**CHAPTER 1 – Quick Revision Points (QRP)**

**INFORMATION SYSTEMS CONCEPTS**

**System:**
- System means a set of interrelated elements that operate collectively to accomplish some common object.
- It takes input from its environment and returns output again to the environment.

**General classification of system:**

<table>
<thead>
<tr>
<th>System Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical system</td>
<td>can be seen and touched. Eg: Transport, computer, business system etc.</td>
</tr>
<tr>
<td>Abstract system</td>
<td>cannot be seen and touched. Eg: System of religious beliefs, theology.</td>
</tr>
<tr>
<td>Open system</td>
<td>takes input from its environment and returns some output to the environment.</td>
</tr>
<tr>
<td>Closed system</td>
<td>does not interact with the environment. Eg: Production system, computer system.</td>
</tr>
<tr>
<td>Automated system</td>
<td>computer system is used to carry out the entire task.</td>
</tr>
</tbody>
</table>

**SYSTEM**

<table>
<thead>
<tr>
<th>Elements</th>
<th>Interactive behavior</th>
<th>Degree of human intervention</th>
<th>Working/Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>Physical</td>
<td>Manual</td>
<td>Automated</td>
</tr>
<tr>
<td>Open</td>
<td>Closed</td>
<td>Deterministic</td>
<td>Probabilistic</td>
</tr>
</tbody>
</table>

### I. Classification of system based on “Elements”

<table>
<thead>
<tr>
<th>Physical system</th>
<th>Abstract system</th>
</tr>
</thead>
<tbody>
<tr>
<td>- can be seen and touched. Eg: Transport, computer, business system etc</td>
<td>- cannot be seen and touched. Eg: System of religious beliefs, theology</td>
</tr>
<tr>
<td>- can be of different size and serve different purpose</td>
<td>- can only be visualized by our mind. Eg: Diagrams and flowcharts</td>
</tr>
</tbody>
</table>

### II. Classification of system based on “Interactive behavior”

<table>
<thead>
<tr>
<th>Open system</th>
<th>Closed system</th>
</tr>
</thead>
<tbody>
<tr>
<td>- takes input from its environment and returns some output to the environment. Eg: Business, Marketing, communication system etc.</td>
<td>- does not interact with the environment. Eg: Production system, computer system.</td>
</tr>
<tr>
<td>- can only be relatively closed. Eg: “use and throw” sealed digital watch</td>
<td>- does not change according to the environment.</td>
</tr>
</tbody>
</table>

### III. Classification of system based on “Human intervention”

<table>
<thead>
<tr>
<th>Manual system</th>
<th>Automated system</th>
</tr>
</thead>
<tbody>
<tr>
<td>- work done by human efforts. Eg: Manual accounting system</td>
<td>- computer system is used to carry out the entire task.</td>
</tr>
<tr>
<td>- human intervention is nil or very less.</td>
<td>- human intervention is always there.</td>
</tr>
<tr>
<td>- some manual intervention is always there.</td>
<td>- E.g. auto-pilot aviation, software controlled processes, business ERP system.</td>
</tr>
<tr>
<td>- E.g. software controlled processes, business ERP system.</td>
<td></td>
</tr>
</tbody>
</table>
IV. Classification of system based on “Working/Output”

<table>
<thead>
<tr>
<th>Deterministic system</th>
<th>Probabilistic system</th>
</tr>
</thead>
<tbody>
<tr>
<td>- gives exact output.</td>
<td>- provide expected output.</td>
</tr>
<tr>
<td>- operate in a predictable manner</td>
<td>- uncertainty about the outcome and behavior</td>
</tr>
<tr>
<td>- behavior of the system is known with certainty</td>
<td>- for a given set of input, the output cannot be known with certainty</td>
</tr>
<tr>
<td>- Eg: accounting information system, communication system, computer system, production system etc.</td>
<td>- Eg: weather forecasting system, sales forecasting system, pricing system, inventory management system, marketing system etc.</td>
</tr>
</tbody>
</table>

**System Concepts:**

- **System environment:** external world which is outside the system boundary
- **System boundary:** boundary separates the system from its surrounding environment

- **Subsystem:** smaller systems with forming part of a bigger system are called subsystem
- **Interface:** interconnections and interactions between the subsystems
- **Supra system:** system immediately above a sub-system
- **System entropy:** measure of disorder in a system
- **System Stress and System Change:** force transmitted by a system’s supra-system on the sub-system

**Characteristic of sub-system:**

i. **Decomposition (Factoring):** dividing a system into smaller units i.e. subsystem

ii. **Simplification:** reduce the number of interconnections between all the sub-systems

iii. **Decoupling:** each sub-system is as independent as possible

**Decoupling mechanism:**

- a) Inventories, buffer, or waiting lines
- b) Slack resources
- c) Standards

**Information:**

**Information:** Information is data that has been arranged into meaningful and useful context

**Data:** Data is unorganized collection of facts or events
Attributes (Characteristics) of information:

1. Availability
2. Purpose
3. Mode and format
4. Decay
5. Rate
6. Frequency
7. Completeness
8. Reliability
9. Cost benefit analysis
10. Validity
11. Quality
12. Transparency
13. Value of information

Types of Information:

<table>
<thead>
<tr>
<th>Internal Information</th>
<th>External Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Generated within the organization</td>
<td>- collected from external environment</td>
</tr>
<tr>
<td>- E.g. budgets, accounts, reports</td>
<td>- E.g. Govt policies, economic trends</td>
</tr>
<tr>
<td>- mainly used by middle and lower management</td>
<td>- mainly used by top management</td>
</tr>
</tbody>
</table>

Role of Information System in management:

1. Effective decision making.
2. Competitive advantage.
3. Pooling of resources.
4. Enhanced operational efficiency.
5. Enhanced control environment.

Factors on which information requirements of executives depends:

1. Operational functions
   i. Production
   ii. Finance
   iii. Marketing
   iv. Purchase
   v. Material management etc

2. Type of decision making:
   i. Structured (Programmed)
   ii. Unstructured (Non-programmed)
   iii. Semi-structured

3. Level of management: In broader terms there can be following three levels of management
   i. Top level management (Strategic level)
   ii. Middle level management (Tactical level)
   iii. Lower level management (Operational level)
### Components of Computer Based Information System:

1) Hardware  
2) Software  
3) Data  
4) Procedures  
5) People

### Characteristics of Computer Based Information Systems are as follows:
- Predetermined objectives  
- Interrelated and interdependent subsystems  
- Interaction amongst subsystems  
- Work done by individual subsystem is integrated

### Major areas of computer-based applications are:
1. Finance and accounting  
2. Marketing and sales  
3. Production  
4. Inventory management  
5. Human resource management

### Types of Information Systems:

#### INFORMATION SYSTEMS

|-----------------------------|-----------------------------|--------------------------|
| 1) TPS  
2) MIS  
3) ERP | 1) DSS  
2) EIS  
3) ES | 1) Text Processing Systems  
2) Electronic Document Management Systems  
3) Electronic Message Communication Systems  
4) Teleconferencing and Video-conferencing Systems |

#### Transaction Processing System (TPS):
- Implemented at operational level  
- Process routine business transactions  
- Base for higher level systems  
- Rapidly process transactions  
- Batch processing or on-line processing

Generally TPS involves the following activities:
1. Punching the transaction  
2. Processing of transaction  
3. Generating reports  
4. Answering queries

#### TPS Components:
- (i) Inputs  
- (ii) Processing  
- (iii) Storage  
- (iv) Output

#### Features of TPS:
- (i) Large volume of data  
- (ii) Automation of basic operations  
- (iii) Benefits are easily measurable  
- (iv) Source of input for other systems
Management Information System:

Definition - MIS is an integrated system of man and machine for providing the information to management for decision making and control.

Characteristics of an effective MIS:
1. Management oriented
2. Management directed
3. Integrated
4. Common data flow
5. Heavy planning element
6. Sub-system concept
7. Common data base
8. Computerized.

Misconceptions about MIS:
1. MIS relates to computer only
2. More data means more information
3. Reports should be highly accurate

Pre-requisites of an effective MIS:
1. Database
2. Qualified staff
3. Support of top management
4. Control and maintenance
5. Evaluation of MIS

Constraints (Limitations) in operating MIS:
1. Non-availability of experts
2. Problem in selecting the sub-system
3. Non-standardized approach
4. Non-cooperation from staff
5. High turnover of experts
6. Difficulty in quantifying the benefits

Effects of using computers in MIS:
1. Fast processing and retrieval
2. Up-to-date information
3. In-depth analysis of data
4. Handling of more complex business operations
5. Integration of sub-systems

Limitations of MIS:
1. Poor quality of input data in the MIS gives the poor quality results.
2. MIS is not a substitute for effective management but only a helping tool
3. Lack of flexibility can make the MIS obsolete very soon.
4. MIS cannot provide direct help for unstructured decision making.
5. MIS ignores qualitative aspects of business organization
6. MIS is highly sensitive and requires constant monitoring
7. MIS implementation can be very expensive
8. MIS becomes less effective if there is frequent change in top and middle management.

ERP (Enterprise Resource Planning): ERP will be discussed in chapter 7
**Decision Support System (DSS):**

**Definition** –
DSS is information systems that
- support semi-structured and unstructured decision making activities
- useful for top and middle level management by giving them various decision alternatives
- DSS is not meant for making decisions but to help in taking decisions.

