Information Systems

Control & Audit

*

Chapters Summary

Benifitial for exam time

By- Pardeep Rohilla

Contact : 098125-98398

www.facebook.com/pardeep.rohilla

CHAPTER 01

INFORMATION SYSTEM

1. BASIC CONCEPTS:

- A system includes set of components which work together to achieve certain objectives or goals.
- A system includes some inputs which undergo thorough processing to provide the required outputs.

2. TYPES OF SYSTEM:

- OPEN SYSTEM:
  - Adaptable to changes
  - Costly to develop & maintain
  - Longer life span than closed system
  - Require more maintenance than closed system
- CLOSED SYSTEM:
  - Not adaptable to changes
  - Not normally developed for business organizations
  - Easy to manage & inexpensive to develop
  - Shorter life span than open system
- DETERMINISTIC SYSTEM:
  - Provide exact output
  - Account for past data as input
- PROBABILISTIC SYSTEM:
  - Provide expected output
  - Take into account data for expected future transactions
- ABSTRACT SYSTEM:
  - Include design & drawings containing set of ideas or planning
  - Non-working system, ultimately converted into physical system
- PHYSICAL SYSTEM:
  - Includes all working system
  - Contain some physical components

3. SYSTEM CONCEPTS:

- SYSTEM BOUNDARY: It represents the periphery or limit within system components work together.

- SYSTEM ENVIRONMENT: The components outside the system boundary with which the system interacts is the system environment. System can accept inputs from & provide outputs to the environment.

- SUB-SYSTEM: Parts of a system are sub-systems. A complex system is divided into various sub-systems which help in easy development & management of the complex system.
- SUPRA-SYSTEM: it is the system immediately above the sub-system.
- SYSTEM DECOMPOSITION: It is the process of dividing the system into various subsystems. This is based on the principles that:
  - Systems should be divided into sub-systems until the overall system is easy to manage & develop
  - Every sub-system should have relevance to the main system.
- SYSTEM SIMPLIFICATION: This concept is used to divide a system into large number of sub-systems. It describes a methodology to manage the sub-systems. Here, similar subsystems are grouped together to form clusters & one cluster is linked to another to provide integrated system.
- SYSTEM STRESS: In a normal process, a supra-system provides stress / pressure to its sub-system due to change in its objectives or goals. The sub-system can adapt to these changes only if they are open-type systems and by changing their components/ rocesses.
- SYSTEM ENTROPY (or) MAINTENANCE: In order to avoid the system losing its value over time due to positive entropy (natural energy leakage), it should be provided continuously with some upgradations (negative entropy).

4. INFORMATION:

- Processed data is known as information.
- The data which has some value for its receiver is information.
- Information Systems are developed to process the data & provide information which help in decision-making process.

5. CHARECTERESTICS OF GOOD INFORMATION:

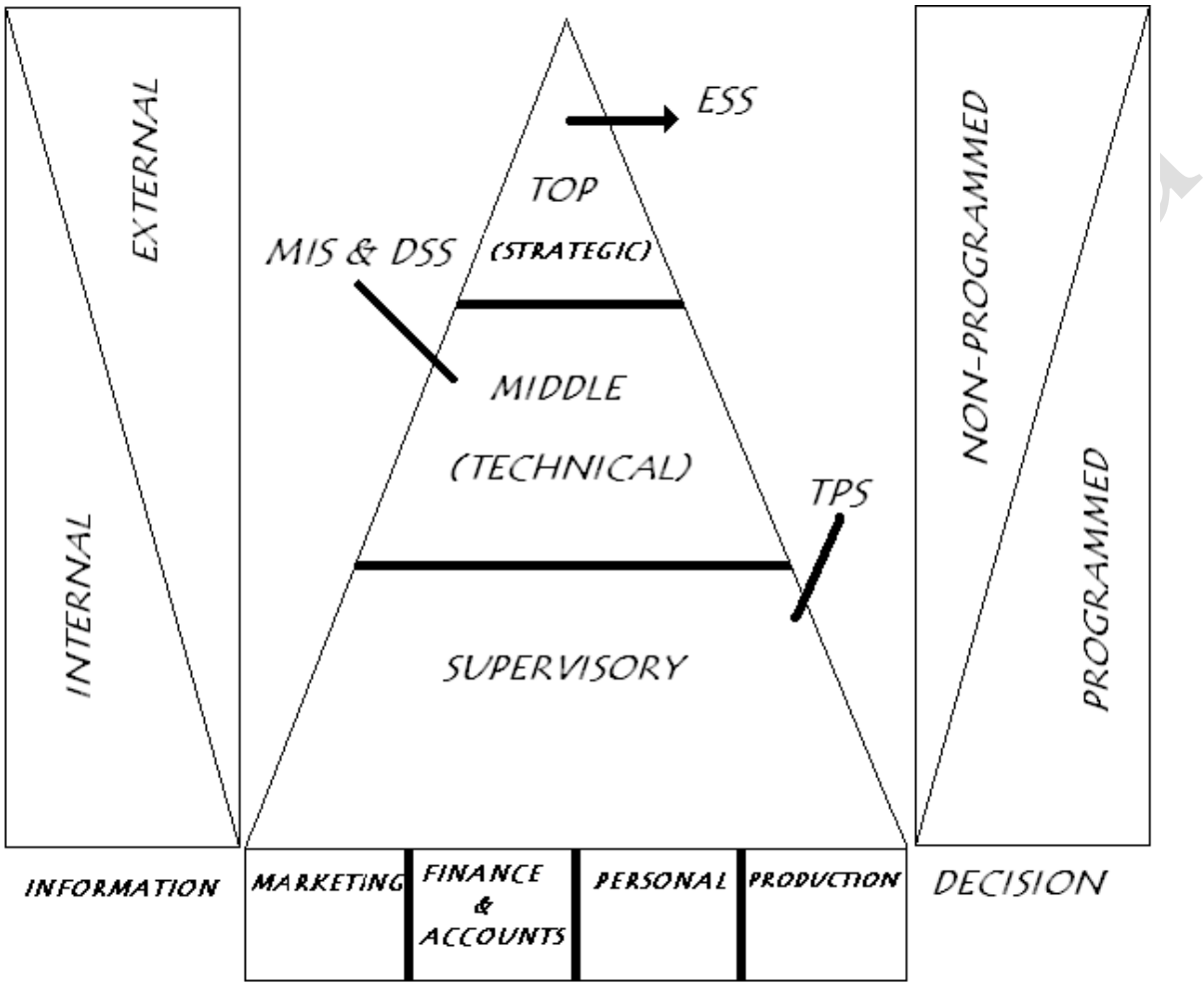
- Accuracy
- Timeliness
- Appropriate mode & format
- Complete & up-to-date
- Reliable source of information
- Adequate & purposeful
- May include redundancy
- Transparency
- Free from any bias
- Quality

6. FACTORS ON WHICH INFORMATION REQUIREMENTS OF EXECUTIVES DEPENDS:

- Functions of the executive: Management or Operational
- Level of the executive in the management

- Type of decision the executive wants to make

The information requirement of top executives is normally through external sources and the Information requirement of middle and supervisory management if through internal sources.



7. TYPES OF DECISIONS EXECUTIVES WANT TO MAKE:

This factor includes two analysis for deciding the information requirements of the activities:

- Program decisions
- Non-program decisions

In case of program decisions, given information is without any uncertainty, whereas in no program decisions, the information will include a factor of uncertainty.

8. INFORMATION SYSTEM & ITS ROLE IN BUSINESS:

Information System is a collection of software, hardware, data & users etc. It helps organization in efficient and effective decision making. Its key roles are:

- Provide competitive edge
- Provide efficient operation

- Provide updated information
- Helps to integrate operational functions
- Helps to achieve set strategic goals

9. VALUE / DIMENSIONS OF INFORMATION:

- **ECONOMIC DIMENSION:** information is evaluated in terms of cost & benefits. It is a difficult task due to its intangible nature but an appropriate analysis for cost incurred and benefits to be derived is performed.
- **BUSINESS DIMENSION:** the importance of information for business continuity is determined.
- **TECHNICAL DIMENSION:** Technical characteristics are evaluated in terms of security, access control & availability to user when required.

10. TYPES OF INFORMATION SYSTEM:

- Transaction Processing System
- Management Information System
- Decision Support System
- Executive Information System

11. TRANSACTION PROCESSING SYSTEM:

- TPS is used to process transactions & provide routine & regular reports.
- TPS is known as basic information system & it acts as a base to other IS like MIS & EIS.
- TPS automates the routine procedures of transaction-processing which helps to provide the required outputs in an efficient manner.
- TPS is developed using SDLC Methodology & is known as Life-cycle system.

12. COMPONENTS USED IN TPS:

- Input, used for capturing and classifying transactions
- Processing, used to process transaction as per business logics
- Storage, used to maintain the data of transactions in form of master file and transaction files
- Output, used to provide required reports from TPS. It gives 2 types of reports:
  - Operational reports
  - Financial reports

13. MANAGEMENT INFORMATION SYSTEM:

It is an extension of TPS. MIS provides some value-added reports by using operational database of TPS. It provides reports based on exceptions & mathematical sign principles which help in management decision making.

It is also based on a life cycle system & it is extensively used in various management functions.

14. CHARECTERESTICS OF A GOOD MIS:

- Management-oriented
- Management-directed
- Need-based
- Exception-based
- Integrated
- Common data flow
- Common database
- Modularity
- Comprehensive, flexible & capable of updating

15. ELEMENTS OF MIS:

- **Management:** process for planning, organizing, initiating & controlling works on information provided by MIS.
- **Information:** Processed data.
- **System:** components which work together to achieve goals.

MIS is an IS which helps in efficient decision-making by providing value-added & timely information to management for various purposes.

16. MISCONCEPTIONS ABOUT MIS:

- More data means more information
- Accuracy is highly important
- MIS means only computer-based IS
- INFORMATION SYSTEM CONCEPTS

17. PRE-REQUISITES OF MIS:

Components & activities which help to provide a quality or good MIS:

- Common database
- Expert staff
- Controls & established standards
- Maintenance
- Time to Time Evaluation

18. CONSTRAINTS IN OPERATING COMPUTER-BASED MIS:

- Non-availability of experts
- Turnover of experts
- Non-supporting staff

- Non-standardization of MIS
- Starting Trouble

19. EFFECTS OF USING COMPUTERS FOR MIS:

- Fast data processing-updated information
- Fast access of required information
- Comprehensive / detailed information
- Information acts as resource
- Helps in effective & efficient decision-making
- Wider / sensitivity analysis

20. LIMITATIONS OF MIS:

- Quality of output depends on quality of input
- MIS depends upon TPS & hence TPS limitations will be limited to MIS
- Can be used to solve only structured problems
- Provides output based on quantitative data
- Does not allow user to use judgement for problem solutions
- MIS are available as function-based MIS & this may lack tight integration among functions.
- Complex & costly process.

21. DECISION SUPPORT SYSTEM:

DSS is used for solution of semi-structured & unstructured problems. It is a pro-type system used to solve Ad-hoc problems & is user-friendly.

DSS are knowledge-based system. These systems allow its users to apply his knowledge for solution of problems by using “what-if analysis”.

22. CHARACTERiSTICS OF DSS:

- Solves both semi-structured & unstructured problems
- Used for knowledge-based system
- Sensitivity analysis
- User-friendly & graphical interface
- Can use any type of data of any structure

23. COMPONENTS OF DSS:

There are 4 major components of DSS:

- **User:** applies its knowledge for solution of problems. There are two types of users for DSS:
- **Analysts:** they normally design & develop the DSS using complex formulae & functions for a problem solution.
- **Managers:** these users have knowledge of problem to be solved & they use already created DSS for problem's solutions.
- **Planning Language:** provide GUI for structuring of problems or creating model base. They
- provide various functions & features for efficient solution of problems. There are two types of planning languages:
- **General Purpose Planning Language:** provides general functions & features to solve general purpose semi-structured or ad-hoc problems. Used for those problem's solutions which have low data volumes.
- **Special Purpose Planning Language:** used for solution of problems which have large data volume. Provides special functions & features which help to solve complex functions or procedures.
- **Model Base:** this is the most important component of DSS. It is also known as brain of DSS. It provides the structure of the problem to be solved by DSS.
- **Data Base:** this component is used to provide inputs for a DSS problem. There are 2 types of database in DSS:
- **User Database:** includes data or inputs collected by user from various sources.
- **Corporate Database:** includes data values provided by organization's operational database.

