysts, planner and managers in decision making process.

c. Planning support systems and control support systems are specific instances of broad concept of a DSS.

d. Expert systems are a type of DSS that incorporates the knowledge base of an expert with a flexible interface so that a layman can use the computer system.

e. DSS are especially useful for semi structured and unstructured d problems where problem solving is enhanced by an interactive dialog between the system and the user.

## B. Characteristics of DSS

a. Used for semi-structured and unstructured decisions

b. They have the ability to adopt to the changing needs.

c. DSS are easy to learn and use

## C. Components of DSS

a. Users

b. Databases

c. Planning Language

d. Model base

## D. Tools of DSS

a. Database software

b. Model base Decision support software

c. Tools for statistics and data manipulation

d. Display based decision support software

## E. Examples of DSS in accounting

a. Cost Accounting System – Example of health care industry

b. Capital Budgeting System – considers financial, non financial, quantitative and qualitative factors in decision making

c. Budget Variance Analysis System

d. General Decision support system

**F. Executive Information System:**

a. Executives are referred to as top level managers who can exert a strong influence on the course of action to be taken by the organisation.
b. The executives can be a chief source of information for the organisation to plan for the future which is uncertain and to plan strategic decisions.
c. Executives can monitor the external environment for new technologies, competitors, etc.

**G. What are the types or classes of executive decisions?** They are as follows:

a. Strategic Planning
b. Tactical Planning
c. Fire Fighting
d. Control

**H. Characteristics of types of executive decisions**

a. Lack of structure
b. High degree of uncertainty
c. Future Orientation
d. Informal source
e. Low level of detail

**I. Executive Information System vs. Traditional Information System**

EIS unlike TIS:

a. Is specifically tailored to executives information needs.
b. Accesses specific issues and problems
c. Provides extensive online analysis tools
d. Can access broad range of external and internal data
e. Easy to use
f. Used directly by executives
g. Is screen based
h. Is presented by pictorial and graphical means
i. Is presented in summary format.

**J. Purpose of EIS**

a. Managerial Support
b. Timely Information
c. Direction to specific areas

# Chapter 6 – Enabling Technologies

**A. Traditional Computing Model**

***1. Mainframe Architecture –***

1. *Architecture:* There is one central processor which is connected to many dumb terminals. The user requests are sent through key strokes from dumb terminals and the processor does all the processing
2. *Merits:* Many users can share a single computer's application, database and peripherals.
3. *Demerits*: High cost. Does not support graphic user interface. Access to multiple database over wide geographical area is not possible

**2. Personal Computers –**

a. *Architecture:* Enables independent computing and does not require a central processor.

b. *Merits:* Lower cost. The work load of central processor is brought down as disconnected workstation processes by itself.

c. *Demerits:* Disconnected computing model of PC deprives it from sharing expensive resources that mainframe users can share like printers, modems, etc

**3. File Sharing Architecture –**

a. *Architecture*: The server downloads files from the shared location to the desktop environment. The requested user job is then run in the environment.

b. *Merits***:** In this architecture, workstation is intelligent terminals that shares required files with the server.

c. *Demerits:* Here the server directs the data and the workstation processes the data. It is a dumb server-smart workstation relationship. Max of 12 terminals are allowed.

**B. Client server model:**

1. Intelligent division of processes between client and the server
2. Concept of smart processor and smart workstation.
3. Server handles global tasks and workstation handles local tasks.
4. Server sends only the information required for the client thus reducing network traffic.

**C. Why should one change to client/server computing?**

1. Improves the flow of management information
2. Better service to end user departments
3. Lowering IT costs
4. Ability to manage IT costs better

5. Direct access to required data
6. High flexibility of information processing
7. Direct control of the operating system.

**D. Benefits of Client Server Technology**

1.

**E.** Characteristics of client server technology

**F.** Approaches to client server technology

**G.** Components of Client server technology

1. Client
2. Server
3. Middleware
4. Fat client or fat server
5. Network

**H.** Control Security or techniques to be ensured by IS auditor in client server technology

**I.** Client/Server risks and issues

1. Technological Risks
2. Operational Risks
3. Economic risks
4. Political Risks

**J.** Server Centric Model