**Characteristics of DSS:**
(i) Semi-structured and Unstructured Decisions
(ii) Ability to adapt to changing needs
(iii) Ease of Learning and Use

**Components of DSS:**
1) User
2) User interface (planning language)
   i. general purpose planning language
   ii. special purpose planning language
3) Model base
   - Mathematical functions
   - Statistical functions
   - And financial functions
4) Database

**Implementation of database:** Database is implemented at three levels as shown below:

```
Physical Level

Logical Level

External Level
```

**Software tools of DSS:**

<table>
<thead>
<tr>
<th>Database software</th>
<th>Model based software</th>
<th>Statistical software</th>
<th>Display based software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>MS Excel</td>
<td>SPSS</td>
<td>Chartmaster</td>
</tr>
<tr>
<td>Microsoft Access</td>
<td>Lotus 1-2-3</td>
<td>SAS</td>
<td>SAS Graph</td>
</tr>
<tr>
<td>Microsoft SQL server Dbase</td>
<td>Foresight</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Omnicalc</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Use of DSS in accounting function:**
1. Cost accounting system
2. Capital budgeting system
3. Variance analysis
4. General financial analysis
5. Portfolio management

Some of the DSS available in market are: 1) Expert Choice   2) AutoMan
Executive Information System (EIS):

Definition: An Executive Information System (EIS) is a type of information system which provides information to executives for decision-making.

Characteristics of EIS:
- Same as Executive Support System (ESS).
- Complementary to Decision Support System.
- Graphical displays, easy-to-use user interfaces.
- Drill-down capabilities
- Analyze, compare, highlight trends
- Monitor performance
- Identify opportunities and problems
- Access to both internal and external data
- Supports data mining

Type of decisions made by executives: Executive decisions relate to the following:
1. Strategic planning
2. Tactical planning
3. Fire fighting measures
4. Control

Characteristics of information used in executive decision making:
For executive decision making following information is required:
- Environmental information
- Competitive information and
- Internal information is required

The characteristic of such information is:
1. Lack of structure
2. High degree of uncertainty
3. Future orientation
4. Informal source
5. Low level of detail

Purpose of EIS:
1. Support learning
2. Timely access to information
3. Highlights the problem

Information Contents of EIS:
1. Anything which is useful for the executives
2. Targets and budgets
3. Data about work processes
4. Performance measurement indicators.
5. External information
6. Information contents can change according to the changing environment

Expert System:
- Highly developed DSS
- Utilizes the knowledge generally possessed by a human expert
- Imitate (copy) human reasoning
- Uses the concept of artificial intelligence
- Useful for solving structured and semi-structured problems.
Components of Expert Systems:

(i) **Knowledge Base**: stores the rules, data and relationships
(ii) **Inference Engine**: main processing component
    - forward-chain
    - backward chain
(iii) **Knowledge Acquisition Subsystem**
(iv) **User Interface**: interacts with a user

Expert system can be used in the following areas:
1. Accounting and finance
2. Marketing
3. Help desk function
4. Manufacturing
5. HR

Need for Expert Systems:
1. Experts are expensive
2. Experts are short in supply
3. Human experts can handle only a few factors

Benefits of Expert Systems:
1. Preserve knowledge
2. Can be used anytime.
3. Help beginners
4. Not subject to human fallings
5. Strategic tool

Problems areas for which expert system can be developed:
1. **Availability**: One or more experts are available to support the knowledge base
2. **Complexity**: problems is complex
3. **Domain**: problem is limited to a relatively well-defined problem area.
4. **Expertise**: Solutions to the problem require the efforts of experts
5. **Structure**: must be able to cope with ill-structured and uncertain situation

**OFFICE AUTOMATION SYSTEMS (OAS):**

Different office activities can be broadly grouped into the following types of operations:

(i) Document Capture
(ii) Document Creation
(iii) Receipts and Distribution
(iv) Filling, Search, Retrieval and Follow up
(v) Calculations
(vi) Recording Utilization of Resources
Benefits of Office Automation Systems:

(i) Improves communication
(ii) Reduces time
(iii) Reduces cost
(iv) Increases accuracy

I. Text Processing Systems:
- Widely used office system
- Automate the process of development of documents
- Use of standard stored information to produce personalized documents.
- Support laser printers, inkjet printers, scanners
- Example - MS Word.

II. Electronic Document Management Systems:
- Used to store, retrieve and manage document files or scanned copy of documents.
- Linked to text processors, electronic message communication systems etc.
- Provide remote access of documents
- Helps in internal communication of document
- Helps traveling executives to share work space in the office.

III. Electronic Message Communication Systems:
1) Electronic Mail
   - Electronic transmission
   - Online development and editing
   - Broadcasting and Rerouting
   - Integration with other Information systems
   - Portability
   - Economical

2) Facsimile (Fax):
   - Transmission of images of documents over telephone lines
   - Computer system permits sharing of fax facilities
   - Uses special software and fax servers to send and receive fax messages using common communication resources
   - These servers have the ability to receive fax messages and automatically reroute them to the intended recipient after viewing it at the central computer

3) Voice Mail:
   - Variation of the email
   - Messages are transmitted as digitized voice

IV: Teleconferencing and Video-conferencing Systems:
- Used for conducted meeting
- Persons located at two or more different places can participate
- Reduce the time and cost
- Teleconferencing has audio link
- Video conferencing has both audio and video link
- Can be used on PC with a camera
- Uses visual communication software

Best Wishes
CHAPTER 2 – QRP (Quick Revision Points)

SYSTEMS DEVELOPMENT LIFE CYCLE METHODOLOGY

Obstacles in achieving System Development Objectives
(i) Lack of senior management support and involvement
(ii) Shifting user needs
(iii) Difficulty in development of strategic systems
(iv) Unfamiliarity with new technologies
(v) Lack of standard project management methodologies
(vi) Overworked or under-trained development staff
(vii) Resistance to change
(viii) Lack of user participation
(ix) Inadequate testing and training

System Development Team
• Steering committee
• Project management team
• System analyst
• Systems designer
• Accountant/auditors
• End-users

SYSTEMS DEVELOPMENT METHODOLOGY
A system development methodology is a formalized, standardized, documented set of activities used to manage a system development project.

Common features of all systems development methodologies:
• Division of project
• Every stage should have some deliverables
• Signoffs/approvals at every stage
• Testing
• User Training
• Change management
• Post implementation review (PIR)

Approaches to System Development
   (i) Traditional/Waterfall/sequential: (Linear)
   (ii) Prototyping: (Iterative)
   (iii) Incremental: (Linear + Iterative)
   (iv) Spiral: (Linear + Iterative)
   (v) Rapid Application Development (RAD): (Iterative)
   (vi) Agile Methodologies: (Iterative)
(i) **The Traditional / Waterfall Approach / Sequential Approach:** *(Linear)*

**Basic Principles:**
1. Sequential phases
2. Some overlap and splash back
3. Heavy planning
4. Heavy documentation
5. Heavy controls
6. Implementation of an entire system at one time.
7. Reviews and approval at every stage.

**Strengths:**
1. Support less experienced project team/manager
2. Support project teams whose composition fluctuates
3. Quality, reliability and maintainability of the developed software
4. Progress of system development is measurable
5. Conserves resources.

**Weaknesses:**
1. Inflexible, slow and costly
2. Forward movement only
3. Iteration not done
4. User requirements to be clear at the start
5. Inconsistencies are discovered during design and coding.
6. Problems discovered during testing
7. Under capacity may be difficult to correct
8. Changes are more costly
9. Excessive documentation
10. Documentation is difficult to understand
11. Gap between users and developers

(ii) **The Prototyping Model:** *(Iterative)*

- Used to develop smaller systems such as DSS, MIS and Expert systems.
- First develop a small or pilot version of the new system called a prototype
- Built quickly and at a lesser cost
- Prototypes are generally throwaway
- Users work with the prototype and gives suggestions to improve it
- These suggestions are then incorporated into prototype and again evaluated
- Finally actual system is made
**Basic Principles**

Step 1 - Identify Information System Requirements  
Step 2 - Develop the Initial Prototype  
Step 3 - Test and Revise  
Step 4 - Obtain User Signoff of the Approved Prototype

**Strengths:**

(i) User participation  
(ii) Resolve unclear objectives  
(iii) Knowledge gained in an early iteration can be used in later iterations.  
(iv) Removes doubts  
(v) Innovation  
(vi) Flexible designs.  
(vii) Better definition of user needs  
(viii) Immediately evaluate proposed system changes  
(ix) Errors are detected and eliminated early

**Weaknesses:**

(i) Low approvals  
(ii) Low controls  
(iii) Incomplete or inadequate problem analysis  
(iv) Non-functional elements not included  
(v) Limits future system potential  
(vi) More user time is required  
(vii) Low testing and documentation of actual system  
(viii) Behavioral problems

**The Incremental Model:** *(Linear and Iterative)*

**Basic Principles:**

- Development in increments  
- Software is decomposed into a number of components (Builds)  
- A little more is added each time  
- Component is delivered to the client when it is complete  
- Allows partial utilization  
- Simplify implementation

There can be three variations/strategies for this model:

(a) Requirements, designing and development of single a “Build”  

or

(b) Overall requirements are defined for the complete systems but designing and development of a single “Build”  

or

(c) Overall requirements and design of architecture and system core are defined using the Waterfall approach, followed by Prototyping
Strengths:
(i) Knowledge gained in an early increment can be used in the development of later increments.
(ii) Moderate control
(iii) Concrete evidence of project status
(iv) More flexible
(v) Early mitigation of integration risk
(vi) Ease of implementation
(vii) Limited negative impact

Weaknesses:
(i) Lack of overall consideration
(ii) Do not consider interdependent parts.
(iii) Poor overall system architecture
(iv) Requires well-defined interfaces
(v) Difficult problems may be deferred

**Spiral Model:** *(Linear and Iterative)*

**Basic Principles:**
(i) Risk driven model
(ii) Intended for large, expensive and complicated projects.
(iii) Steps
   A) Define user requirements
   B) Create a preliminary design
   C) Identify and resolve all the possible risks
(iv) Create first prototype
(v) Create second prototype:
   o evaluating the first prototype in terms of its strengths, weaknesses, and risks;
   o defining the requirements of the second prototype;
   o planning and designing the second prototype;
   o constructing and testing the second prototype.