24. SOFTWARE TOOLS USED FOR CREATING DSS:

- Database software-Back end
- Model-based software-Front end
- Statistical Software-Process
- Graphical Software-Output

25. USE OF DSS IN ACCOUNTING APPLICATIONS:

- In capital budgeting applications for investment analysis
- In cost accounting problems
- General budgeting problems
- Portfolio management

26. EXECUTIVE INFORMATION SYSTEM:

- User-friendly
- Provides information for top executives

- Helps to solve complex problems without much know-how
- Timely information on monitoring organization
- Provides information on internal & external databases
- Supports online functions
- Lacks structure
- Future oriented
- Low-level details
- Internal sources

27. CHARACTERISTICS OF EIS:

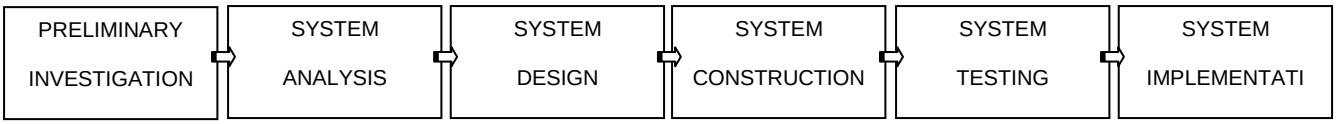
- Economic environment
- External environment
- Competition environment
- Internal environment

28. PURPOSE & CONTENT OF EIS:

- Timely information of any aspect
- Provides information about problem area
- Monitoring of organization's working

CHAPTER 02
SYSTEM DEVELOPMENT LIFE CYCLE METHODOLOGY

STAGES IN SDLC



1. SYSTEM DEVELOPMENT PROCESS is that process which takes place in an organization whenever that organization wants to convert an old system into a new system or wants to upgrade or change the existing system.

2. REASONS FOR FAILURE OF SYSTEM DEVELOPMENT IN ORGANIZATIONS

- Changing requirements or needs of users and lack of clarity in this regard
- Lack of support from management, users
- Resistance to change
- Rapid change in technologies
- Lack of technical know-how among developers and users

3. APPROACHES TO SYSTEM DEVELOPMENT

- Traditional approach
- Prototype approach
- End user approach
- Top Down & Bottom Up approach
- SD approach in small organizations

4. TRADITIONAL APPROACH

- Popular and usable approach. Used primarily to develop large & complex IS.
- All steps of SDLC are followed as it is
- Initial traditional approach was based on principle that there will be no error in previous step of SDLC
- Later, the old approach was modified to include feedback to rectify errors in previous phases
- Latest traditional approach has been further modified to simultaneously starting 2 or more phases to cut time
- Also known as WATER FALL APPROACH

5. PROTOTYPE APPROACH is used in developing non recurring systems. Following steps are used to determine exact requirements of system:

- User specifies the requirements from the system
- Construct a design of the system based on the requirements specified above
- Build a prototype. PROTOTYPE is a system with basic functionality, primarily presenting
- inputs and outputs.
- Evaluation of prototype by the users to determine correct requirements
- Implement suggestions of the users in the prototype.

These steps continue till the time the user provides his consent for the prototype.

- Once the user is satisfied with the prototype system, the remaining system is developed using normal traditional approach.

Prototype approach has the following advantages

- Helps to determine exact requirement
- Helps to provide input & output formats in advance
- Helps to ensure success of system
- Helps in sorting technical issues of System Development

Prototype approach has the following disadvantages

- Time consuming
- Causes inefficient System Development
- Disappointment to user

6. END USER APPROACH

- User specifies requirements from system and accordingly, user procures or develops system
- Low cost & easy to use
- Disadvantages
- User cannot specify all requirements
- Lack of integration among all systems in organization
- Lack of complete use of new system

7. TOP DOWN & BOTTOM UP APPROACH

TOP DOWN APPROACH	BOTTOM UP APPROACH
Those systems, which satisfy organization objectives or which help top management in working, are procured first	Those systems, which help operational executives in day to day operations, are procured first
Top management is involved in System Development	Operational executives help in System Development
Once system is developed for top management, the system is extended to satisfy requirements of operational executives	Once system is developed, it is extended to satisfy requirements of top management

8. SD APPROACH IN SMALL ORGANIZATIONS is an easy to use and low cost approach.

Following are the steps to be used:

- Organization determines its requirements for a system
- Organization evaluates various software available in market, which can satisfy its requirements
- Organization selects the software and procures the required hardware accordingly
- Organization implements the software & hardware for system use.

9. RAPID APPLICATION DEVELOPMENT

A. RAD is the latest system development approach, to develop complex systems rapidly or in lesser time

B. This approach is an extension of the traditional system development approach. Here,instead of developing software by analysts & developers on a standalone basis, a joint application process / approach is followed by involving user as a part of development.

C. In this approach, system development work are organized with following components as
   a. part of that workshops:

- Users
- Analysts
- Developers
- Computer Aided Software Engineering (CASE) tools
- Previously developed applications

D. These components help to develop applications rapidly by using the following process

- Document the requirements of the user
- Design the system
- Develop the system
- Test the system
- Jointly develop the application
- Satisfy the requirements of the user

All the above processes are iterative process & are continued till the final product is out for use.

10. SYSTEM DEVEOPMENT METHODOLOGY

- Divide entire project into manageable tasks
- Every task or activity has to be properly documented
- Ensure involvement of users
- Thorough testing of system before its implementation
- Ensure proper training of user for system
- Perform post-implementation review of the system to find out the various problems encountered in system development & outputs.

11. SYSTEM DEVELOPMENT TOOLS]

These are software & methods used for efficient system development. They help to document the specification of the system to be built. They are of the following types:

A. System component & flow tools
B. User interface tools
C. Data attribute & relationship tools
D. Detailed logics tools

12. DATA FLOW DIAGRAM

It is a graphical representation of the logical flow of data from origin to destination with an intermediate process and storage. It helps in expressing the system requirement in simple and understandable form. It helps programmers & users in understanding the working of a particular process with required entities.

13. SYSTEM FLOWCHART

- ❖ It is used to present a system and its component along with its interaction with other systems.
- ❖ It provides a higher level view of system to be developed.
- ❖ It represents a graphical model of physical information system, whether present or proposed.

14. SYSTEM COMPONENT MATRIX

This tool is used to represent the system components in a tabular form. It is primarily used to provide information about system components to end users in an easy to understand form.

15. DATA DICTIONARY

- ❖ It is used to maintain data about data and also known as metadata.
- ❖ It maintains structural information, which helps in efficient operation of database. It does all valuations for database operations. & provides information on database structure.

16. CASE TOOLS

- ❖ COMPUTER AIDED SOFTWARE ENGINEERING tools
- ❖ Used for efficient software development
- ❖ Helps in increasing the productivity of the software developers
- ❖ Increases the quality of the developed software

17. DIFFERENT CODING SYSTEM

A. Classification Codes: This scheme is used to classify objects or entities by using 1 or 2 digit codes.
B. Functional Codes: This coding scheme is used to different functions or activities.
C. Subset of Digits Code: This coding scheme is used to provide data code to large volume of data by dividing data into certain sets or parts, which help in efficient input & processing.
D. Mnemonics Code: Here, abbreviations or short forms are created for frequently used data values.
E. Hierarchical Codes (Work Breakdown Structure Code): This is similar to subset of digits coding scheme. This is used for providing data codes to projects / activities, in an hierarchical manner.

18. DATA STORAGE DESIGN

Here, analyst and database administrator design the data management system of the IS to be developed and the structure of the database to be used. There are 2 methods of data management:

A. File System is a conventional or old method of data management and in this, data is managed using flat files.
B. DBMS is the most popular method of data management and it provides various advantages over the file system such as data integrity, concurrent data access and reduced redundancy.

19. SOFTWARE DEVELOPMENT

Software development involves development of programs. Program development includes various steps or phases known as program development life cycle. They are:

A. Program Analysis: In this step, programmer analyses the program to be developed in terms of given inputs, required outputs and processes or logics to be used to convert given inputs into required outputs.
B. Program Design: In this step, programmer develops or designs the program to be developed normally with help of flowcharts. Program design helps in efficient coding of program.
C. Program Coding: In this step, programmer writes a program by using some high level language. This program developed in high level language is known as source program. To execute a program on computer, the source program is converted into an object program with help of compiler.
D. Program Debugging: To execute a program on a computer, it is required that the program is correctly compiled. A program may have many types of errors or bugs which should be removed for correct execution of program. This removal of errors or bugs from a program is known as program debugging.
E. Program Documentation: here, documents are prepared for development of program. Various types of documents are prepared for a program.
F. Program Maintenance: Here, developed program is maintained for various upgradations. A program maintenance normally includes up gradation or changes to following:
    - Change of input formats & new input processing
    - Change of logics and implementation of new logics
    - Change of output formats and implementation of new outputs

20. PHASE 1 OF SDLC - PRELIMINARY INVESTIGATION

This is the first stage of SDLC and in this phase, the user's requests for new system or change in the existing system are validated through various analysis. The purpose is to collect information and apprise the feasibility of the project.

Following steps are part of this phase:

A. Defining problem – User request for new system or change in existing system

Is properly defined by analysts.

B. Conducting preliminary investigation

- Conducting interviews with users for determining requirements
- Review of documents to determine the workings & the problems of the existing system and the requirements from the new system

C. Exploring viable options – Analyst explores various viable options which can be used to satisfy user requirements from system
D. Conducting feasibilities – various feasibilities are tested for the selected viable options. They include:
   - Technical feasibility
   - Operational feasibility
   - Economic feasibility
   - Legal feasibility
   - Schedule feasibility
   -
E. Submission of reports – After analysis, complete analysis is documented as a report for submission to management. This report also includes the recommendations for options to be used in a new system.

21. PHASE 2 OF SDLC - SYSTEM ANALYSIS

In this phase, exact requirements of the user from the new system are specified. Here, following steps are performed to determine and specify the exact requirements from the proposed system:

A. Collect information – Detailed investigations are performed to determine user requirements and also to determine the data being used in the existing system for various business operations.

Analysts use various methods to collect information and these methods are known as fact finding techniques. Following are some popular fact finding techniques:

- Structured interview
- Questionnaires
- Collect documents
- Observation

B. Analysis of existing system – Detailed analysis of existing system is performed by the analyst in terms of the following:

- Inputs
- Outputs
- Methods, procedures & data communication
- Data files
- Internal controls
- History

After all the above analysis, analyst prepares 2 more things:

- ❖ FLOW DIAGRAM of existing system's working, which includes all details of the existing system in terms of input, process & output
- ❖ Analysis of the flow diagram, prepared above, is performed in terms of:

    - Excess workload
    - Inefficient and non required operation
    - Efficient operation
    -

C. Analysis of proposed system – Requirements from proposed system are then specified in a document known as requirement specification document. Detailed analysis of proposed system is performed by the analyst in terms of the following:

    - Inputs
    - Outputs
    - Methods, procedures & data communication
    - Data files
    - Internal controls

Database is analyzed in terms of types of DBMS to be used to provide the required system.

D. Preparing requirement specification document – All requirements from proposed system are specified in a document known as REQUIREMENT SPECIFICATION DOCUMENT. This acts as a base for further development of system. This document is submitted to management for further process.

22. PHASE 3 OF SDLC - SYSTEM DESIGN

In this phase, system is designed for its component as per the specifications given in the Requirement Specification Document.

A. Characteristics of a Good Design
    - It should be easy to understand
    - It should be comprehensive & efficient

- It should be easily expandable
- It should be flexible to implement changes

B. Components to be designed

❖ Output Design – This provides the design of reports and message boxes. Output design should be in such a way that it provides output / reports in appropriate form.

- Factors to be considered for output design: content, volume, format, mode,
- timeliness & media
- Presentation of information :

  ✓ Format: tabular & graphical
  ✓ Mode: Printed & Display

❖ Input Design – Purpose is fast, error free entry of voluminous data

- Factors to be considered for input design: content, volume, format, mode, timeliness & media
- Design of Input forms: A good Data entry form helps in efficient data entry. It should be easy to fill, should ensure accurate completion, should be attractive and should meet intended purpose.
- Design of Input Codes: Codes help in efficient data entry. They are, usually, the primary key. They should be unique, of appropriate size, easy to use, suggestive, expandable and permanent.

C. System Manual – It is a document which contains all the design specification of, both, the existing as well as the proposed system. Design specifications are used to construct the proposed system and is included as part of the system manual.

23. PHASE 4 OF SDLC - SYSTEM ACQUISITION AND SOFTWARE DEVELOPMENT

A. Various factors to be considered for hardware procurement

- Hardware should be procured to meet design specifications for data processing of proposed system
- Hardware should be of latest technology
- It should support the required types and a number of input and output devices
- There should be support services from hardware supplier for both maintenance and operation of hardware
- There should be a consideration to various software provided by hardware suppliers for providing optimum performance of their hardware

B. Make or Buy Software – Factors

- If required software is readily available in market
- Organization does not have the required skill to develop the software
- Organization does not want to spend time and money required for software Development

C. Advantages of packaged software

- Rapid installation and use
- Cost efficient
- High quality
- Low risk of failure

D. Limitations of packaged software

- Partial usefulness – not all features are used
- Inflexibility
- Low quality of documents
- Lack of continuity or support from seller

E. Steps used for vendor system verification

- Prepare design specification
- Prepare request for proposal document (RFP) based on design specifications
- Provide RFP document to reputed vendors and ask them to submit proposal
- Evaluate submitted proposals and remove inferior proposals
- Ask remaining vendors to provide presentation on system
- Provide suggestions to vendors to improve system and to resubmit the proposal
- Evaluate resubmitted proposals
- Contact existing users of their systems to determine system performance
- Conduct benchmark tests of vendor systems
- Select best system

F. Criteria for vendor system verification

- Check list method
- Support, training & maintenance
- Cost v/s. Benefit
- Adaptability, flexibility, upgradability
- Compatibility with existing systems

G. Methods to evaluate vendor's systems

- Check list method
- Point scoring analysis method
- Bench mark test
- Evaluation from published reports

H. Sources of packaged software
   - Software development organization
   - Channel partners or distributors
   - Hardware manufacturers or suppliers

24. PHASE 5 OF SDLC – SYSTEM TESTING

In this phase, system is traditionally tested before its implementation or use. Normally, following procedures are used for system testing:

A. Prepare realistic test data. Realistic in terms of values and volumes
B. Execute test data on developed system
C. Review the outputs in terms of errors, response time, formats and required content etc.
D. Then, appropriate action should be taken for correction of errors and outputs
E. Review the outputs with users for any correction

System is, normally, put into testing even after implementation under parallel testing procedures, in which the newly developed system is used in parallel with the existing system. System, also goes through various types of testing, like:

A. Alpha Testing: This is performed by expert developers;
B. Beta Testing: This is performed by expert users of similar system; and
C. Gamma Testing: his testing is performed by expert system analyst and designers.

There is one more popular type of system testing, which is conducted for multi user systems, known as STRESS TEST. In this test, system performance is evaluated for number of users and volume of data which, systems can handle without degrading its performance.

25. PHASE 6 OF SDLC – SYSTEM IMPLEMENTATION

System implementation is a process, which ensures that information system is properly operational and allows its users to take over its operation for use & evaluation. It includes activities for conversion of an old system to a new system. The system implemented can be a totally new system or a major modification to the existing system. In either case, a proper implementation is necessary to provide a reliable system to meet user's requirements. System implementation consists of following activities:

A. Equipment installation – In this, procured hardware is installed in the organization for usingthe developed or acquired software. Steps involved are:
   - Site Preparation: Here, a layout is prepared regarding where the equipments will be installed in terms of their place, user locations etc.
   - Install Equipments: Once a site is prepared, the equipments are installed physically and connected to power line and communication lines etc.
   - Check equipments: Installed equipments are checked for proper utilization and various routine tests.

B. Training personnel – It is an important aspect for effective utilization of the installed system.Whenever a new system is installed in the organization, a need of training arises for both general users and computer professional as the new system often contains some new types of software and hardware. Normally, 2 types of training are provided, namely:
   - Training to system operators
   - Training to end users
   -

C. Conversion procedures – This involves the activities carried out for successful conversion from old system to new system. Following activities are carried out:
   - Procedures Conversion: For implementing the new system, the procedure & methodsfor working on the new system must be clearly defined and converted from oldprocedures and methods.
   - File Conversion: Old data files should be converted to as per the requirements of the new system and these conversions must be done before the new system is implemented.
   - System (Processing) Conversion
   - Scheduling of personnel and equipment:
   - Preparation of alternative plan in case of equipment failure:

Conversion Strategies

- ❖ Direct conversion: On a given date, old system is totally discontinued and new system is started from next date.
- ❖ Parallel conversion: Both old & new system are used together for some time and after that, the old system is discontinued.
- ❖ Gradual conversion: Here, the volume of transactions is gradually reduced in the old system and subsequently increased in the new system.
- ❖ Modular prototype conversion: Here, each part of the system is developed, redefined, implemented and then, the next one and so on and so forth until the whole system is converted.
- ❖ Distributed conversion: This system is used when the same system if to be installed in several places at the same time.

D. Post implementation evaluation

Evaluation provides the feedback necessary to assess the value of information and performance of the system. It provides information about how successful is the system in satisfying the user's requirements and where it has drawbacks. Evaluation covers the following:

- Development Evaluation: Checks whether the system is developed on schedule & within the budget.
- Operation Evaluation: includes the operational aspects of the developed system. It is very essential that the developed system should be easy to operate and should work as per the user requirements.
- Information Evaluation: This evaluation is related to finding out the value of information that the developed system is providing to the user and how it is affecting the quality of decision making.

E. System Maintenance: Organizations have changing information requirements from time to time. Hence, the system requires to be modified to adapt to these changing requirements. Maintenance can be of 2 types:

- Schedule Maintenance (planned maintenance), includes antivirus run, updating run etc.
- Rescue maintenance, includes tackling situations which are not expected but have arisen etc.

A proper system operation requires the proper maintenance of system and the system staff should continuously plan and implement the required changes to provide the system utility in an optimum manner

CHAPTER 03
CONTROL OBJECTIVES

1. CONTROL

- Checks or management tools which are implemented to ensure that process or system willwork as per its intended purpose

- Types of control systems:

  - System development & acquisition controls
  - Control over system implementation
  - Control over system & program changes
  - Application controls
  - Logical access controls
  - Physical access controls
  - Environmental controls

- Classification controls:

- **General Controls:** those controls which are applicable to overall system components, processes & data for a given organization or systems environment. Include data centers & networking operations, system development & acquisition, system change & maintenance access & computer processing.

- **Application Controls:** those controls that are applicable to individual accounting subsystems such as payroll or accounting payable.

2. IMPORTANCE OF CONTROL

  - Information is an important resource
  - Increasing threats of various types to IS
  - Increasing need for regulatory compliance
  - IS is a set of integrated resources
  - Growing importance, education & awareness of information security & controls

3. EFFECTS OF COMPUTERS ON INTERNAL AUDIT

- Finance & accounting system has become more automated
- Changed the ways auditors used to carry out auditing
- Changed audit style from manual audit to ***audit around computers***, & then to ***audit through computers***

- Impact of computers in preparation & maintenance of financial books & reports:

  - **Changes in audit trail & audit evidence:**
    Reasons of changes in audit trail in computerized IS compared to manual system:

    - Data retention & storage
    - Absence of input documents
    - Lack of visible audit trail
    - Lack of visible output
    - Audit evidences
    - Legal issues

  - **Changes in internal control environment:**
    Following are used in both manual & computerized systems:
    - Personnel
    - Segregation of duties
    - Authorization procedures
    - Record-keeping
    - Access to assets & controls
    - Management & supervision & review

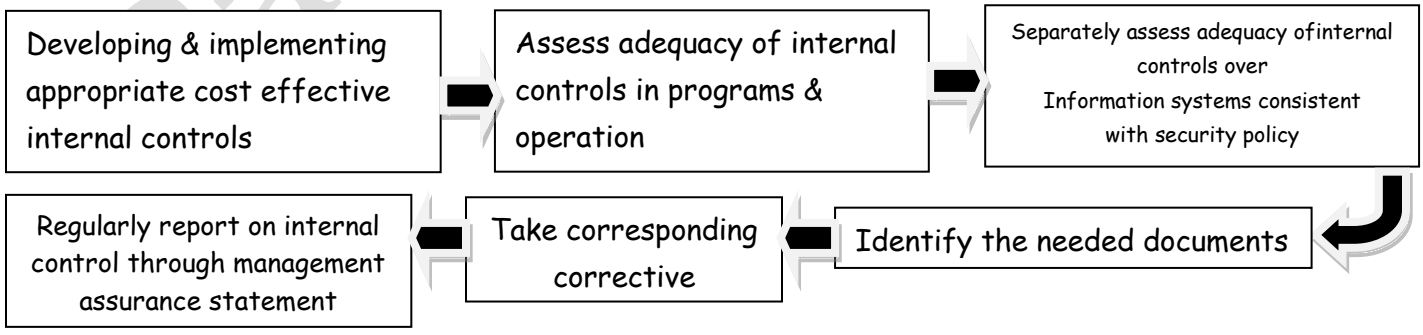
Following is the difference between manual & computerized systems:

- Concentration of programs & data

- New causes & sources of error:
  - System-generated transactions
  - Systematic errors

- New audit procedures:

4. RESPONSIBILITIES FOR IMPLEMENTING CONTROLS



5. CONTROL OBJECTIVES FOR INFORMATION RELATED TECHNOLOGY (COBIT)

- COBIT is a set of best practices or framework for IT management created by **Information Systems Audit & Control Association (ISACA)** & **IT Governance Institute (ITGI)** in **1996.**

- COBIT provides framework for:
  - Management
  - Users
  - Auditors

- COBIT provides a set of generally accepted indicators, processes & best practices to assist them in maximizing benefits derived through use of IT
- It helps in appropriate IT governance & controls in a company.
- Provides balance between risk & control investment in the IS environment

- COBIT framework addresses issues of controls effectiveness from three dimensions:
  - Business objectives
  - IT sources
  - IT processes

6. IS CONTROL TECHNIQUES

- Control framework primarily divides controls into 3 categories:
  - Accounting controls
  - Operational controls
  - Administrative controls

- COSO's Objectives for organizations:
  - Reliability of financial reporting
  - Effectiveness & efficiency of operations
  - Compliance with applicable laws & regulations

Auditor's categorization of controls:

- **Preventive Controls:** designed to an error or malicious activity in system. Devised by understanding probable threat, understanding vulnerabilities & exposure of assets for threats & finding necessary preventive controls to avoid probable threats.
- **Detective Controls:** used to detect errors or malicious activities in system. Devised by having clear understanding of lawful activities, using preventive controls & establishing detective controls which report unlawful activities.
- **Corrective Controls:** designed to reduce impact of errors or malicious activities by correcting errors & avoiding malicious activities in future. Help to minimize

impact of threats or problems, rectify issues & modify processing system to minimize future occurrence of problems.

- **Compensatory Controls:** where organizations can't implement preventive controls,
- compensatory controls are used.

7. AUDIT TRAILS
   - Audit trails used as detective controls.
   - Logs that can designed to record user activities on system & applications.
   - Help to accomplish security policy
   - Objectives of audit trail:
   - Detecting unauthorized access to system
   - Reconstruction of events
   - Personal accountability

8. SYSTEM DEVELOPMENT & ACQUISITION CONTROLS

➢ There are 3 major threats to system development & acquisition:
   - May consume excessive time & resources
   - May not be developed as per requirement
   - May contain unauthorized/ fraudulent instructions

➢ Following components can be uses to protect system from above problems:
   - Developing strategic master plan
   - Use project control techniques:

❖ System authorization
❖ User involvements
❖ Technical design
❖ Testing
❖ Internal auditor's involvement
❖ User acceptance & testing

   - Proper data processing schedules
   - Measuring system performance:

❖ Response time
❖ Utilization
❖ Stress test
❖ Throughput
❖ Post-implementation review

   - Post-implementation review

9. CONTROLS OVER SYSTEM IMPLEMENTATION

- Once system is developed & ready, User Acceptance Test is carried out. Its aim is to confirm that:
  - User requirement specifications are met
  - Operational documentation is accurate, comprehensive & usable
  - Helpdesk & other ancillary functions are properly operating
  - Back-up & recovery procedures will work effectively

- Acceptance testing includes:
  - Performance testing
  - Volume testing
  - Stress testing
  - Security testing
  - Procedure testing
  - Back-up & recovery
  - Parallel operation
- Auditor's validations for user acceptance & testing:

  Auditor has to ensure & verify that:

  - An acceptance test plan has been drawn up
  - A manager with adequate authority has been appointed to handle proceedings
  - Testing is working in actual environments
  - Proper data conversion plan has been developed considering all material issues
  - Adequate controls exist to prevent unauthorized changes from being made
  - Proper resources are available
  - Responsibility allocation is complete
  - Ensure that end-users are fully involved

- Post-implementation review (PIR):

  PIR must evaluate whether the implemented system has met its:
  - Business objectives
  - User expectations
  - Technical requirements

10. CONTROLS OVER SYSTEM & PROGRAM CHANGES

- Following controls should be used for control over system & program changes:
  Change management controls
  - Authorization controls
  - Documentation controls
  - Testing & Quality controls

11. CONTROLS OVER DATA INTEGRITY & SECURITY

- Information classification is done as per level of sensitivity of information. Information is to be classified under:

  - Top secret
  - Highly confidential
  - Proprietary
  - 'for internal use'
  - Public documents

- Data integrity aims to prevent, detect & correct errors in transactions as they flow through various stages of data processing. Further, data integrity helps protect data from malicious or accidental data alteration or destruction & provide assurance about quality & integrity of information to the users.