Strengths:
(i) Low overall project risk.
(ii) Helps to select the best methodology
(iii) Can incorporate Waterfall, Prototyping, and Incremental methodologies

Weaknesses:
(i) Highly customized
(ii) Complex
(iii) Limited reusability
(iv) Skilled and experienced project manager is required
(v) More work for the next cycle
(vi) No firm deadlines
(v) Rapid Application Development (RAD): (Iterative)

**Basic Principles**
- (i) Minimum planning
- (ii) Fast development
- (iii) High quality system
- (iv) Low cost,
- (v) Flexible (Ease-of-change)
- (vi) Fulfilling the business need
- (vii) Use of Computer Aided Software Engineering (CASE) tools
- (viii) Timeboxes
- (ix) Joint Application Development (JAD)
- (x) Active user involvement
- (xi) Basic documentation
- (xii) Standard can be fitted

**Strengths**
- (i) Faster development
- (ii) Low cost
- (iii) Quick reviews
- (iv) Encourages user feedback
- (v) Commitment from stakeholders
- (vi) Concentrates on essential elements
- (vii) Ability to rapidly change
- (viii) Tighter fit between user requirements and system specifications.
- (ix) Savings in time, money and human effort

**Weaknesses**
- (i) Lower overall system quality.
- (ii) Misalignment
- (iii) More requirements than needed (gold plating).
- (iv) Feature creep, more and more features are added
- (v) Inconsistent designs
- (vi) Violation of programming standards
- (vii) Difficulty in module reusability
- (viii) Lacks scalability.
(ix) Lacks controls  
(x) Lacks reviews and audits  
(xi) Difficult problems to be pushed to the future  
(xii) Well–defined interfaces are required  

(vi) **Agile Methodologies:** (Iterative)

**Basic Principles:**
1. Fast development  
2. Iterative and Incremental  
3. Working S/W is delivered frequently (Build Short – Build Often)  
4. Time Box  
5. Collaborative, Self-organizing, Cross-functional team  
6. Close co-operation between user and developers  
7. Face-to-face conversation  
8. Rapid and flexible response to changes

**Strength:**
1. Adaptive  
2. Face-to-face communication  
3. Minimum documentation  
4. High quality S/W

**Weakness:**
1. Difficult to assess the efforts required for S/W development at the beginning  
2. Lacks proper design and documentation  
3. Less knowledge transfer  
4. More re-work required  
5. Project deviates if user in not clear about final objective/outcome  
6. Experienced team is required  
7. Lacks attention to outside integration

**SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)**

The System Development Life Cycle (SDLC) key features:
- Sequential in nature  
- Document driven  
- Deliverables at every stage  
- Process oriented

The advantages of this system are as follows:
- Better planning and control  
- Compliance  
- Documentation  
- review and signoff

From the perspective of the IS Audit, the following are the possible advantages:
1. IS auditor can understanding  
2. IS auditor and check compliance  
3. IS auditor and guide  
4. IS auditor can evaluate

**Risks/Shortcoming Associated with SDLC:**
1. Cumbersome  
2. End product is not visible  
3. Rigid  
4. not be suitable for small and medium
Stage I. THE PRELIMINARY INVESTIGATION

Objective: Evaluation of project request (Cost/Benefit)

Steps
(i) Identification of Problem
(ii) Identification of objective
(iii) Delineation of scope
(iv) Feasibility Study

Issues addressed in the Feasibility Study:
(i) Solution is as per the business strategy.
(ii) Can existing system can rectify the situation
(iii) Time frame
(iv) Cost
(v) Whether the vendor product offers a solution


(i) Identification of Problem:
- Identify and define the problem
- Discussions with the user group
- Existing system may be outdated
- Manager want new report/information
- Old systems are ineffective or inefficient.
- System analyst is assigned to make a preliminary investigation

(ii) Identification of Objective:
- Objective of new system is set

(iii) Delineation (Description) of Scope:
(i) Functionality requirements
(ii) Data to be processed
(iii) Control requirements
(iv) Performance requirements
(v) Constraints
(vi) Interfaces
(vii) Reliability requirements

During preliminary investigation, the analyst collects the data through two primary methods:

a) Reviewing internal documents
b) Conducting Interviews

(iv) Feasibility Study:
• Technical: Is the technology needed available?
• Financial: Is the solution viable financially?
• Economic: Return on Investment? (Cost/Benefits)
• Schedule / Time: Can the system be delivered on time?
• Operational: How will the solution work?
• Human resource feasibility: Availability of skilled people for the new system
• Behavioral: Is the solution going to bring any adverse effect on quality of work life?
• Legal: Is the solution valid in legal terms?
Stage II. SYSTEM REQUIREMENT ANALYSIS

The following activities are performed in this phase:

• Identify the stake owners.
• Consult the stake owners
• Analyse requirements
• Correct conflicts
• Determine priorities.
• Requirements are complete and consistent
• Gather data
• Model activities
• Document activities


Fact finding Techniques
(i) Documents
(ii) Questionnaires
(iii) Interviews
(iv) Observation

Analysis of the Present System: The following areas should be studied in depth:
(i) Review historical aspects
(ii) Analyse inputs
(iii) Review data files maintained
(iv) Review methods, procedures and data communications
(v) Analyse outputs
(vi) Review internal controls
(vii) Model the existing physical system and logical system
(viii) Undertake overall analysis of present system

Systems Analysis of Proposed Systems
- Uses management by exception principle.
- Online processing capabilities.
- Input directly from source documents
- Work volumes and timings
- output-to-input approach to be followed

System Development Tools: Four categories
(I) System components and flows
  o System flow charts
  o data flow diagram
  o system component matrix

(II) User interface
  o Layout forms and screens
  o Dialogue flow diagrams

(III) Data attributes and relationships
  o Data Dictionary
  o Entity-Relationship diagrams
  o File layout forms
  o Grid charts

(IV) Detailed system process
  o Decision trees
  o Decision tables
  o Structure charts
We will now describe some tools in detail:

(i) **Structured English:**
Structured English (also known as Program Design Language (PDL) or Pseudo Code)
English language (for simplicity) + syntax (for precision)

(ii) **Flowcharts:**
Graphical representation of inputs, outputs and processing

(iii) **Data Flow Diagrams:**
- Logical diagram of any process or activity.
- Four basic elements: Data Sources and Destinations, Data Flows, Transformation processes, and Data stores

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Name</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data source and data destination</td>
<td>The people and organizations that send data to and receive data from the system</td>
</tr>
<tr>
<td></td>
<td>Data flows</td>
<td>The flow of data into or out of a process</td>
</tr>
<tr>
<td></td>
<td>Transformation process</td>
<td>The processes that transform data from inputs to outputs</td>
</tr>
<tr>
<td></td>
<td>Data stores</td>
<td>The storage of data is represented by two horizontal lines.</td>
</tr>
</tbody>
</table>

(iv) **Decision Tree:**
A Decision Tree uses a tree-like graph of decisions and their possible consequences, probabilities, resource costs, and utility

(v) **Decision Table:**
A Decision Table is a table which defining the possible options that may be considered within the program and the suitable action for each option
The four parts of the decision table are as follows:
(i) **Condition Stub** - list of conditions
(ii) **Action Stub** — list of actions
(iii) **Condition entries** - list of possible answer to conditions
(iv) **Action entries** – lists of actions to be taken

(vi) **CASE** (Computer-Aided-Software Engineering) Tools:
- CASE tool are those software which help to automatically develop high quality, defect free and maintainable software.
- Features of CASE - Data Dictionary tools; Computer aided Diagramming Tools; Screen and Report generator; Prototyping tools; Code Generation; and Reverse Engineering.

(vii)**System Components matrix:**
- A table of activities and resources required in a system
- E.g. system component matrix of a sales processing and analysis system
<table>
<thead>
<tr>
<th>Output</th>
<th>POS terminals, management workstations</th>
<th>Paper reports &amp; receipts</th>
<th>Report generator program, graphic program</th>
<th>Output use and distribution procedures</th>
<th>Sales clerk managers, customers</th>
<th>Sales receipts, sales analyses reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>Magnetic disk drive</td>
<td>Magnetic disk packs</td>
<td>Database management system</td>
<td>Computer operators</td>
<td>Customer, inventory &amp; sales database</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td>POS terminals, management workstations</td>
<td>Paper doc &amp; control reports</td>
<td>Performance &amp; security monitoring program</td>
<td>Correction procedures</td>
<td>Computer operators, control clerks</td>
<td>Customer, inventory &amp; sales database</td>
</tr>
</tbody>
</table>

(viii) **Data Dictionary:**
- Data dictionary is data about data (also called meta-data)
- Data dictionary contains information about a single data item
  - File in which it is stored
  - Source document
  - Who can access
  - Who cannot access
  - Who can read or modify
- Auditors can get audit trail from data dictionary

Fig. below shows a sample record from a data dictionary

(ix) **Layout form and Screen Generator, Menu Generator, Report generator, Code Generator**

**Layout form and Screen Generator:** Template or pre-printed electronic forms on which the size and position of titles, headings, data and information can be designed

<table>
<thead>
<tr>
<th>Customer Order Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
</tr>
<tr>
<td>Order Number</td>
</tr>
<tr>
<td>Customer Name</td>
</tr>
<tr>
<td>Catalog Number</td>
</tr>
<tr>
<td>X</td>
</tr>
<tr>
<td>X</td>
</tr>
<tr>
<td>X</td>
</tr>
<tr>
<td>X</td>
</tr>
</tbody>
</table>

**Menu Generator:** Used for Menu and Sub-menu designing

**Report Generator:** Used for output report designing (Header, footer, format etc)

**Code Generator:** Used for generating source code from the high level specifications

**Systems Requirement Specifications (SRS):** Contents -
1. Introduction
2. Information description
3. Functional description
4. Behavioral description
5. Validation criteria
6. SRS Review
Roles involved in SDLC:

(i) **Steering committee:** Functions -
- Gives overall direction
- Representation of all deptt
- Monitor cost
- Monitor schedule
- Take corrective actions

(ii) **Project manager:**
- Overall coordination and direction.
- Many projects under him
- Coordinate with the client
- Coordinate with his team and project leader
- Deliver the project within time and budget

(iii) **Project leader:**
- Responsible for one project
- Directly involved in the project
- Entire project team reports to him

(iv) **Systems analyst / Business analyst:**
- Understand the user requirement and tell it to the development team
- Link between the user and the programmer

(v) **Team leader / Module leader:**
- Responsible for each module
- For example Treasury, Accounts payable, Accounts receivable module leaders
- Responsible for the delivery of tested modules within the allowed time and cost

(vi) **Programmer / Code developer:**
- Mason of software industry
- Converts design into programs
- Conducts debugging activity

(vii) **Database administrator (DBA):**
- Maintain Database
- Ensures the integrity and security of Database
- Gives approval for change in Database

(viii) **Quality Assurance:**
- Gives standards system development
- Quality review
- Should be independent

(ix) **Tester:**
- Junior level quality assurance personnel
- Attached to a project

(x) **Domain Specialist:**
- Subject matter expert e.g. CA, Engineer, Doctor
- Provides help to development team
- Need not have knowledge of software systems.

(xi) **IS Auditor:**
- Checks internal controls in system
Stage III. SYSTEMS DESIGN

The design phase involves following steps:
(i) Architectural Design
(ii) Design of the Data / Information Flow
(iii) Design of the Database
(iv) Design of the User-interface
(v) Physical Design; and
(vi) Design of the hardware/system software platform

(i) **Architectural Design:** This involves designing of system in modules
- major modules
- hierarchy of modules
- function and scope of each module
- module interface
- direct and indirect linked modules
- design is done by Functional Decomposition

The module is represented by a box and connection between them by arrows. Couple is data element that moves from one module to another and is shown by an arrow with circular tail.

![Functional decomposition diagram](image)

(ii) **Design of Data / Information flow**
- Problems of present data flow
- Objective of new system
- Design of new data flow diagrams (DFD)

(iii) **Design of Database**
- Database can be local (decentralised) or global (centralised)
- Design of database involves three levels
  I. Conceptual modelling (design for external user)
  II. Data modelling (logical design of database tables and structure)
  III. Physical modelling (storage of data on media)

(iv) **Design of User-Interface:** User interface means how user will interact or communicate with the system. This involves designing of -
- source documents
- output reports
- screen layouts
- inquiry screens
- graphic and colour displays
- special input/output device

**Important factors in Input / Output design:**
- Content
- Timeliness
- Format
- Media
- Form
(v) **Physical Design:**
- Logical design is converted into physical design which is then developed and implemented
- Auditor should see effectiveness and efficiency issues during designing
- CASE tools and simulation should be used
- Designing involves
  - Type of hardware for client application and server application
  - Type of Operating systems
  - Type Network
  - Processing – batch – online, real – time
  - Frequency of input, output

**Design Principles:**
- Design two or three alternatives and choose the best one on pre-specified criteria.
- The design should be based on the analysis.
- The software should be designed as per business needs
- The design should follow standards, for e.g. the user interface should have consistent colour scheme, menu structure, location of error message and the like.
- The design should be modular
- **Modularity:** A module is a small unit containing data and instructions to perform a well-defined task. Modularity is measured by two parameters: *Cohesion (internal linking)* and *Coupling (external linking).*
  - In a good modular design, cohesion will be high and coupling low.

(vi) **Design of the Hardware / System Software Platform:**
- New hardware and operating system may be required for new software
- New hardware and operating system should be modular
- New hardware and operating system should be compatible

**Stage IV: Systems acquisition and software development**

**SYSTEM ACQUISITION** – To purchase readymade system from software vendors

**Acquisition Standards:** Management should establish documented acquisition standards which ensures that –
- Security, reliability, and functionality already built into a product.
- Managers review the appropriate vendors, contracts, and licensing agreements.
- New products are compatible with existing systems.
- Functional, security, and operational requirements are clearly defined in request-for-proposals (RFP)

Acquiring Systems Components from Vendors
(I) **Hardware Acquisition:**
- New hardware may be required for new software
- Hardware acquisition is complex
- Long term support needed

(II) **Software Acquisition:**
- Requirements must be assessed before acquisition

(III) **Contracts, Software Licenses and Copyright Violations:**
- Only licensed software should be used in the organization
- Software contract should be in writing
- Contract should provide for source code accessibility
- Software are governed by “end user license agreement”
- Copyright laws protect proprietary as well as open-source software
- Use of unlicensed software can lead to possible litigation.
(IV) Validation of vendors’ proposals:
- Factors to be considered for vendor evaluation.
  - Performance capability
  - Costs and Benefits
  - Maintainability
  - Compatibility
  - Vendor Support

(V) Methods of validating the proposal:
  i) Checklists: Simple and subjective method. Various criteria are put in check list in the form of suitable questions
  ii) Point-Scoring Analysis: objective method

<table>
<thead>
<tr>
<th>Software Evaluation Criteria</th>
<th>Points</th>
<th>Vendor A</th>
<th>Vendor B</th>
<th>Vendor C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the software meet all mandatory specifications?</td>
<td>10</td>
<td>7</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>Will program modifications be minimal?</td>
<td>10</td>
<td>8</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>Does the software contain adequate controls?</td>
<td>10</td>
<td>9</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>Is the performance (speed/accuracy/reliability) adequate?</td>
<td>10</td>
<td>7</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>Are other users satisfied with the software?</td>
<td>8</td>
<td>6</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>Is the software user-friendly?</td>
<td>10</td>
<td>7</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Can the software be demonstrated and test-driven?</td>
<td>9</td>
<td>8</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Does the software have an adequate warranty?</td>
<td>8</td>
<td>6</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Is the software flexible and easily maintained?</td>
<td>8</td>
<td>5</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>Is online inquiry of files and records possible?</td>
<td>10</td>
<td>8</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>Will the vendor keep the software up to date?</td>
<td>10</td>
<td>8</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>123</strong></td>
<td><strong>94</strong></td>
<td><strong>106</strong></td>
<td><strong>85</strong></td>
</tr>
</tbody>
</table>

iii) Public Evaluation Reports: Industry association magazines, Survey reports etc
iv) Benchmarking problem for vendor’s proposals: Demo of software using routine input data
v) Test problems: Demo of software using extreme test data to test the true capabilities of system

SYSTEMS DEVELOPMENT – To develop in-house software

A good coded program should have the following characteristics:
- Reliability
- Robustness (Strength)
- Accuracy
- Efficiency (Consumes less resources)
- Usability (Easy to use)
- Readability (Easy to maintain)

Some other issues in systems development:
(I) Program Coding Standards:
- To be followed by programmers
- Helps in communication between teams
- Coding Standards reduce impact of programmer turnover
- Coding standards provide, simplicity, efficient use of storage and least processing time.

(II) Programming Language:
- There are many programming languages. Like:
  - High – level general purpose programming language such as COBOL and C language.
  - Object oriented languages such as C++, JAVA etc.
  - Scripting language like JAVA Script, VB Script.
  - Decision Support or Expert System languages like PROLOG.

Choice of Programming Language: Depends upon
- Type of operating system
- Type of hardware
- Type of application being developed
(III) Program Debugging:
Debugging means to remove the errors in program script. It is done by following four steps:
• Inputting the source program to the compiler,
• Letting the compiler find errors in the program,
• Correcting lines of code that are erroneous, and
• Resubmitting the corrected source program as input to the compiler.

(IV) Test the program
(V) Program Documentation
(VI) Program Maintenance

Stage V. Systems Testing

Level 1: Unit Testing – Testing of individual units of software

Categories of unit testing
i) Functional Tests – testing main function of S/W
ii) Performance Tests – testing the speed if S/W
iii) Stress Tests – testing the stress limit of S/W
iv) Structural Tests – testing the logic of S/W
v) Parallel Tests – testing old and new unit together

Types of Unit Testing:

(a) Static testing (i.e. testing done by reading the program script)
   i) Desk Check – done by programmer himself
   ii) Structured walk-through – Programmer with one more person
   iii) Code inspection – Formal committee review the unit

(b) Dynamic testing (i.e. testing by actual running of program on computer)
   i) Black Box Testing (internal logic is not examined)
   ii) White Box Testing (internal logic is examined)
   iii) Gray Box Testing (Combination of black box and white box)

Level 2: Integration Testing –
This involves testing the linking of different units of software to see that units connect correctly.
This is carried out in the following manner:

i) Bottom-up Integration:
   - Traditional strategy used to integrate
   - Lower modules are tested first, then higher modules
   - Easy to implement
   - Disadvantage: major decision points are tested later

ii) Top-down Integration:
   - Higher modules are tested first
   - If any lower module is not ready then stub (dummy module) is added
   - Advantage: higher modules are tested early
   - Disadvantage: higher modules are tested with dummy inputs

iii) Regression Testing:
   - Repeated testing
   - Testing of complete system when any new unit is integrated with the system
   - Regression testing ensures that that changes to system does not bring new errors
   - Same data can be used in regression test as used in the original test.
Level 3: System Testing
In systems testing complete system is tested as a whole. Following testing is done:

i) Recovery testing: system can recover from crash
ii) Security testing: system has security controls to protect information
iii) Stress testing: How much stress can the system tolerate during peak processing hours
iv) Performance testing: speed of system

Level 4: Final Acceptance Testing
It has two major parts:

i) Quality assurance testing: Quality standards are followed in developing the system
ii) User acceptance testing: User requirements are fulfilled by the system
   a) Alpha Testing: First stage, done in lab environment
   b) Beta Testing: Second stage, done in live environment

Stage VI: Systems Implementation

Activities: Following activities are involved in System Implementation:
- Conversion of data to the new system files.
- Training of end users.
- Completion of user documentation.
- System changeover.
- Evaluation of the system at regular intervals.