There are 6 data integrity controls:

- Source data controls
- Input validation routines
- Online data entry controls
- Data processing & storage controls
- Output controls
- Data transmission controls

12. ACCESS CONTROLS

IS has two types of access:

- Logical access
- Physical access

13. LOGICAL ACCESS CONTROLS (LAC)

- Objectives:

  - Only Authorized access to system
  - Restrict users to only authorized transactions
  - Restricted access of network to authorized only
  - Protecting system from malicious programs & viruses
  - Helps to protect integrity of application & data

- Types of Logical Access Paths:

  - Online terminals
  - Operation console (directly connected to servers)
  - Dial-up ports
  - Telecommunication links
  - Batch processing

- Possible exposures/ revelations in losses:

  - Technical exposures
  - Asynchronous exposures (attacks)
  - Loss of exposures

- LAC violators:

  - Hackers
  - IS Personnel
  - End users
  - Former employees
  - Interested or educated outsiders
  - Competitors & crackers
  - Part-time & temporary personnel

- Types of LAC:
  - Using User-id & password
  - Using access control
  - Using data encryption
  - Using firewall
  - Using network monitoring

- Access of Control mechanisms:

- Identification & authentication
- Authorization

- Audit of LAC: Role of IS auditor:

  - Review relevant documents relating logical access & associated risks
  - Review potential unauthorized access paths
  - Review working of various logical access controls
  - Review password policy of organization

14. PHYSICAL ACCESS CONTROLS

- Reasons of physical access violations:
  - Abuse of data processing resources
  - Embezzlement or fraud
  - Blackmailing or revenge
  - Damage to equipments & resources
  - Theft of equipments & resources
  - Public disclosure of sensitive information

- Physical access violations are mostly done by:

  - Ignorant employees
  - Former employees
  - Striking employees
  - Interested or informed outsiders

- Audit of physical access controls:

- Assess various threats & risks to facilities
- Review controls used to avoid these threats & risks
- Observe & test controls to protect hardware facilities, computer terminals

15. ENVIRONMENTAL CONTROLS

- Primarily due to elements of nature.

- Common environmental threats are:
  - Fire damage
  - Water damage/ flooding

- Power strike
- Electrical shock
- Natural disasters
- Equipment failure
- AC failure
- Bomb threat/ attack

16. SECURITY CONCEPTS & TECHNIQUES

- Cryptosystems
- Data encryption standards
- Private key encryptions
- Public key infrastructure
- Firewall

CHAPTER 04
TESTING – GENERAL & AUTOMATED CONTROLS

- Testing is a process to verify correctness, completeness & quality of developed software or any other product. It is known as criticism or comparison. It helps to verify that developed software or product would be working, as it is intended to.

1. SOFTWARE TESTING FUNDAMENTALS

Following rules to be followed as software testing fundamentals:

- ✓ Testing objectives:
  - Program with an intention to find errors
  - Having high probability of finding yet undiscovered errors
  - Uncovering a yet undiscovered error

- ✓ Starting time of test:
  - Should start as early as possible in life cycle as early testing helps to reduce errors

- ✓ Cause of bugs:
  - Specifications
  - Design
  - Coding

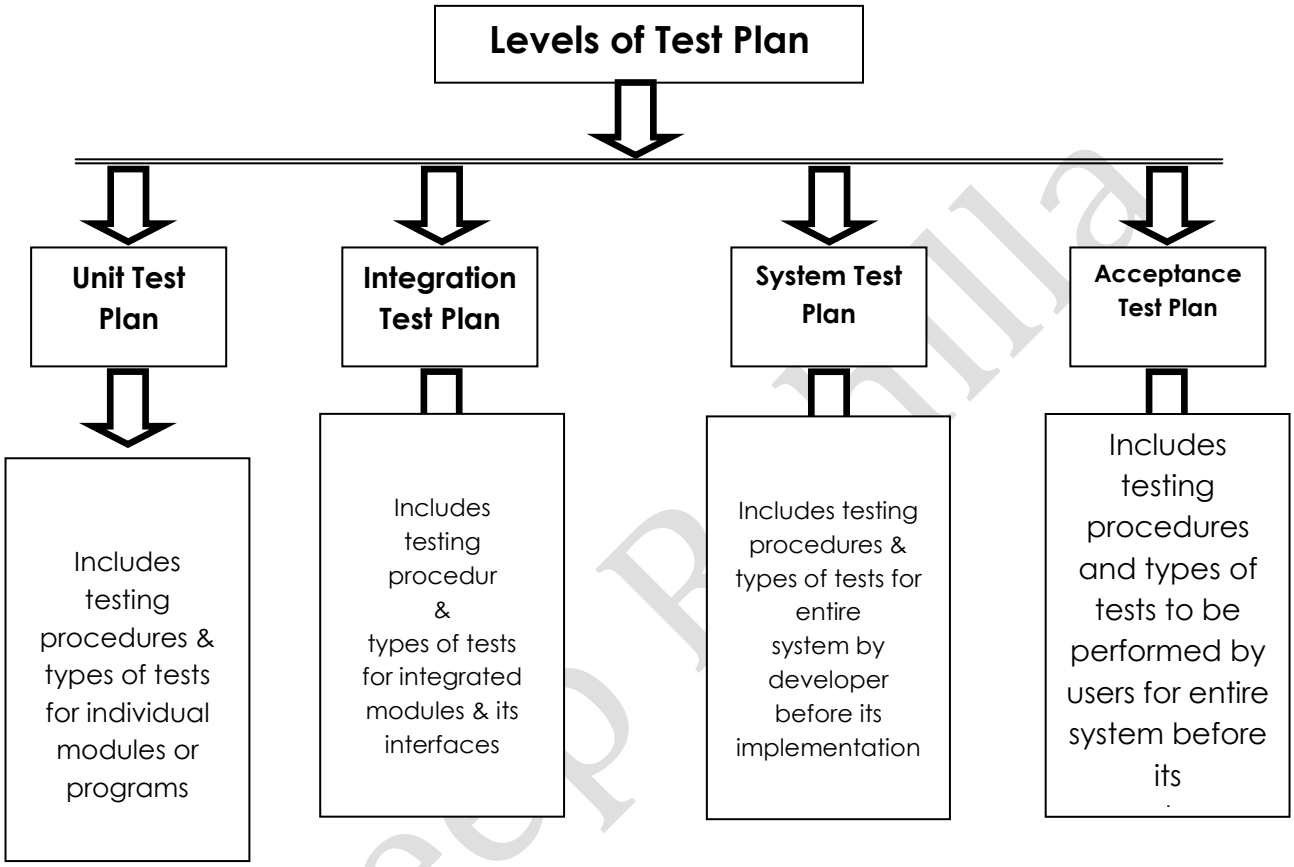
- Testing costs:
  - Costs increase manifold if bugs not detected on time. Fixing bugs at early stages of life cycle will cost less.

- Stopping time of testing:
  - When deadlines are met
  - When test cases are completed
  - When testing budget is depleted
  - Rate of finding bugs is too small
  - Risk in project found to be under acceptable limits

- Testing strategy:
  - Specific

- Practical justified

2. LEVELS OF TEST PLAN



3. TEST PLAN OUTLINE

a) Background
b) Introduction
c) Assumptions
d) Test items
e) Features to be tested
f) Features not to be tested
g) Approach
h) Test item pass/ fail criteria
i) Suspension/ resumption criteria
j) Test deliverables
k) Environmental needs
l) Responsibilities
m) Staffing & training
n) Schedule
o) Resources
p) Risks & contingencies
q) Approvals

4. TYPES OF SOFTWARE TESTING

- **Static testing:** used for verification activities. To check whether work being done is as per is as per set standards of organization.

- **Dynamic testing:** involves working with software, giving input values & checking if output is as expected. Includes validation activities, unit tests etc.

5. BLACK BOX TESTING

- Treats software as a "black box, without any knowledge of internal implementation"
- Valid & invalid inputs selected to determine accuracy of outputs
- Mainly concerned with correct acceptance of inputs & relevant outputs
- Applicable to all levels of testing
- Can cover unimplemented parts also
- Testing method includes:
  - Equivalence partitioning
  - Boundary value analysis
  - Cause effect graphics techniques

- **Equivalence Partitioning:** software testing technique that divides input data of software unit into partition of data from which test cases can be derived. Tries to define test cases that uncover classes of errors. Its goals are: **1)** to reduce number of test cases to necessary minimum & **2)** to select right test cases to cover all possible scenarios.
- **Boundary Value Analysis (BVA):** since more application errors occur at boundary levels of input domain, BVA is used to identify errors at boundaries rather than finding them in center of input domain.
- **Cause Effect Graphing Techniques (CEG):** provides a concise representation of logical conditions & corresponding actions. Performed once requirements have been reviewed for ambiguity & content is reviewed. There are 4 steps if CEG: Causes & effects listed for a function Development of cause-effect graph Graph converted into decision table Decision table rules converted to test cases

6. WHITE BOX TESTING

- Used when tester has access to internal data structure & algorithms & also access to
- implement these algorithms
- Provides test cases for testing internal structure of programs
- Used to test all details of software for:
  - Logical errors &
  - Syntax errors (typographical errors)

Types of tests used:
Basis path testing: every path of program is derived & tested. Ensures that every statement is executed & tested at least once, takes help of flow graphs to simplify derivations of each path.
Loop testing: focuses exclusively on validity of loop constructs. There are four different classes of loops: *simple loop, nested loop, concatenated loop & unconstructed loop.*

7. UNIT TESTING

- Software verification & validation method where programmer gains confidence that
- individual units of source code are fit for use.
- Done by stepping through each & every line of code.
- A unit test is a method of testing the correctness of a particular module of source code & write test cases for every function in module such that each test case is separate from others.

- **Benefits:**
  - Encourages change
  - Simplifies integration
  - Documents the code

- **Limitations:**

  - Cannot capture every error in program
  - Cannot catch integration errors

8. REQUIREMENT TESTING

- Helps to ensure that system's requirements communicated by users are correct &
- requirements are correctly understood & specified by developers for further system development.
- Helps in developing correct system in efficient manner

- **Objectives:**

  - To ensure that system's requirements are correctly communicated & specified
  - To ensure that system performs correctly for sustainable & considerable period of time
  - To ensure successful implementation of user requirements
  - To ensure that all user needs are fulfilled
  - To ensure compliance organization's policies & procedures

- **Advantage:** minimizing extensive re-work by minimizing requirements-related defects that could have been prevented/ rectified earlier.

9. REGRESSION TESTING

- "The process of testing changes to computer programs to make sure that older programs still work with new changes."

- A regression test re-runs previous tests against changed software to ensure that changes made in current software do not affect functionality of existing software.

- **Objectives:**
  - To ensure that older programs still work with new changes
  - To ensure that documents remain updated as per new software
  - To ensure that test-data & test-conditions remain updated as per changes

- To be used when there is high risk that new changes may affect unchanged areas of application software.
- Used in both development & maintenance phases of software.

10. ERROR HANDLING TESTING

ERROR HANDLING refers to the detection and resolution of programming, application and communication errors. There are 2 types of errors:

a. Development error (also known as syntax and logical error) – Happens due to typing mistakes or incomplete logics; and
b. Run time error – Happens due to invalid inputs

Error handling testing means establishing that all error handling procedures are in place for applications, i.e. errors will be detected and handled as per set guidelines.

Error handling Objectives are:

- Applications recognizes all expected error conditions,
- High probability that errors will be corrected, and
- Reasonable controls will be maintained for error corrections

11. MANUAL SUPPORT TESTING

MANUAL SUPPORT means that certain functions will be performed by people rather than automated IS. Manual Support Testing is the testing of the manual support functions. Manual support testing is best done during the installation phase. It has the following objectives:

- Verify that manual support procedures are correct and documented properly
- Determine that manual support responsibilities are established & defined correctly
- Determine that manual support people are adequately trained
- Determine that manual support procedures are properly connected

12. INTER SYSTEM TESTING

Inter System Testing ensures that interconnection between various systems & applications work properly. It is done to ensure that:

- Parameters and data are correctly passed between linked applications and systems
- Proper coordination between working of different linked systems exists

13. CONTROL TESTING

Control is a check and it acts as a management tool to ensure that processing is performed in accordance to the intents of the management. It ensures that:

- Input data is accurate & complete
- Transactions being processed are authorized
- Audit trail is in existence
- Processes being used are efficient, effective & economical
- Processing meets the needs of the users

Methods to use control testing

- First, all risks are to be identified
- Testers should have negative approach
- Testers should run test data and ensure that controls are effective

14. PARALLEL TESTING

- It is done to ensure that the processing of the new application is consistent with respect to the processing of the previous system.
- The objective is to ensure that the new system performs correctly and to demonstrate the consistency and inconsistency between the 2 applications.

15. VOLUME TESTING

- It is the testing of the system when the maximum numbers of users are simultaneously active and when the database contains the greatest volume of data.
- The purpose of volume testing is to find out the weakness in the system with respect to its handling of large amount of data during the extended time periods.

16. STRESS TESTING

- The purpose of stress testing if to find defects in the system capacity of handling large

numbers of transactions during peak periods.

- Server testing deals with the quality of the application in the expected environment. The idea is to create a environment more demanding of the application than the one the application would experience during its normal course of operation.

17. PERFORMANCE TESTING

- System performance is generally assessed in terms of response time and throughput rates under different processing and configuration conditions.
- The performance problems are most often the result of the client or server being configured inappropriately.

The best strategy for improving client server performance is a three step process:

- 1st, execute controlled performance tests that collects data about volume, stress and loading tests.
- 2nd, analyse the collected data
- 3rd, examine and tune database queries.

18. CONTINUOUS AUDIT TECHNIQUES

- **Integrated Test Facility (ITF):**

  - Used in IS which is to be audited
    Auditor uses a dummy account for testing & reviewing. The dummy transactions do not affect IS.
  - Mainly used in online system
  - Test transactions can be submitted along with actual transactions on frequent basis without disrupting regular processing operations.

- **Snapshot Technique:**

- Involves having audit software taking pictures of transactions as it flows through an application system.
- Both before-images & after-images of transactions are captured
- Decision to be made regarding location of snapshot points & reporting of snapshot data captured

- **System Control Audit Review File (SCARF):**

- Similar to snapshot technique
- An embedded audit module is used to continuously monitor transactions & collect data

on transactions with special audit significance

- One of most complex online audit techniques
- The audit modules are placed at predetermined points to gather information about transactions which auditors deem to be material
- Two key decisions: what information to be collected & what reporting system to be used.

➢ **Continuous & Internal Simulation (CIS):**

- Embeds audit module in DBMS
- This can be used when application system uses DBMS
- Uses DBMS to track exceptional transactions

➢ Advantages of continuous audit:

- Timely audit
- Comprehensive & detailed auditing
- Surprise test capability
- Assessing whether IS meets set objectives
- Training for new users

➢ Disadvantages of continuous audit:

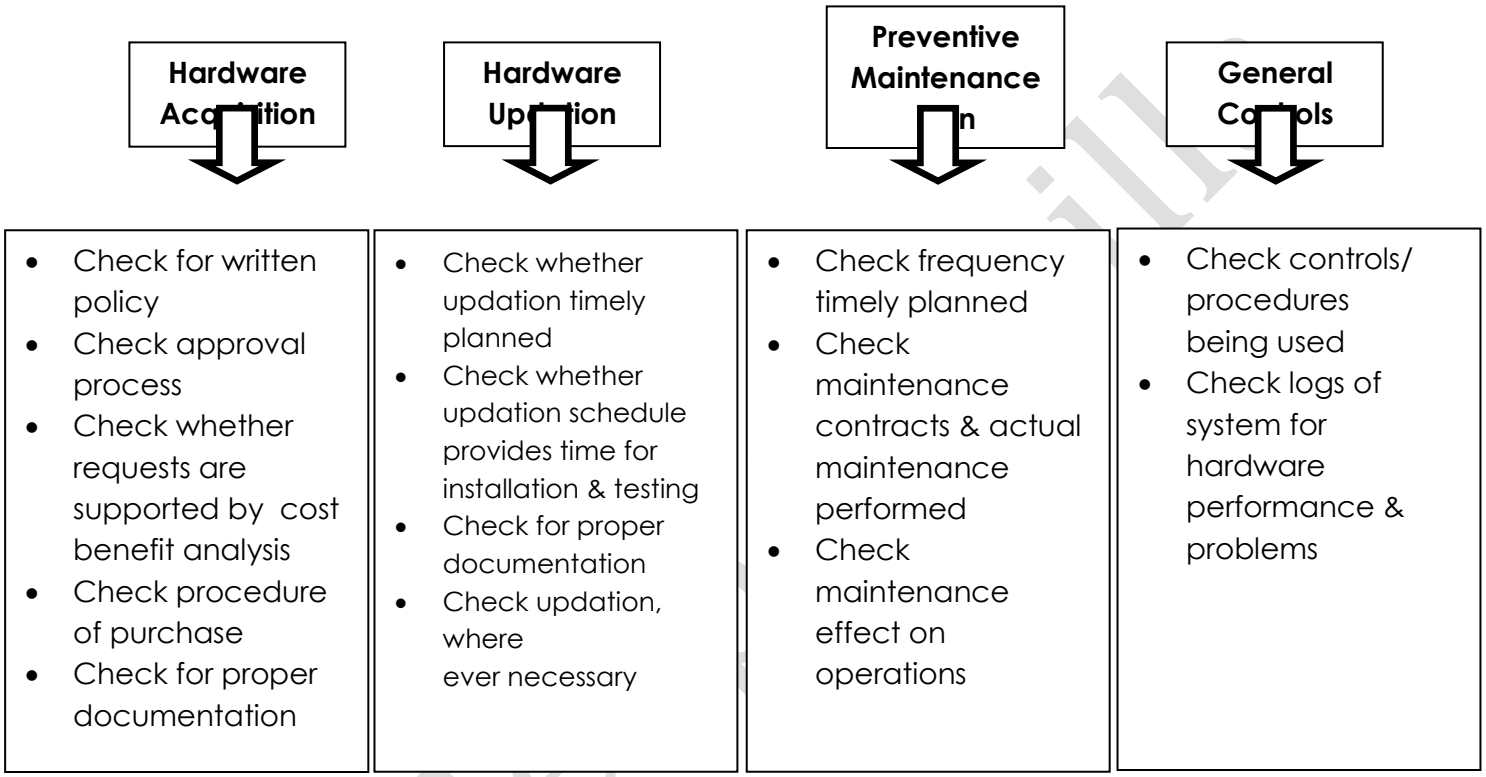
- Rationing of available resources
- Involvement in system development
- Expert knowledge of IS being used
- Missing audit trail
- Stable application system required for implementation

19. HARDWARE TESTING & REVIEW

- Normally, hardware should be tested for:
- Memory
- Performance
- Security
- Reliability
- Error handling/ exit testing
- Max. no. of users supportable
- Maintenance support
- Accessibility testing

➢ Auditor should review & audit procedures for:

Audit Review & testing of Hardware



20. OPERATING SYSTEM REVIEW

Here, the auditor reviews the procurement, implementation, execution and maintenance of system software such as operating system, in terms of:

- Approval process of software selection
- Cost / benefit analysis of system software procurement
- Controls over installation of the software
- System documentation
- Test software implementation
- System software security procedures

21. NETWORK REVIEW

- Network Audit Objectives
- Standards are in place for designing and selecting a LAN architecture
- Controls are there to ensure continuous working of LAN
- Ensure that there is cost benefit in operating a LAN

The reviewer / auditor of networks should have knowledge about networks, network topology, LAN technicalities etc. The auditor should review, test and validate the following controls for networks:

- Physical controls
- Logical controls
- Environment controls

CHAPTER 05
RISK ASSESSMENT METHODOLOGIES & APPLICATIONS

1. RISK

- It is the likelihood that an organization may be exposes to some threats that may cause harm to an organization.
- Reasons for occurrence of risk:

  - Use of new technologies
  - Extensive use of network applications
  - Use of distributed systems
  - Frequent technological changes
  - Easy-to-conduct & hard-to-detect electronic arracks
  - Decentralization of management & control
  - Unfavourable legal &regulatory requirements

- Possible impact on critical business operations:

  - Hacking, virus attack & leakage of corporate confidential information
  - Bad effects on privacy & ethical values
  - Danger to IS availability & robustness

2. DEFINITIONS

- **Threat:** An action or event which may cause harm to organization in terms of business continuity problems, disclosure of confidential information, data destruction &denial of information etc.
- **Vulnerabilities:** The weakness in the safeguard or security of the system that exposes the IS to various threats.
- **Exposure:** The extent of loss organization may face in case of risk. It is impact of occurrence of risk in immediate & longer term.
- **Likelihood:** The probability of occurrence of any risk.
- **Attack:** Actions which may compromise the integrity & confidentiality & other desired features of an IS. The type of attack & its degree of success determine the results or consequences of attack.
- **Residual Risk:** Any risk that still remains after all the security majors to prevent the risks are analyzed & implemented. Here, organization Management needs to consider two areas:
  - Acceptance level of residual risk
  - Selection of safeguards to be implemented to reduce overall risks to reach level of acceptance

As long as residual risks can be minimized & kept at acceptable level, the risks are considered to be managed.

3. THREATS TO COMPUTERIZED ENVIRONMENT

- Power loss
- Communication network failure
- Disgruntled employees
- Errors
- Malicious codes (programs)
- Abuse of access privilege by employees
- Natural disasters
- Theft & destruction of computing resources
- Downtime due to technology failure

4. CYBER CRIME & THREATS DUE TO CYBER CRIME

Cyber Crime is the general nomenclature for “electronic offences” due to increasing use of computer network & internet & frauds thereof.

Examples of cyber crimes:

- embezzlement
- unauthorized use of ATM/ DC/ CC
- theft of proprietary information
- denial of service
- vandalism or sabotage
- computer virus

5. RISK MANAGEMENT

The systematic application of management policies, procedures & practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, monitoring & communicating risk.

Risk Management Steps:

- **Risk Identification**
- **Risk Assessment:** process of analyzing & measuring risk to quantify risks to system
- **Risk Evaluation**
- **Risk Mitigation Development:** involving implementation of measures to reduce or eliminate some or all risks
- **Risk Mitigation Implementation**

- **Re-assessment/ Re-evaluation of risks**

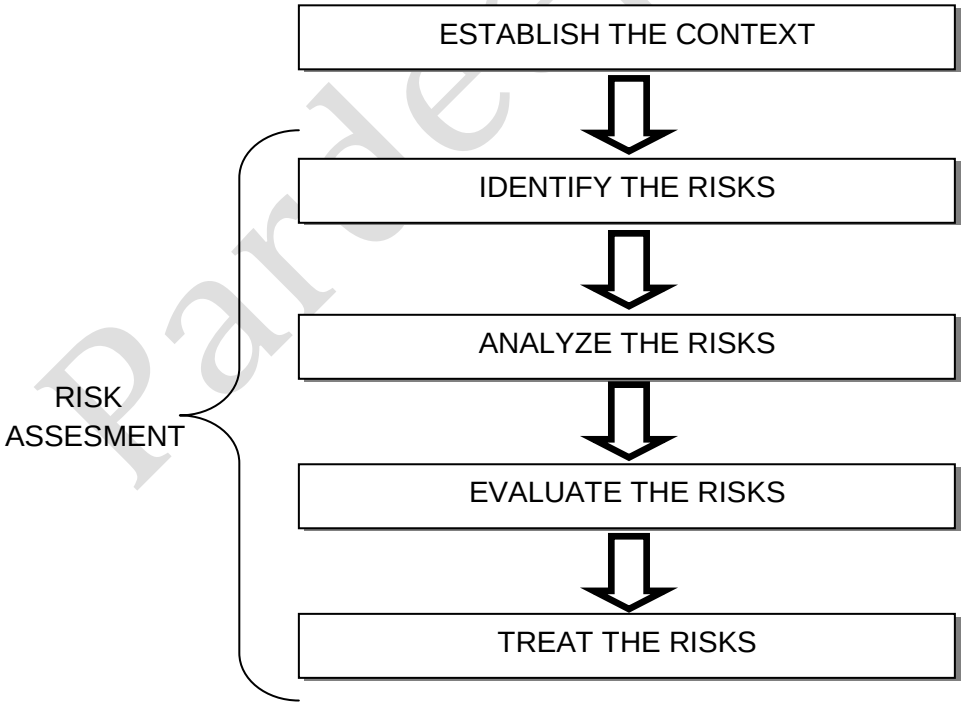
6. CLASSIFICATION OF RISKS

- **Systematic Risk:** normally avoidable risks; same for all organizations; primarily from external factors; organizations have little control over them
- **Unsystematic Risk:** specific & unavoidable risks; from specific application or technologies