Activities during Implementation Stage:

I. Equipment Installation:
   (a) Site Preparation
   (b) Installation of new hardware / software
   (c) Equipment check out

II. Training Personnel:
   (a) Managers training
   (b) End user training
   (c) IT staff training

III. System Implementation Conversion Strategies:

Direct / Abrupt Conversion:
- Old system is discarded and new system is implemented at the same time
- Low cost
- High risk

Phased Conversion:
- Old system is discarded in a phased manner and the new system is also implemented module-by-module
- Implementation becomes easy
Parallel Conversion:
- new system and old system work for some time until the new system becomes completely reliable
- high cost
- low risk

Pilot implementation: The new system is first implemented in non-critical branch and if it is successful then it is moved to larger branches.

Activities involved in conversion:

i) Procedure conversion:
   - Operating procedures for the new system are documented
   - Communicated to users through training

ii) File conversion:
   - File conversion is done to make the old files compatible for the new system
   - This should be done in time
   - Controls like hash totals and record counts needs to be used while conversion
   - Old files should be kept for some time

iii) System conversion:
   - Shifting daily processing to the new system
   - Checking and balancing should be done with old system for some time

iv) Scheduling personnel and equipment:
   - Deciding data processing schedules for different departments
   - Should be done jointly by IT and department managers

Post Implementation Review (PIR)
- Review of new system after its implementation
- PIR should be done after 6 weeks to 6 months
- Three issues are evaluated
  I. Development evaluation
  II. Operation evaluation
  III. Information evaluation

System Maintenance
i) Scheduled maintenance – can be planned or pre-scheduled
ii) Rescue maintenance – for existing problems in system
iii) Corrective maintenance – for errors when they occur
iv) Adaptive maintenance – to change according to environment
v) Perfective maintenance – to add features
vi) Preventive maintenance – to prevent future occurrence of problems

Operation manuals (user guide/Operation Manual):
- Cover page, a title page and copyright page
- Introduction
- Table of content
- Main functions
- Troubleshooting
- A FAQ (Frequently Asked Questions)
- Contact details
- Glossary and index
Auditors Role in SDLC

The audit of system under development can have three main objectives:

1. To check the **efficiency, effectiveness and economy**
2. To check audit **trails and controls**
3. To check system’s **operation controls**

The auditor can achieve the above objectives by:

i. Attend project and steering committee meetings
ii. Examine project documentation
iii. Conducting interview
iv. Check the compliance with development standards
v. Examine systems operational documentation to see operational controls
vi. The auditor can give rating (1 to 10) for various SDLC phases
vii. Auditor may ask for technical expert report on technical aspects (e.g. database design)

Some control considerations for an auditor to examine are:

i. Documented policy and procedures
ii. Established project team
iii. Good infrastructure
iv. Trained development staff
v. Appropriate approvals
vi. Separation of development and test environment
vii. Standards are followed
viii. User department approval before implementing
ix. Version control
x. Safety of source code
xi. Systems maintains proper audit trail

*Best Wishes*
CHAPTER 3 – QRP (Quick Revision Points)

CONTROL OBJECTIVES

■ Need for controls in IT environment:
  1) High Cost of Data Loss
  2) Incorrect Decision Making
  3) Costs of Computer Abuse
  4) Value of Computer Hardware, Software and Personnel
  5) High Costs of Computer Error
  6) Maintenance of Privacy
  7) Controlled evolution of computer Use

■ Objective of the information systems audit function:
  1) Asset Safeguarding
  2) Data Integrity
  3) System Effectiveness
  4) System Efficiency
  5) Compliance

■ Effect of computers on internal control: (How internal controls changed due to computerization)
  a. Selection of personnel:
     - IT skills of new employees has to be seen
  b. Segregation of duties (SOD):
     - Separate login ID’s for users with different access rights
     - SOD more required in IT department
  c. Authorization procedure:
     - System based authorization
     - e.g. programmed credit limit approvals
  d. Record keeping:
     - Computerized controls are used. E.g. validity control, completeness control, user control, application control etc.
  e. Access to assets and records:
     - Earlier locks and keys were used
     - Now more focus on logical access controls
  f. Management supervision and review:
     - In manual system there was direct supervision and review of employees work
     - In IT environment supervision is done by system itself through logs
  g. Concentration of program and data:
     - More logical protection is required since program and data is concentrated in IT deptt.

■ Interrelated Elements of internal control: (as per COSO)
  1) Control environment
  2) Risk Assessment
  3) Control activities
  4) Information and communication
  5) Monitoring
Effects of computers on audit: Change in evidences collection and evidence evaluation technics in computerized environment

(a) Data retention and storage: Data in binary format
(b) Temporary logs: Logs are overwritten
(c) Absence of input document
(d) Lack of visible audit trail
(e) Lack of visible output
(f) Audit evidence
(g) Legal issues
(h) New opportunities and mechanism of fraud and errors:
   - System generated transactions
   - Systematic errors

Responsibility of controls: Management fulfills this objective by taking the following steps:
1. Develop and implement appropriate cost effective controls.
2. Assess the adequacy of internal controls in programs and operations.
3. Alignment of internal controls with the security policy of the company.
4. Reporting on internal controls.
5. Take corrective actions.
6. Identify scope of improvement.

Knowledge requirement for IS auditor:
1. Knowledge of business operations
2. Knowledge of legal compliance
3. Knowledge of information technology environment
4. Knowledge of control procedures
5. Knowledge of IS audit standards and IT controls standards
6. Knowledge of audit software tools

Functions of IS Auditor:
1. Review IT security policies and procedures
2. Risk assessment
3. Evaluation of controls
4. Evaluation of IS in terms of economy, efficiency, and effectiveness
5. Review of BCP/DRP
6. Investigating IT related frauds

Categories/Types of IS audits:
1. Application systems audit
2. Operating systems audit
3. Database audit
4. Network systems audit
5. IT Infrastructure audit
6. Systems Development, implementation and maintenance audit
7. Regulatory compliance audit
8. Investigation of IT related crimes, frauds & forensics

Steps in Information Technology Audit:
1. Scoping and pre-audit survey
2. Planning the audit
3. Fieldwork
4. Analysis
5. Reporting
6. Closure
**Audit Standards:**

Following are some of the audit standards or best practices standards related to IS audit:
1) Audit standards issued by ICAI
2) ISACA standards
3) COBIT
4) ISO 27001
5) ITIL
6) SAS 70
7) Global Technology Audit Guide (GTAG):
   - Issued by The Institute of Internal Auditors (IIA), USA
   - Provides control and security guidelines in IT environment
   - Following is the list of GTAG developed by IIA.
     - GTAG 1: Information Technology Controls
     - GTAG 2: Change and Patch Management Controls
     - GTAG 3: Continuous Auditing
     - GTAG 4: Management of IT Auditing
     - GTAG 5: Managing and Auditing Privacy Risks
     - GTAG 6: Managing and Auditing IT Vulnerabilities
     - GTAG 7: Information Technology Outsourcing
     - GTAG 8: Auditing Application Controls

**Cost effectiveness of control procedures:**

Internal controls are essential element in any business process but they have two problems which should be taken care of:
1st – Controls involve cost.
2nd – Controls make the process slow.

Thus the cost of implementing internal control should not exceed the benefits derived from it.

---

**Benefits:**
Reduction in expected loss due to control

**Costs:**
- Cost of design,
- Implementation
- Operation
- Maintenance

---

**Cost Benefit-Analysis of Control**

**Definition of controls:**
Controls are defined as “The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected”.

**Categories of Controls:**

- **Preventive controls**: To prevent error, omission or malicious act from occurring. These are designed by using three step process as follows:
  1. Understanding the vulnerability of the asset or process
  2. Understanding the probable threats
  3. Making provision to encounter such threats.