7. RISK IDENTIFICATION

- Purpose is to identify various risks inherent to performing business functions, especially w.r.t. use of IT
- Risk identification should be comprehensive
- Risk identification should be for operations, financial objectives & compliance
- Questions to be asked:
  - What assets to be protected
  - What could go wrong with assets
  - How could we fail to deliver
  - What are various threats to A & L
  - What info. to be relied upon
  - What is greatest legal, financial & operational exposure

8. RISK ASSESSMENT & EVALUATION PROCESS



RISK = PROBALILITY OF DISRUPTION x POSSIBILITY OF EXPOSURE

Purpose of risk analysis & evaluation:

- Identify probability of failures & threats
- Calculate the exposure

9. RISK ASSESSMENT & EVALUATION TECHNIQUES

- Judgement & Evaluation
- Delphi Techniques
- Scoring Approach
- Quantitative Techniques

10. RISK ASSESSMENT

- Process used to identify risk factors, & then analyse & evaluate tie identified risk factors to develop an appropriate risk mitigation plan
- Provides an effective approach that serves as foundation to avoid losses
- Helps to identify, assess & mitigate risks
- Includes development of clear summary of current situation & systematic plan to identify, assess & mitigate risks
- In general, includes the following for protection of an IS & its applications:
  - Prioritization
  - Identifying critical components & applications
  - Assessing their impact on organization
  - Identification of exposures & implications
  - Determination of recovery-time period
  - Assessment of Insurance coverage
  - Development of recovery plan

11. RISK RANKING

- Technique to measure impact of potential risks
- Requires that each component & application be analyzed separately before ranking
- Two quantitative parameters used for ranking:
  - Probability of occurrence
  - Possible impact or exposure of threats

- Considering & analyzing risk impacts & probability of occurrence includes:
  - Investigating the frequencies of particular types of disaster
  - Determining the degree of predictability of disaster
  - Analyzing speed of occurring impact of disaster
  - Determining amount of forewarning associated with disaster
  - Estimating situation of disaster
  - Considering impact of disasters if vital records are destroyed/ not destroyed
  - Identifying consequences of disaster
  - Estimating potential loss
  - Determining cost of contingency planning

12. RISK MITIGATION

- Means avoiding risks
- Should be based on probability of occurrence of risk & severity of risk in terms of losses
- Some risk mitigation measures are:
  - Creating supportive environment
  - Strengthening internal controls
  - Establishing reserve funds
  - Setting up of operational risk limits
  - Setting up independent operational risk management departments
  - Establishing disaster recovery plan
- Common risk mitigation techniques:
  - Insurance
  - Outsourcing
  - Service Level Agreements

13. RISK & CONTROLS

Excessive Risk leads to:	Excessive Control leads to:
❖ Loss of assets	❖ Increased bureaucracy
❖ Poor business decisions	❖ Reduced productivity
❖ Non-compliance	❖ Increased complexity
❖ Increased regulations	❖ Increased processing cycle-time
❖ Increased frauds	❖ Increase of activities having no value

CHAPTER 06
BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY PLANNING

1. BUSINESS CONTINUITY PLANNING

- Defines the plans to avoid crisis & disasters, and in case crisis & disasters occur, then, it defines plans for immediate recovery from these.
- Defines steps, plans & procedure for continuance of business activities irrespective of any situation.
- BCP covers three important areas:
  - Business Resumption Planning
  - Disaster Recovery Planning
  - Crisis Management
- Following resources play an important role in **Business Continuity Life Cycle:**
  - IT & Telecommunication
  - Business Processes
  - People
  - Liquidity
  - Facilities
- The above resources are assigned based on following Business Continuity Life Cycle assessment:
  - Risk Assessment
  - Determination of Recovery
  - Alternatives
  - Recovery Plan Implementation
  - Recovery Plan Validation

2. OBJECTIVES OF BCP

- 'Objectives' are used for 'long-term aim' & 'Goals' are used for 'short-term aim'
- Objectives:
  - Safety to people at time of disaster
  - Immediate resumption of critical business operations
  - Minimization of losses
  - Minimum resource disruption
  - Reduce complexity of recovery tasks
  - Ensuring effective co-operation of recovery tasks
  - Establish required emergency powers & management succession
- Goals:

- Identify weaknesses & implement DRP accordingly
- Minimizing duration of serious disruption to business operations

3. DEVELOPING BCP

➢ General aspects of sound BCP:
- Provide a complete understanding of efforts required to maintain effective DRP
- Develop easy-to-maintain, understand & implement DRP
- Document possible losses, recovery tasks & procedures
- Integrate the BCP into ongoing other business planning processes
- Select proper BCP team
- Focusing on preventing disaster, minimizing impact of disasters & orderly & timely recovery from disaster

➢ Phases of BCP:
- **Pre-planning:** understanding existing & projected business operations; establish a steering committee; develop a policy to support BCP; provide awareness & education
- **Vulnerability Assessment:** analyse possible threats/ disasters; assess all security measures
- **Business Impact Analysis (BIA):** identify critical systems, process & functions & assess economic impact of various incidents. Use questionnaire, workshops, interviews & examine documents.
- **Detailed definition of requirements:** requirements classified into short-term, mediumterm & long-term
- **Design & develop BCP Plan:** two aims:- business recovery & technical recovery
- **Testing:** ensure recovery procedures are complete & workable; adequate competence of personnel; availability of resources; workability of manual procedures; proper training of BCP programmes
- **Implementation:** implement selected plan; define periodic test schedules; define test approaches; identify test types with procedure to conduct tests; analyse test results; modify plans as per maintenance program
- **Maintenance:** determine ownership of responsibility for maintenance; identify events which may trigger maintenance of BCP; ensure proper maintenance & updation of plan

4. TYPES OF DRP (Disaster Recovery Sub-plans)

➢ **Emergency plan:** identify who is to be notified immediately; actions to be undertaken on priority
➢ **Back-up Plan:** decide what back-up to be maintained; resources to be considered for backup
➢ **Recovery Plan:** explains steps to be taken to recover immediately from disaster; decide which applications to be recovered first

- **Test Plan:** frequently test to check whether all plans are properly functioning

5. THREATS MANAGEMENT

- Potential Threats:
  - Human errors
  - Equipment failures
  - Electricity/ communication outages
  - Natural disasters
  - Virus attack/ hacking
  - Outsourcing

- Threats may cause:
  - Loss of data integrity
  - Loss of data confidentiality
  - Loss of system availability
  - Unauthorized access to system
  - resources
  - Industrial espionage

- Possible appropriate controls:
  - Data encryption
  - Installing firewall
  - Use of data validation &
  - reconciliation
  - User identification & authentication
  - Updated anti-virus
  - Regular back-up
  - Audit trail control
  - System & network monitoring

- **Single Point of Failure Analysis:** a particular failure may disrupt entire services in organization.

6. SOFTWARE & DATA BACK-UP TECHNIQUES

- **Full back-up:** all files entirely backed-up; restores entire sessions' data; stored in **.zip** format
- **Differential back-up:** all file changes from last full back-up are backed-up again
- **Incremental back-up:** only those files which have changed since last back-up are backedup; most effective & economical
- **Mirror back-up:** exact copy of files; stored in exact format in a parallel to original one

7. ALTERNATE PROCESSING FACILITY ARRANGEMENT

- **Cold Site:** maintains critical equipments & resources in duplicate form at some off-site location. In case of disasters, these resources & equipments operate from off-site. Lowcost, but does not provide 100% downtime elimination
- **Hot Site:** maintains critical equipments & resources in synchronized form at some off-site location. Most expensive, but nil downtime.
- **Warm Site:** between hot & cold sites. Better than cold, worse than hot sites.
- **Reciprocal Agreement:** two organizations maintain each-other's back-up to facilitate other in continuance of services in case of disaster. Each party maintains extra capacity to serve other's critical systems.

8. BACK-UP REDUNDANCY

- **Off-site back-up:** maintain at least one back-up at different location *(if the back-up is maintained at working location itself, it is active back-up)*
- **Multiple Back-up:** maintain same back-up in multiple disks
- **Media rotation:** rotate active back-up with off-site back-up to update off-site back-up with latest values

9. BACK-UP MEDIA TYPES & BASIS OF SELECTION

- Various types of back-up media are:
  - Floppies
  - CD
  - Magnetic tape
  - Disk Drive
  - Removable disks
  - Digital audio tape (DAT) Drives
  - Optical jukeboxes
  - Autoloader tape systems
  - USB Flash drives
  - Zip drive
  - DVD

- Selection of appropriate tools & back-up devices depends upon:
  - Speed
  - Reliability
  - Capacity
  - Extensibility
  - Cost

- Flexibility

- Back-up Tips:
  - Develop simple & easy-to-understand plan
  - Be organized
  - Utilize user-friendly software
  - Verify the available back-up
  - Restrict data storage privilege
  - Create a step-by-step guideline

10. DISASTER RECOVERY PLAN

- DRP is a document which includes all the procedures to be followed to recover from disasters
- A very detailed document which lists all procedures & plans.
- Also known as **DRP Document** or **DRP Manual**
- Includes:

  - Emergency plan
  - Recovery plan
  - Back-up plan
  - Test plan
  - Insurance

11. INSURANCE

- Considered to spread the cost & risk of loss from individual to large number of people
- Policies are obtained to cover loss of following:

  - Equipments
  - Facilities
  - Storage media
  - Business interruption
  - Extra expenses
  - Valuable documents
  - Accounts receivables
  - Third party damage claims

- Types of Insurances:
  - First party insurance
  - Property damage
  - Business interruption

- ❖ Third party insurance
- ❖ General liability
- ❖ Directors & officers

12. TESTING MEDHODOLOGY & CHECK-LIST

- Following tests are conducted for DRP:
  - **Hypothetical test:** paper test where verification of all procedures & actions specified in recovery plan are conducted
  - **Component test:** used to verify details & accuracy of individual procedures within recovery plan
  - **Module test:** combination of components is tested together for functionality
  - **Full test:** used to verify that multiple modules will recover immediately from any disaster. Main objective is to ensure that: **1)** total time for recovery meets set time objective & **2)** recovery plan is efficient & can be performed without obstacle

- Following methodologies are used for testing:
  - Setting test objectives
  - Defining boundaries
  - Defining scenarios
  - Setting testing criteria
  - Developing assumptions
  - Testing pre-requisites
  - Briefing sessions
  - Checklists
  - Analyzing the tests
  - Debriefing sessions

13. AUDIT TOOLS & TECHNIQUES FOR DRP

- Automated tools
- Internal control auditing
- Disaster & security check-list
- **Penetration Testing** *(used to locate specific vulnerabilities & threats)*

14. AUDIT OF DRP / BUSINESS RESUMPTION PLAN

Steps:

- Audit the methodology of DRP preparation
- Audit the back-up & recovery procedures
- Audit the test plan
- Audit the team & personnel responsibilities

CHAPTER 07
AN OVERVIEW OF ENTERPRISE RESOURCE PLANNING

1. INTRODUCTION

- ERP is a solution to overall business problems. It is an attempt to integrate the five major resources of an organization, i.e. Man, Material, Money, Machine & Market
- Involves managing a large volume of data, number of users & multiple system components

2. DEFENITION

- ERP is "Software solution that addresses the need of the enterprise by tightly integrating all functions of an enterprise."
- ERP is reengineering of the current business practices for more efficient & accurate functioning. It is a mix of software tools enabled with newly designed, well-planned business practices.

3. EVOLUTION OF ERP

Basic requirements of businesses to remain in competition:

- Aggressive cost-cutting
- Cost/ Revenue Analysis
- Flexibility to respond quickly to enhancing requirements
- Better-informed decision-making

To assist businesses in their needs, following IS were introduced:

- Management Information System (MIS)
- Integrated Information System (IIS)
- Executive Information System (EIS)
- Enterprise-wide Information System (EWIS)

The above IS lacked integration. Then,

- Materials Requirement Planning (MRP)
  Was introduced which integrated manufacturing process with other business IS.

MRP was further extended to include vendors, suppliers etc. through LAN & WAN. This was known as:

- Manufacturing Requirement Planning (MRP II)

- ERP evolved from MRP II.

4. ENABLING TECHNOLOGIES FOR ERP

Most of ERP systems use power of **Three-Tier Client/Server Architecture:**

In three-tier C/ST:

- Environment is stored on back-end database server
- Application logic/ business rules are stored on middle ware
- Presentation for data entry & viewing is kept at client workstation

To facilitate online transactions, other important enabling technologies for ERP systems are:

- Workflow,
- Work group,
- Electronic Data Interchange,
- Internet & Intranet; and
- Data warehousing.

5. CHARECTERISTICS OF ERP

- Flexibility
- Modular & Open
- Comprehensive to support wide range of functionality
- Ability to connect with external databases
- Employ best business practices & processes
- Incorporate use of latest technologies

6. FEATURES OF ERP

- Comprehensive
- Supports business process integration
- Provides end-to-end supply chain management solutions
- Provides customer relations management solutions
- Bridges information gap across organization
- Inter-group system integration
- Automatic use of latest technologies like EFT, EDI, Data Warehousing & E-commerce
- Provides intelligent business tools

7. BENEFITS OF ERP

- Tangible Benefits

  - Reduction of lead time
  - On-time logistics
  - Increased business activities
  - Reduction in transaction processing cycle time
  - Reduction in inventory of raw material, WIP & finished goods
  - Accurate and updated information at any instant

- Intangible Benefits

  - Better customer satisfaction
  - Improved vendor performance
  - Reduced quality costs
  - Increased flexibility
  - Improved resource utility & decision making capability

BUSINESS PROCESS RE-ENGINEERING

8. DEFINITION

- BPR aims to achieve dramatic improvement by major transformations of business processes.
- BPR is the fundamental rethinking, radical redesign and reinventing of business processes to achieve dramatic improvement in terms of cost, quality, service and speed.

9. MAJOR PRINCIPLES OF BPR

- Single point responsibility for any business process
- Continuous communication and coordination between people performing work in parallel
- Common on-line storage form of database

10. BUSINESS ENGINEERING

Business Engineering is the merger of two concepts. It combines the innovation of information technology with BPR to focus on better business processes. The main thrust of business engineering lies in far reaching, best procedure based, process oriented solutions; which have been greatly enhanced by client / server computing.

11. ROLE OF BPR IN ERP

The basic objective of implementing ERP is to put in place the application and infrastructure

that support organization's business plans & processes in the best possible manner. Thus, BPR is mandatory for successful ERP implementation.

12. BUSINESS MODELING

- The first step in ERP implementation is to carry out BPR by development of business process model showing business processes as one large system with interconnection and sequence of business subsystems and processes. This development of business process model for present and required business process is known as Business Modeling.
- Business modeling is not a mathematical model, but the representation of business as one large system with interconnection and sequence of business subsystems and processes.
- It is kind of diagrammatical and tabular representation of various business processes in an interconnected manner with their underlying data models. First, an existing business model is prepared and based on that, another business model consisting the required business model is prepared.

Business model consists of two main elements:

a. Blue print describing various business processes and their interactions

b. Underlying data model.

13. ERP IMPLEMENTATION – STEPS

a. Identification of the needs for implementing the ERP package
b. Evaluating the as-is situation of the business
c. Deciding upon the would-be situation of the business
d. Conducting of BPR
e. Evaluation of various ERP packages
f. Finalization of the ERP package
g. Installing required hardware & networks
h. Finalizing the implementation consultant
i. Implementation of ERP.

14. GUIDELINES FOR ERP IMPLEMENTATION

1. Understanding the corporate culture and needs
2. Complete business process changes
3. Communicate across the organizations
4. Provide strong leadership
5. Ensure availability of effective, efficient & capable project manager

6. Create a balanced team
7. Select a good implementation methodology
8. Proper & extensive training
9. Commitment of adapting to changes

POST IMPLEMENTATION SCENARIOS

15. EXPECTATIONS

- An improvement in processes
- Increased productivity on all fronts
- Total automation & disbanding of all manual processes
- Improvement of all Key Performance Indicators (KPI)
- Elimination of all manual records
- Availability of real time information systems
- Total integration of all operations

16. FEARS

- Job redundancy & change of job profile
- Loss of importance
- Loss of proper control & authority
- Increased stress due to greater transparency

17. LIFE AFTER IMPLEMENTATION

- Organizations should prepare a list of Critical Success Factors (CSF) & their corresponding KPIs and continuously evaluate the processes against KPI
- CSF is a process name which is critical to the successful working of the organization. Some general CSF are:

  - Transaction processing time
  - Product delivery time
  - Customer complaint response time
  - Labour productivity
  - Quality of product
  - Consumption of resources

- All these CSF have some sort of KPI, i.e. can be quantified in a value known as KPI, which is a continuously changing value.
- Both CSF and their corresponding KPI are defined through BPR.
- Some other tasks to be performed post-implementation are:

- Develop new organization structure and job descriptions
- Determine the skill gap between the existing and required jobs post ERP implementation
- Assess training requirements and implement a proper training plan
- Develop and amend HR, Financial & Operational Policies to suit ERP environment

18. POST IMPLEMENTATION PROBLEMS

- Changing CSF due to changing business environment & corresponding new KPI which require change in processes
- Continuous improvement in technologies

19. LIST OF POPULAR ERP PACKAGES

- BAAN
- MFG / Pro
- ORACLE
- SAP R/3
- JD Edwards

20. BRIEF DESCRIPTION OF CAPABILITIES OF ERP SOFTWARE PACKAGES

SAP AG has developed an ERP package called “SAP R/3”. It is the most popular package and considers the entire business as a single entity. It is a unique system that supports nearly all areas of business on a global scale.

SAP has a number of application modules in the package. Some of these are:

1. Financials
2. Cost control
3. Investment management
4. Treasury management
5. Integrated enterprise management
6. Product data management
7. Sales & distribution
8. Production, planning & control
9. Materials management
10. Human resource management

CHAPTER 09
DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING – A PRACTICAL PRESPECTIVE

1. INFORMATION SECURITY

- Information security means protection of information, which means processed data and this data, is protected against loss, inaccessibility, alteration or wrong disclosure.
- The protection of the interest of those relying on the information and information system and communications that deliver the information, from harms, failures of availability, loss of confidentiality and integrity

2. OBJECTIVE OF INFORMATION SECURITY

- Availability – IS are available and usable when required
- Confidentiality – Information is disclosed only to those who have the right to know it
- Integrity – Information is protected against unauthorized modifications

3. IMPORTANCE OF INFORMATION SECURITY

- Increased dependence of organizations on information
- Information spread geographically and accessed through networks, which are vulnerable
- Organizations depend upon timely, complete, reliable and valid information
- IS are increasingly, coming under threats from internal and external sources
- Security failure may result in both financial and intangible losses

4. SENSITIVITY OF INFORMATION

Following types of information are normally considered sensitive information:

- Strategic Plans: They are very crucial for success of organization and it is required that these plans should be well protected
- Business Operations Information: Business operation consists of organization process and procedures, information of which of proprietary in nature, whose secrecy is to be well guarded
- Financial Information are very crucial and not to be made public

5. PURPOSE AND SCOPE OF INFORMATION SECURITY POLICY

- Purpose is to define, what the organization is trying to accomplish through security policy for IS and its information

6. FACTORS DECIDING LEVEL OF SECURITY OF INFORMATION

- Value of information
- Place of critical data (How information is placed)
- Type of storage media
- Hardcopy output of information
- Access to information (Who all should be provided access)

7. CORE PRINCIPLES OF INFORMATION SECURITY

- Accountability
- Awareness
- Multidisciplinary
- Cost efficient
- Integration
- Reassessment
- Timeliness
- Societal factors

8. INFORMATION PROTECTION METHODS

- Preventive Protection: This is based on use of security controls. This is based on three types of controls, i.e. Physical controls, Logical controls and Administrative controls.
- Restorative Protection: It is necessary to have an effective and timely information backup and recovery plan. The main requirement is that information lost can be recovered.
- Holistic Protection: Protection should be done in such a way that it gives business, appropriate level of security at a cost acceptable to business.

9. METHODS TO IMPLEMENT INFORMATION SECURITY

- **Security Policy:** Security policy sets the acceptable norms for information access and also set out reactions of organization when such norms are violated. A good security policy should provide for procedures and policies that can prevent losses and also help in increasing productivity. The main aim of the policy should be to recognize the value of, and the dependence on, the information of the organization Policy Development: The security policy must be developed on the basis of security objective and core principles of information security. The security policy so developed should also support and complement the existing organization policy.
- **Roles & Responsibilities:** For security to be effective, it is necessary that individual roles, responsibilities and authorities are clearly defined, communicated and understood by all. Design: Design consists of standards, measures, practices and procedures within which, systems and individuals would function and maintain. System should be designed based on the need of the organization.
- **Implementation:** Various controls should be implemented for an effective information

security like:

- Managerial controls
- Identification and authentication controls
- Logical access controls
- Accountability controls
- Cryptographic controls
- SDLC controls
- Physical environment controls
- Computer support and operational controls
- Business continuity & planning controls

- **Security Monitoring:** System established should be continuously monitored to detect and ensure correction of security breaches and acted upon. Monitoring ensures ongoing compliance of policy, standards and security practices.
- **Awareness Training & Education:** All employees should be aware of security policies and its importance. Regular training programs are needed in this regard. Achieving security objectives is not one time implementation but is a mission.

10. INFORMATION SECURITY POLICY

The security policy is a set of laws, rules and practices that regulates how assets and information are managed, protected and distributed within the organization. A policy addresses many issues related to information such as disclosure, integrity and availability issues.

An information security policy discusses the following in detail:

- Issues to address

  - Definition of information security
  - Importance of information security
  - Goals & principles of information security
  - Information security standards

- Members of security policy

  - Management authorities
  - Technical staff
  - Legal experts

11. TYPES OF INFORMATION SECURITY POLICIES

- User Security Policy sets out the responsibilities and requirements from the users of the information system
- Acceptable Usage Policy defines the rules for email and internet services
- Organizational Information Security Policy defines the group of policies for security of the information and information systems
- Network & System Security Policy defines rules for network & Data communication systems
- Information Classification Policy defines the rules for classification of information
- Conditions of Connection define the rules for access of network and it specifies the conditions to be satisfied for connecting to different networks

12. COMPONENTS OF THE SECURITY POLICY

- Purpose and scope of policy and its audience
- Security organization structure
- Classification of assets and their inventory
- Roles and responsibilities of people connected
- IS and its security infrastructure
- Access control mechanism
- Physical and environmental security
- System development and maintenance controls
- Network and data communication controls
- Business continuity planning
- Security incident response and reporting mechanisms

13. RESPONSIBILITY ALLOCATION IN SECURITY POLICY

- An owner should be appointed for each information asset
- All new network communication link must be approved
- Risk assessment for all third party access to information assets and the IT network must be carried out
- A conditions of connection agreement in place for all third party connections

14. INFORMATION ASSET CLASSIFICATION

- An inventory of IS's assets should be defined
- Assets should be classified as per their importance of value, in the policy
- Handling of information must be approved
- Exchange of data must be controlled
- Classified waste information must be disposed off appropriately

15. ACCESS CONTROLS

Access control (AC) is considered as very important mechanism to provide information security. Following rules should be part of policy under access control mechanism:

- AC must be in place to prevent unauthorized access to IS
- Access of business information should be permitted in response to a requirement
- Formal process must be in place to validate and provide individuals with access to information
- Access controls should be regularly audited
- Access rights should be immediately deleted for users who do not need the information any further
- Each user must be provided with unique IDs and should be prohibited from using another user's IDs.
- Proper procedures should be in place for reporting and handling of security related incident(s)

16. INCIDENT HANDLING

- Recording activities on system
- Training staff to inform immediately when security breach happens
- Procedures for security administrator to handle breach & control future activities
- Policies to lay out extent of testing to be done under various phases of audit (planning, compliance testing & substantive testing)

17. CAUTIONS ON ACCESS RIGHTS FOR IS AUDIT

Audit policy should determine when & to whom audit results should be reported. It should define access rights to be given to auditors & must include:

- User/ system level access to any computing or communicating device
- Access to information that may be produced, transmitted or stored on dept. equipments
- Access to work areas
- Access to reports/ documents relating to internal audit
- Access to network traffic

18. AUDIT WORKING PAPERS & DOCUMENTATION

- Working papers should include:
  - Audit plan
  - Nature of audit
  - Timing of audit
  - Details of audit procedures performed
  - Conclusions drawn from evidences obtained

- In case of recurring audit, some papers may also be classified as permanent:
  - Organization structure
  - IS policies of organization
  - Historical background if IS in organization
  - Record of internal controls related to IS
  - Copies of previous audit report
  - Copies of management letters issued by auditors

- Planning documents:
  - Knowing available resources
  - Knowing the audience
  - Knowing scope of work

- Finalizing documents:
  - Thoroughly tested & revised documents
  - Proper glossary & index
  - Proper format

19. CONTENTS OF IS AUDIT REPORT

- Cover & title page
- Table of contents
- Executive summary
- Introduction
  - Context of IT environment
  - Purpose of audit
  - Scope of audit
  - Methodology used for audit
- Findings
- Opinions
- appendices

CHAPTER 10
INFORMATION TECHNOLOGY ACT, 2000

- Information Technology Bill, 1999 got assent of President in August 2000 & came to be known as Information Technology Act, 2000.