  Examples of preventive controls are:
  - Employing qualified staff
  - Segregation of duties
  - Access control
  - Proper documentation
  - Training of staff
  - Using firewalls
  - Using antivirus software
  - Password protection

- **Detective control**: To detect and report errors, omissions or malicious acts that have already occurred. These are implemented as follows:
  1. Setting parameters of desired result / actions
  2. Establishing mechanism for monitoring and reporting the deviations
  3. Updating the preventive controls for their further improvement

  Examples of detective controls are:
  - Hash totals
  - Check points
  - Echo controls
  - Audit logs
  - Duplicate checking of calculations
  - Intrusion detection system
  - Internal audit function
  - Cash count and bank reconciliation statement
  - Variance analysis

- **Corrective controls**: To correct errors or irregularities that have been detected. These are implemented to:
  1. Minimize the impact of threats
  2. Identify the causes of the problem
  3. Resolve the problems discovered by detective controls
(iv) Get feedback from preventive and detective controls
(v) Develop better process to minimize future occurrence of problems

Examples of corrective controls are:
- Business continuity plans
- Disaster recovery plans
- Backup procedure
- Rerun procedure

4. Compensatory controls: These are such controls which are effective for protection of assets in absence of some other direct control.
Example: segregation of duties in not required in very small business since direct supervision of owner compensates for segregation of duties

2. Classification based on Nature of IS resources

Another classification of controls is based on the nature of such controls with regard to the nature of IS resources or activity to which they are applied:
1. Environmental controls
2. Physical Access Controls
3. Logical Access Controls
4. IS Operational Controls
5. IS Management Controls
6. SDLC Controls

3. Classification based on Functional nature

When reviewing a client’s control systems, the auditor will be able to identify three components of internal control. Each component is aimed at achieving different objectives.
1. Accounting and financial controls
2. Operational controls
3. Administrative controls

Control techniques:

1. Organizational controls
2. Management controls
3. Financial controls
4. Data processing controls
5. Physical access controls
6. Logical access controls
7. SDLC controls
8. BCP/DRP controls
9. Application controls

1. Organizational Controls:
1. Definition of responsibilities and objectives of each function
2. Policies and procedures
3. Job descriptions
4. Segregation of duties

2. Management Controls:
   1. Senior management responsibility
   2. An official IT structure
   3. An IT steering committee

3. Financial Control Techniques:
   1. Authorization
   2. Budgets
   3. Cancellation of documents
   4. Documentation
   5. Dual control (Dual access)
   6. Input/ output verification
   7. Safekeeping
   8. Segregation of duties
   9. Sequentially numbered documents
   10. Supervisory review

4. Data Processing Environment Controls:
   - These controls are hardware and software related and include procedures exercised in the IS environmental areas.
   - The IS environmental areas include system software programming, on-line programming, on-line transaction systems, database administration, media library, application program change control and data center.

5. Physical Access Controls:

6. Logical Access Controls:

7. SDLC (System Development Life Cycle) controls:

8. Business Continuity (BCP) Controls:

9. Application Control Techniques:

   *** *** *** *** *** ***

Audit trail:
- Audit trails means logs that record activity at the system, application and user level
- It is a detective control
- Security objectives of audit trail are:
  1. Detecting unauthorized access to the system
  2. Facilitating the reconstruction of events
  3. Creating personal accountability

   *** *** *** *** *** ***
Specific controls in IT environment:
1. User controls
2. Systems development and acquisition control
3. Control over system and program changes
4. Quality control
5. Control over system implementation
6. Control over data integrity, privacy and security
7. Logical access controls
8. Physical access controls
9. Environmental controls

Now let us discuss these controls in details.

Control No 1. User controls (Application system controls)

The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage.

(i) Boundary controls
(ii) Input controls
(iii) Processing controls
(iv) Output controls
(v) Database controls

(i) Boundary Controls: Links the authentic users to the authorized resources

<table>
<thead>
<tr>
<th>Class of information used in boundary control</th>
<th>Type of input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal information</td>
<td>Name, date of birth, Acc No, password, PIN</td>
</tr>
<tr>
<td>Personal characteristics</td>
<td>Signature, figure print, voice, retina</td>
</tr>
<tr>
<td>Personal objects</td>
<td>ID card, badge, key, token</td>
</tr>
</tbody>
</table>

Three step process for boundary control
Step I  - Identification
Step II - Authentication
Step III - Authorization

Boundary control techniques are:
- Cryptography
- Passwords
- Personal identification number (PIN)
- Identification cards

(ii) Input Controls: Ensuring the accuracy and completeness of input into the system

Types of data coding errors:
- Addition
- Truncation
- Transcription
- Transposition
- Double transposition

Factors affecting coding errors are as follows:
- Long length of the code
- Alphabetic numeric mix
- Choice of characters
- Mixing uppercase/lowercase fonts
- Sequence of characters
List of input controls (Data validation controls):
- Proper form design
- Pre-printed forms wherever possible
- Check digit verification
- Field check
- Missing data check (record count)
- Completeness check
- Table lookup check
- Redundant data check
- Automatic system data entry

(iii) Processing Controls: To identify errors during processing of data
- Run-to-run totals (verifying data that is subject to process through different stages)
- Reasonableness verification (Two or more fields can be compared and cross verified)
- Edit checks (to verify accuracy and completeness of result)
- Field initialization (setting all values to zero before inserting the field or record)
- Exception reports (to report processing errors)
- Existence/Recovery Controls (check-point/restart logs)

(iv) Output Controls:
- Storage and logging of sensitive, critical forms
- Log of output program execution
- Control over spooling
- Control over printing
- Report distribution and collection controls
- Retention controls
- Existence/Recovery Controls
- Shredding of output

(v) Database Controls: To protect the integrity of a database
- Update controls:
  - Sequence check of transaction and master files
  - Ensure all records on files are processed
  - Processing of multiple transactions for a single master record in the correct order
  - Maintain a suspense account
- Report controls:
  - Control over standing Data
  - Print Run-to-Run control Totals
  - Print Suspense Account Entries
- Recovery controls:
  - Back-up and recovery strategies
  - Roll-forward (current state database from a previous version)
  - Rollback (previous state database from the current version) methods.

Control No 2. Systems development and acquisition control

Following are the key controls in such activity:
(i) Setting of long range strategic plans
(ii) Periodic review of systems for new requirements
(iii) Assignment of each project to a particular team
(iv) Setting of project milestones
(v) Periodic performance evaluation
(vi) Quality standards and checks throughout SDLC
(vii) Post implementation review
Task that must be undertaken during systems development phase and the controls required over them are as follows:

(i) **Problem definition:**
*Controls:*
- Proper investigation of problem
- Support of top management
- Understanding the impact of possible solutions

*Auditor's role:*
- Ensure that stakeholders have reached agreements on the problem or opportunity
- Ensure that stakeholders have an understanding of the risks in new system

(ii) **Management of change process:**
*Controls:*
- Promoting the need for change
- Preparing the organization (employees) for change
- To help users to understand new roles and responsibilities

*Auditor's role:*
- Review the change management policies and procedures.
- Evaluate the quality of decisions made about project management and changes

(iii) **Entry and feasibility assessment:**
*Controls:*
- Technical feasibility
- Operational feasibility
- Economic feasibility
- Behavioral feasibility

*Auditor's role:*
- Review feasibility reports
- Check that the proposed system is not imposed on the stakeholders

(iv) **Analysis of the existing system:**
*Controls:*
- Study the existing organizational history, structure and culture
- Study the existing information flows

*Auditor's role:*
- Review the methodologies used to analyze the existing system

(v) **Formulation of strategic Requirements:**
*Control:*
- Formulation of documented strategic requirement

*Auditor's role:*
- Strategic requirement is in alignment with overall business objectives

(vi) **Organizational and job design:**
*Controls:*
- The roles and responsibilities of the end-users should be defined and documented

*Auditor's role:*
- Review the organizational structure to see that there is no conflict of duties
- Assess the control risk associated and increase substantive testing if required

(vii) **Information processing systems design:**
*Controls:*
- User requirement mapping
- User interface designing
- Platform designing
- Physical designing
- Database designing
**Auditor's role:**
- Check that the design meets the strategic requirement agreed upon by the stakeholders.
- Review the requirement mapping done by the systems designers.
- Check the cost effectiveness and efficiency of the system.
- Check the auditability of the system.
- Review the need for audit module to be integrated in the system.

(viii) **Application Software Acquisition/Selection Process:**

**Controls:**
- Deciding evaluation criteria used in the vendor selection process, like stability of vendor, existing customer base of vendor, after sales support, customization etc.
- Detailed Request For Proposal (RFP) to be made.
- Technical comparative study of the available softwares.
- Cost Benefit analysis including hardware support required.

**Auditor's role:**
- Review vendor selection process.
- Check adequacy of RFP (request for proposal).
- Review contract with vendors for safeguard and completeness.

**Control No 3. Control over system and program changes**

**Risk associated with changes in system:**
- i) Unauthorized changes
- ii) Data loss
- iii) Poor segregation of duties
- iv) System breakdown
- v) New types of errors

**Change management controls:**
- i) Documented policy and procedures
- ii) Periodical review of systems
- iii) Standardized format for change request
- iv) Assess the impact of the requested change in system.
- v) Setting priorities of change requests.
- vi) Specific procedures for urgent and emergency changes.
- vii) Segregation of duties in systems change procedures.
- viii) Check over access rights during systems change procedures.
- ix) All changes should go through development, testing and implementation phase.
- x) Testing of changes in non-production environment before implementing.
- xi) Proper back-up plans for critical processes.
- xii) Quality checks procedures to see that all standards and procedures were followed.

**IS auditor's role:**
- i) Is the process of system and program change well documented?
- ii) Review change authorization procedure.
- iii) Checking quality review procedures being followed.
- iv) Have all the components of change passed the quality control procedures?
- v) Are defects discovered during quality review have been corrected?
- vi) Review of roles and responsibility of staff during change procedures.
- vii) Review of segregation of duties during change procedures.
- viii) Checking of back-up and contingency plans during change procedures.
- ix) Check that user manuals have also been updated according to the change.
- x) Checking the procedure for reporting of failures during testing the changes.
- xi) Checking data migration procedures and migration reports.
- xii) Checking that new and old parameters are compatible.
Control No 4. Quality control

Quality control management includes the following aspects:
- Establishment of a quality culture
- Defining quality plans and quality control practices
- Defining quality assurance responsibilities
- Quality control in System development life cycle methodology
- Program and system testing and documentation
- Conducting quality assurance reviews and reporting
- Training and involvement of end-user and quality assurance personnel
- Development of a quality assurance knowledge base
- Benchmarking against industry norms

Quality Standards:

(i) **Capability Maturity Model Integration (CMMI):** *(Discussed in chapter 8)*

<table>
<thead>
<tr>
<th>Five levels of CMM:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1 – Initial</td>
</tr>
<tr>
<td>Level 2 – Repeatable</td>
</tr>
<tr>
<td>Level 3 – Defined</td>
</tr>
<tr>
<td>Level 4 – Managed</td>
</tr>
<tr>
<td>Level 5 – Optimizing</td>
</tr>
</tbody>
</table>

(ii) **ISO 9000 Quality Management and Quality Assurance Standards:**
- ISO 9000 is a family of standards for quality management systems
- Not a product standard but a process standard
- monitoring processes to ensure they are effective
- keeping adequate records of processes and activities
- checking output for defects, with appropriate and corrective action where necessary
- regularly reviewing individual processes and the quality system itself for effectiveness
- facilitating continual improvement

Auditor’s Role:
The following are the general questions that the auditor will need to consider for quality control:

i) Does the system design follow a defined and acceptable standard?
ii) Are completed designs discussed and agreed with the users?
iii) Does the project’s quality assurance procedures ensure that project documentation (e.g. design documents, specifications, test and installation plans) is as per the organization’s technical standards and policies.
iv) Do quality reviews follow a defined and acceptable standard?
v) Are quality reviews carried out under the direction of a technically competent person who is managerially independent from the design team;
vi) Are auditors/security staffs invited to comment on the internal control aspects of system designs and development specifications?
vii) Are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends?
viii) Are defects uncovered during quality reviews always corrected?
ix) Are all system resources (hardware, software, documentation) that have passed quality review been placed under change control management and version control?
x) Has a System Installation Plan been developed and quality reviewed?
x1) Has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery?
Copyright Violations:
- Softwares can easily be copied
- Software piracy can be prevented by
  - Training
  - Policy and procedures
  - Application of general internal controls.
- Violation of copyright laws may lead to potential risk
- Copyright Notice

Contract / Warranties: Auditors review of IT-related contracts are:
  i) Contract does not limit supplier liability.
  ii) Contract objectives and performance measurements.
  iii) Acceptance criteria
  iv) Three key goals to achieve while contracting are:
      - clear criteria
      - negotiating
      - monitoring
  v) Identify major control weakness
  vi) Escrow agreement for source code
  vii) Approval procedure
  viii) Monitoring of performance
  ix) RFP is properly drafted
  x) Legal consultant was present
  xi) Verified with management
  xii) Acceptance tests are performed
  xiii) Documentation

Service Level Agreements (SLA):
- Formal agreement between a customer and organization
- Essential component of a legal contract
- Defines the terms and conditions of service
- Performance indicators are to be agreed and monitored
- E.g. SLA with organization’s IT Department, a facilities management contractor, an external agency, a telecommunications supplier, or a hardware maintenance contractor.

SLA should define the following:
  i) The level of technical support to be provided to users.
  ii) The procedures for proposing changes to the system.
  iii) Standards of security over data access, monitoring system and network use.
  iv) Emergency requirements
  v) And a schedule of charges for the services to be provided.

Auditors review:
  i) Service provider should comply with all legal requirements
  ii) Should provide for a right to audit clause and requirement of control responsibilities.
  iii) Responsibility of the service provider to establish performance monitoring procedures.
  iv) SAS 70 audit compliance by the service provider.
  v) Business continuity measures to be put in place to ensure continuity of service.
  vi) Non disclosure requirements
  vii) Insurance requirements.
Control No 5. Control over system implementation

(i) Procedure development:
- Procedures should cover every aspect
- Procedures should cover both hardware and software
- Procedures should be documented in clear terms
- Procedures should be as per the job responsibilities of the users

(ii) Conversion:
Conversion from old to new system involves the following activities:
- Deciding the procedures for data migrating
- Data cleansing before data conversion
- Accuracy of conversion like record counts and control totals
- Exception reports
- Verifying and signing off by the system owner

Conversion strategies:
- Direct / Abrupt conversion
  - High risk
  - Low cost
- Phased conversion
  - Balanced approach
- Parallel conversion
  - Low risk
  - High cost

Auditor's review:
- Review data conversion plan
- Data conversion strategy
- Conversion timetable
- Allocation of staff
- Roles and responsibilities during conversion
- Data cleaning was done before conversion
- How rejected data was treated
- Testing of tailor-made software
- Review data correctness of data migration
- Review segregation during conversion
- Data backup of new system
- Audit trail is preserved

(iii) Acceptance testing:
Accepting testing is a complete end-to-end test of the new system including all its manual procedures. It is aimed to provide the confirmation that:
- The end user requirement has been met
- Operational documentation is accurate, comprehensive and usable
- End user documentation is accurate, comprehensive and usable
- Supporting manual procedures work effectively
- Help desk function is performing effectively
- Backup and recovery procedures are working effectively

In acceptance testing following testing are done:
(a) Performance testing
(b) Volume testing
(c) Stress testing
(d) Security testing
(e) Clerical procedure checking
(f) Back-up and recovery procedure testing
Role of IS Auditor in systems acceptance testing phase:
   a) Review of acceptance testing plan
   b) Is the acceptance testing plan:
      - fully documented
      - allocates adequate resources for testing
      - defines individual roles and responsibility
      - fully involves end-user in testing
      - includes ancillary procedures
   c) Segregation of duties during testing phase.
   d) System has built-in controls
   e) System provides the capability to track events
   f) How testing data has been designed
   g) Access controls during testing to avoid unauthorized changes.
   h) Audit trail of testing and changes is maintained
   i) Review regression tests

(iv) User training:
   Training would involve
   - Manager’s training
   - End user training
   - IT staff training
   - Systems administrator training
   - Other support staff training
   - Ongoing user support along with training

(v) Systems maintenance:
   Three categories of maintenance:
   I. Corrective maintenance
   II. Adaptive maintenance
   III. Perfective maintenance
   Auditor’s review:
   - Ratio of actual maintenance cost per application versus the average cost
   - Average time to fix a problem
   - Different types of change requests
   - Number of production problems per application.
   - Instances of divergence from standards
   - Number of softwares returned to development due to errors
   Common performance measurement techniques are:
   - Throughput
   - Utilization percentage
   - Response time

(vi) Post implementation review:
   PIR is done to see whether the new system:
   - Fulfills the business objectives
   - Fulfills the user expectations
   - Fulfills the technical requirements
   Timing - not be done too early or too late
   PIR team – impartial
   Activities to be reviewed/undertaken in PIR:
   - Main functionality of the new system
   - Systems performance and operations
   - Development techniques used
   - Authorizations
   - Final conclusions and recommendations
   - Any new benefit
Action on PIR report: The authorizing authority, based on the PIR report:
- Approve the system
- Approve plans to modify the system
- Terminate the system and give instructions for new course of action

Control consideration: Auditors review during PIR:
- Interview end-users in each functional area to know their satisfaction level.
- Interview security, operations and maintenance staff to know their response.
- Whether system fulfills all “user requirement specifications”.
- Previous system has been removed, if not, then the reasons for that.
- Review problem reports of the new system.
- Internal controls in the new system are operating as planned.
- Check service level agreements with internal as-well-as with external agencies.
- Check systems back-up and restoration mechanism is documented and working.
- Review the “business case”

Control No 6. Control over data integrity, privacy and security

Information classification policy / guideline:
- Top secret
- Highly confidential
- Proprietary
- Internal use only
- Public documents

Data integrity control:

<table>
<thead>
<tr>
<th>Control category</th>
<th>Threat/Risk</th>
<th>controls</th>
</tr>
</thead>
</table>
| Source data control               | Invalid, incomplete or inaccurate source data input | - Proper form design  
- Pre-printed forms wherever possible  
- Titles, headings and instructions in manual forms  
- Sequentially pre-numbered forms  
- Turnaround documents  
- Authorization review  
- Cancellation of processed documents  
- Check digit verification |
| Input validation routines         | Invalid or inaccurate data in transaction files | - Field check  
- Range and limit check  
- Sequence check  
- Duplicate check  
- Missing data check  
- Reasonableness check  
- Completeness check  
- Table lookup check  
- Batch check  
- File check  
- Maintain error logs |
| Online data entry controls        | Invalid or inaccurate transaction input entered through on-line terminals | - Field check  
- Reasonableness check  
- Redundant data check  
- Used ID’s and password check  
- Automatic system data entry  
- Completeness check  
- Maintenance of transaction logs |
| Data processing and storage control | Inaccurate or incomplete data in computer-processed | - Design of policies and procedures  
- Exception reporting |
<table>
<thead>
<tr>
<th><strong>Data Integrity Policies:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>i) Regular updating the Virus-Signature</td>
</tr>
<tr>
<td>ii) Software Testing</td>
</tr>
<tr>
<td>iii) Division of Environments</td>
</tr>
<tr>
<td>iv) Avoiding Version Zero Software</td>
</tr>
<tr>
<td>v) Offsite Backup Storage</td>
</tr>
<tr>
<td>vi) Quarter-End and Year-End Backups</td>
</tr>
<tr>
<td>vii) Disaster Recovery plan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Auditors review over data privacy and security:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>i) Who is responsible for the accuracy of the data?</td>
</tr>
<tr>
<td>ii) Who is permitted to update data?</td>
</tr>
<tr>
<td>iii) Who is permitted to read and use the data?</td>
</tr>
<tr>
<td>iv) Who is responsible for determining who can read and update the data?</td>
</tr>
<tr>
<td>v) Who controls the security of the data?</td>
</tr>
<tr>
<td>vi) Control over outsourced activities</td>
</tr>
<tr>
<td>vii) Contractually liability to protect the sensitive information</td>
</tr>
</tbody>
</table>

\[ *** \quad *** \quad *** \quad *** \quad *** \quad *** \]

**Security concepts and techniques**

**Cryptosystem:**
- **Cryptography**: science of encrypting and decrypting written communication.
- **Cipher**: algorithm for performing encryption or decryption
- **Encryption**: process of transforming readable information into unreadable format
- **Decryption**: reverse process of encryption in which unreadable information is converted back into readable information.
- **Plain text**: original human readable text before encryption.
- **Cipher text**: unreadable text generated after encryption.
- **Symmetric encryption**: single key encryption (e.g. DES, AES, Blowfish)
− **Asymmetric encryption**: uses key pair, private key and public key (e.g. RSA)

![Asymmetric Encryption Diagram]

− **One-way encryption**: cannot be converted back to the plain text (e.g. MD5, sha1)

**Data encryption standard (DES):**
− Algorithm for symmetric encryption.
− Developed by National Institute of Standards and Technology (NIST), USA in 1976.
− Small key size of 64 bits
− Weak algorithm.
− Replaced by TDES (Triple DES), Advance Encryption Standard (AES), Blowfish encryption standard, RC5 encryption standard etc.