1. OBJECTIVES OF THE ACT

- To grant legal recognitions for transactions carried out by means of EDI & other means of communication commonly referred to as “electronic Commerce” in place of paper-based method of communication
- To give legal recognitions to digital signature for authentication of any information or matter which requires authentication under any law
- To facilitate electronic filing of documents with government departments
- To facilitate electronic storage of data
- To facilitate & give legal sanctions to EFT between banks & financial institutions

2. STRUCTURE OF THE ACT

- 94 sections spread over 13 chapters & 4 schedules

CHAPTER	CONTENTS	SECTIONS	PARTICULARS
I	Scope & Definitions	1 & 2	Legal Validity of Electronic Transactions & Involved Participants
II	uthentication of E-records using digital signature	3	
III	E-governance	4-10	
IV	Attribution, receipt & dispatch of E-records	12 & 13	
V	Secure E-records & secure digital signatures	14-16	
VI	Regulation of certifying authorities	17-34	
VII	Digital signature certification	35-40	
VIII	Duties of subscriber	41-42	
IX	Penalties & Adjudication	43-45	Offences & Structure for dealing with such offences
X	Cyber Regulation Appellate Tribunal	48-64	
XI	Offences	65-78	
XII	Network service provider not to be liable in certain cases	79	
XIII	Miscellaneous	80-93	Powers to various govt. bodies to make rules under IT Act, 2000

- Chapters & schedules contain related amendments to other acts to bring them in line with requirements of IT Act like IPC, Indian Evidence Act, 1972, Banker’s Book Evidence Act, 1891 & the RBI Act, 1934

3. SCOPE OF THE ACT: CHAPTER I

Act extends to the whole of India, unless otherwise provided in the act. Also applies to any offence or contravention hereunder committed outside India.

Act does not apply to:

- A negotiable instrument under NI Act, 1881
- A power-of-attorney under PoA Act
- A trust (deed) under Indian Trusts Act
- A will under Indian Succession Act
- Sale deed or registry for immovable property
- Any such documents as may be NIOG

4. DEFINITIONS

- **Affixing Digital Signature:** using methodology for the purpose of authentication of edocuments using digital signature
- **Asymmetric Crypto System:** a system consisting of secure key pair, private key & public key
- **Computer Network:** interconnection of one or more computers using satellite, microwave or other communication channels
- **Digital Signature:** authentication of any electronic record by a subscriber by using
- electronic method
- **Key Pair:** a private key & corresponding mathematically related public key
- **Private Key:** key of key pairs used to **create** digital signature
- **Public Key:** key of key pairs used to **verify** digital signature
- **Secure System:** computer system which is secured from unauthorized access & misuse

5. DIGITAL SIGNATURE: CHAPTER II

- Generation of DS used Key Pair technology
- Requirements of any electronic document to be legally valid:
  - Integrity using Hash Function
  - Authentication

6. HASH FUNCTION

- Used for integrity of document
- An algorithm which is run over a message & generates a big alphanumeric requirement known as **Message Digest**.
- Message Digest is unique value for one message
- Any change in original message will be followed by Hash function, which will generate a different message digest. *i.e. the change in message digest will indicate that original*

message has been altered.

7. E-GOVERNANCE: CHAPTER III

- E-Gov. is filing of any form, application or other document with govt. dept. in e-form & similarly grant of any license or permit from govt. offices, also in e-form.
- Low cost, efficient & transparent working
- Rules for making E-Gov. possible:
- Provide legal recognition for E-records
- Provide legal recognition for digital signatures
- Provide for filing of any form, application or other document with govt. dept. in e-form & similarly grant of any license or permit from govt. offices, also in e-form
- Specify ways for retaining e-documents
- Mandate manual filing of forms in govt. depts. in addition to e-forms in case of violation of Rights

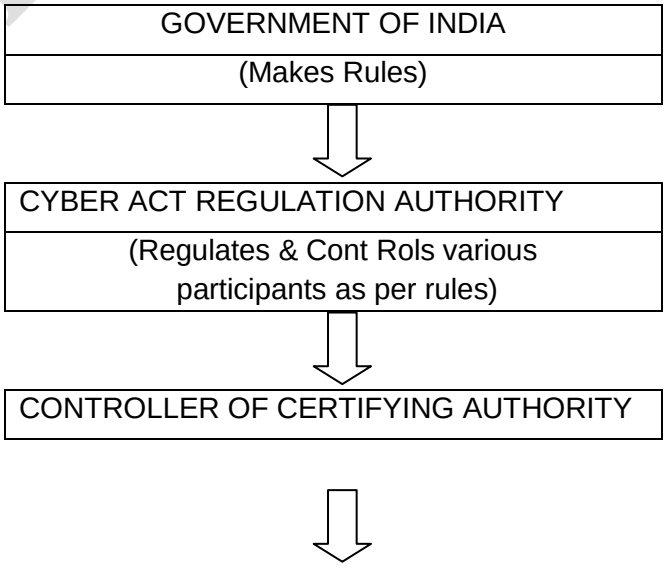
8. RECEIPT & DISPATCH OF E-RECORDS: CHAPTER IV

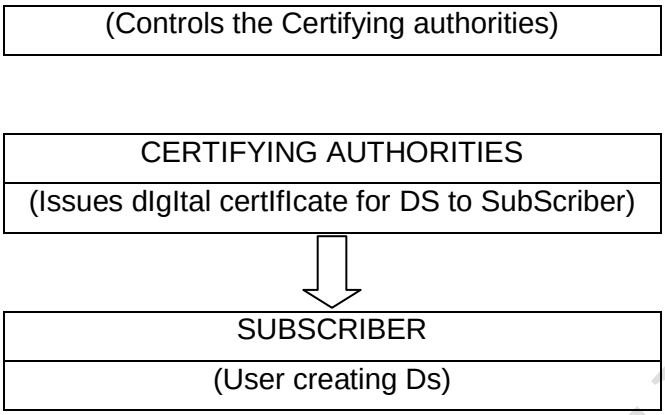
- This chapter provides the manner in which acknowledgement of receipt & dispatch of electronic records shall be made &
- The manner in which the time & place of dispatch & receipt of electronic records sent by sender shall be identified

9. SECURE E-RECORDS & DIGITAL SIGNATURES: CHAPTER V

- This chapter provides the security procedures to be applied to digital signatures for being considered as secured &
- The power of CG to specify security procedures for secured DS & E-records

10. CERTIFYING AUTHORITIES: CHAPTER VI

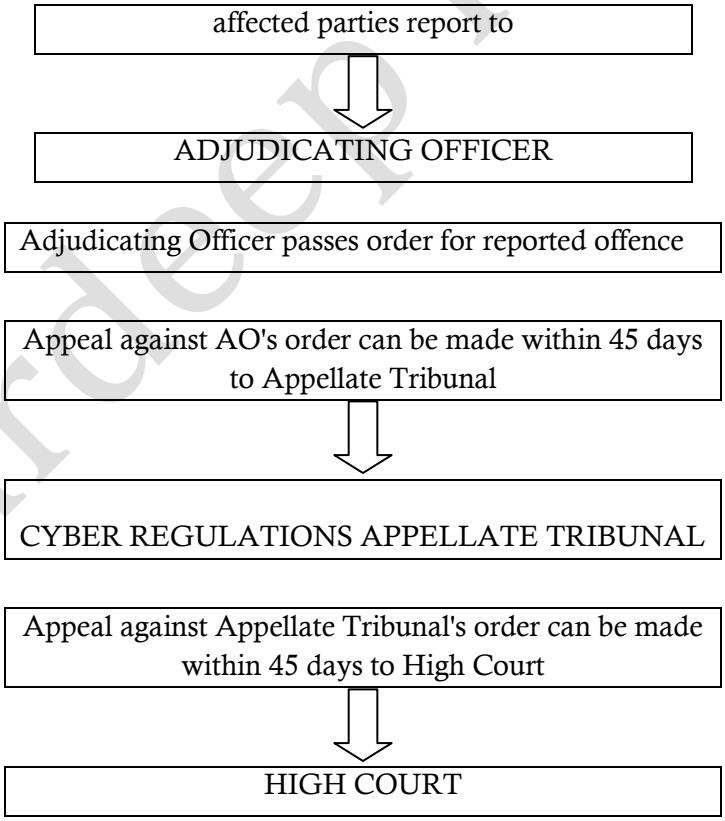




11. DIGITAL SIGNATURE CERTIFICATION: CHAPTER VII

Certifying authority will issue digital certificate to subscriber on payment of fees not exceeding Rs. 25,000.00 after being satisfied that the subscriber holds the private key for corresponding public key to be listed in DC & that private key is capable for creating DS.

12. CYBER REGULATIONS APPELLATE TRIBUNAL: CHAPTER X



13. OFFENCES: CHAPTER XI

- Offences:
  - Tampering with Computer source documents
  - Hacking
  - Publishing of obscene info. In e-form
  - E-forgery for cheating, harming information
  - Mala fide usage of forged e-records
  - Publication of DSC for fraudulent purpose
  - Breaching confidentiality & privacy
  - Publishing false DSC
  - Suppression or misrepresentation of material facts

- Punishments:

  - For publishing false DSC: Imprisonment upto 2 years or Rs. 1 Lakh penalty or both
  - For fraudulent publishing: Imprisonment upto 2 years or Rs. 1 Lakh penalty or both
  - For Hacking: Imprisonment upto 3 years or Rs. 2 Lakhs penalty or both
  - For publishing obscene information: Imprisonment upto 5 years or Rs. 1 Lakh penalty or both for first conviction & upto 10 years & Rs. 2 Lakhs on subsequent conviction
  - For Misrepresentation: Imprisonment upto 2 years or Rs. 1 Lakh penalty or both

14. NETWORK SERVICE PROVIDER NOT TO BE LIABLE IN CERTAIN CASES: CHAPTER XII

The network service provider shall not be liable for third parties' info. Or data made available by him if he proves that the offences were committed without his knowledge or consent.

15. MISCELLANEOUS: CHAPTER XIII

- The following bodies are authorized to frame rules:
- CG
- SG
- Cyber Regulations Advisory Authority
- Controller of Certifying Authority
- Police Officers (for searching purposes)

16. DIGITAL CERTIFICATE

- DC is used to ensure the receiver that the sender's public key is valid

- For this purpose, sender has to obtain DC from trusted third party (Certification Authority)

17. PROCEDURES FOR OBTAINING DC:

- Subscriber sends his public key to Certification Authority (CA) along with hid ID information
- The CA verifies info. Provided by subscriber & returns to sender a DC that confirms the validity of sender's public key
- The CA certifies public key by digitally signing the sender's public key with the authority's private key

18. DUTIES OF CONTROLLER OF CERTIFYING AUTHORITY

U/s. 18 of the IT Act. 2000, duties of CCA are:

- Exercise supervision over activities of CA
- Certifying public keys of CA
- Laying down standards to be maintained by CA
- Specifying qualifications & experience of CA
- Specifying form & content of DSC
- Resolving any conflicts between CA & subscriber
- Laying down duties of CA
- Maintaining database of CA

19. DUTIES OF CERTIFYING AUTHORITIES

- Make use of secure hardware, software & procedures
- Provide a reasonable level of reliability
- Adhere to security procedure to ensure secrecy & privacy of DS are assured
- Ensure strict compliance of act

20. DUTIES OF SUBSCRIBER

- Generate public key & private key
- Publish DSC on acceptance of DSC
- Control private key

21. POWERS OF CG TO MAKE RULES

- Specify manner for e-records which may be authenticated by DS
- Specify format by which e-records shall be filed or issued
- Specify type of DS & manner & format in which it may be affixed
- Specify security procedure for creating e-records & DS

- Specify the requirements, manner & form for application for license to issue DSC
- Specify the validity of license
- Specify qualifications of CA, AO

22. ISSUES COVERED UNDER IT ACT, 2000

- Jurisdiction aspects of electronic contracts
- Jurisdiction of courts & tax authorities

23. ISSUES NOT COVERED UNDER IT ACT, 2000

- Requirements in writing
- Requirements of document
- Requirements of signature
- Requirements of legal recognition for electronic messages, records & documents to be admitted as evidence in court of law or for e-governance

All the best friends

Never listen to other people tendencies to be negative orpessimistic... because they take your most wonderful dreams
&
Wishes away from you- the ones you have in your heart!

Just Do It! Do What You Want!

-Pardeep Rohilla