**Public Key Infrastructure (PKI):** Public Key Infrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. It uses asymmetric encryption and hash function to generate digital signature.

**Digital certificate:**
- Certify the identity of an individual or institution.
- Links the identity of an individual or institution to a digital public key.
- Contents are prescribed by the X.509 standard

<table>
<thead>
<tr>
<th>Content of an X.509 V3 Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Version number of the certificate format</td>
</tr>
<tr>
<td>- Serial number of the certificate</td>
</tr>
<tr>
<td>- Signature algorithm identifier</td>
</tr>
<tr>
<td>- Issuer of digital certificate</td>
</tr>
<tr>
<td>- Validity period</td>
</tr>
<tr>
<td>- Unique identification of certificate holder</td>
</tr>
<tr>
<td>- Public key information</td>
</tr>
</tbody>
</table>

**Certifying authority**: Certifying Authority (CA) provides all of the services required to issue, store, manage, and revoke digital certificates for users of digital signature.

**PKI control policies:**
- Methods of initial verification of the user (identity and address proof)
- Maximum validity period of digital certificate should not be more than 2 years.
- Digital certificate will be revoked when private key of user is lost.
- Updating the database of revoked certificates.
- Protect root key i.e. private key of certifying authority.
- Maintenance of proper logs of all activities.

**Data security and public network:**

**Firewalls:**
- Firewall is a system to protect private network from public network
- Firewalls can be hardware based or software based
- Firewalls block or allow traffic based on rules
- Rules can be static or dynamic
- Firewall should fail close rather than fail open
Types of firewall:

Type I Packet filtering firewall:
- Checks data packet header only
- Fast in performance
- Less secure
- Easy to misconfigure
- Useful for small office and home office (SOHO) systems

Type II Stateful inspection firewall:
- Type of packet filtering firewall
- Monitor the state of the TCP connection
- TCP session starts with an initial “handshake”
- Firewall adds the connection information to a table
- Verifies that inbound traffic is in response to internal requests

Type III Proxy server firewall:
- Intermediary between internal and external IP addresses
- Block direct access to the internal network
- Rewrites packet headers
- content filtering
- anti-spam filtering
- protects against encapsulation techniques

Type IV Application-level firewall:
- Perform application-level screening
- Examine each packet
- Provide additional screening of the packet payload
- Provide the strongest level of security
- Slower
- Require greater expertise to administer properly

Firewall services and configuration: Firewall can provide some additional features like:
1) Network address translation (NAT) – Changing internal IP
2) Dynamic host configuration protocol (DHCP) – allocate dynamic IP
3) Virtual private network gateway (VPN gateway)

Unauthorized intrusion:
- Intrusion means to enter or disrupt any system or network
- Intrusion detection means to monitor and stop intrusion
- Intrusion detection system (IDS) is like firewall but more expensive and intelligent
- IDS is used as complementary with firewall
- IDS update the firewall

Intrusion Detection systems fall into two broad categories:
- Network based systems
- Host based systems
- Operating system kernel
**Hacking**: Hacking is an act of penetrating computer systems to gain knowledge about the system and how it works.

Hackers: Hacking with good intention
Crackers: Hacking with bad intention
Phreakers: Hacking using telephone line

Hacking is normally done through the use of
- backdoor program
- password cracking software
- application exploits
- social engineering

**What damage can a Hacker do?**
- This depends upon what backdoor programs are hiding on the PC
- Different programs can do different amounts of damage
- Hackers can steal data and personal information
- Hackers can put backdoor programs
- Hackers can see everything you are doing, and can access any file on your disk.
- Hackers can write new files, delete files, edit files
- hacker could install several programs on to your system without your knowledge

How do Hackers hack?
(i) NetBIOS: exploits a bug in Windows 98.
(ii) ICMP Ping (Internet Control Message Protocol): Denial-of-Service attack,
(iii) FTP (File Transfer Protocol):
(iv) rpc.statd: unchecked buffer overflow problem.
(v) HTTP (Hypertext Transfer Protocol): unchecked buffer overflow

**Data privacy**:  
- Data privacy means **to protecting private and sensitive data from disclosure**  
- Data has to be shared without disclosing the personnel identity of any individual  
- The most common source of data that are affected by data privacy issues are:
  - Health information
  - Criminal justice
  - Financial information
  - Genetic information
  - Locational information  
- **Protecting data privacy in information systems**: In information systems, the privacy policy has to be communicated and enforced across the system and network. This is done by several **privacy protocols** which communicate and enforce user's privacy preferences automatically. These fall under two categories:
  - **Policy Communication**: P3P - Platform for Privacy Preferences
  - **Policy Enforcement**: XACML - The eXtensible Access control markup language
  - EPAL - The Enterprise Privacy Authorization
  - WS-Privacy - Web Service Privacy

**Control against virus and other malware**:  

**Virus**:  
- Malicious program  
- Attaches itself to other files/program
- Self-replicating
- Geometric progression

There are three types of anti-virus software.
(i) **Scanners**:
  - Based on virus signature
  - Required to be updated frequently
(ii) **Active Monitor and Heuristic Scanner**
  - Studies the behavior of system
o Looks for OS calls and BIOS calls, which resemble virus action
o Sometimes cannot differentiate between genuine systems calls and virus action

(iii) **Integrity Checkers**
- Can detect any unauthorized changes to files on the system
- Stores the CRC (checksum)
- When a program is run, the CRC recomputed and compared with stored value

**Control No 7. Logical access controls**

**Logical access paths:**
- Online terminals
- Operator console
- Batch job processing
- Dial-up ports
- Telecommunication network

**Logical access issues threats and exposures:**

(a) Technical exposures
- **Data diddling:** unauthorized modification in the input data
- **Logic bombs:** malicious program codes deliberately put in the software by the programmer
- **Time bombs:** same as logic bomb, but is set to activate at a particular future time
- **Trojan horse:** non-self-replicating malware that comes from outside
- **Worms:** self-replicating malware
- **Rounding down:** rounding down of amount and transferring it in a separate account.
- **Salami techniques:** cutting small part of amount and transferring it in a separate account
- **Trap doors:** loopholes in program to gain access into the system
- **Asynchronous attack:** intercepting asynchronous transmission lines
- **Data leakage:** coping information out of computer system to some media
- **Wire-tapping:** intercepting data over telecommunication network
- **Piggybacking:** getting unauthorized access by following an authorized data packet
- **Denial of service:** shutdown the service of any website for some period
- **Masquerading:** to impersonates as a genuine user to gain unauthorized access
- **Spoofing:** impersonate as someone else
- **Phishing:** fake website is made resembling the original website

(b) Computer crime exposure

Such frauds results in:
- Financial loss to the organization
- Legal consequences
- Loss of credibility
- Industrial espionage
- Leakage of confidential information.

People involved in computer crime:
- Hackers / Crackers / Phreakers
- Disgruntled Employees
- IS personals
- End users
- Former employees
- Competitors
- Organized criminals.
Logical access controls:

<table>
<thead>
<tr>
<th></th>
<th>i) User registration procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) User access management</td>
<td>(ii) Privilege management</td>
</tr>
<tr>
<td></td>
<td>(iii) Password management</td>
</tr>
<tr>
<td></td>
<td>(iv) Periodic review of user access rights</td>
</tr>
<tr>
<td>b) User responsibilities</td>
<td>(i) Use of strong password</td>
</tr>
<tr>
<td></td>
<td>(ii) Unattended user equipment</td>
</tr>
<tr>
<td>c) Network access control</td>
<td>(i) Policy on use of internet</td>
</tr>
<tr>
<td></td>
<td>(ii) Enforced path using firewall</td>
</tr>
<tr>
<td></td>
<td>(iii) Segregation of networks</td>
</tr>
<tr>
<td></td>
<td>(iv) Network connection and routing control</td>
</tr>
<tr>
<td></td>
<td>(v) Security of network services</td>
</tr>
<tr>
<td>d) Operating system access control</td>
<td>(i) Automated terminal identification</td>
</tr>
<tr>
<td></td>
<td>(ii) Terminal log-on procedures</td>
</tr>
<tr>
<td></td>
<td>(iii) User identification and authentication</td>
</tr>
<tr>
<td></td>
<td>(iv) Password management system</td>
</tr>
<tr>
<td></td>
<td>(v) Use of system utilities</td>
</tr>
<tr>
<td></td>
<td>(vi) Duress alarm to safeguard users</td>
</tr>
<tr>
<td></td>
<td>(vii) Terminal time out</td>
</tr>
<tr>
<td></td>
<td>(viii) Limitation of connection time</td>
</tr>
<tr>
<td>e) Application and monitoring system access control</td>
<td>(i) Information access restriction</td>
</tr>
<tr>
<td></td>
<td>(ii) Sensitive system isolation</td>
</tr>
<tr>
<td></td>
<td>(iii) Event logging</td>
</tr>
<tr>
<td></td>
<td>(iv) Monitor system use</td>
</tr>
<tr>
<td></td>
<td>(v) Clock synchronization</td>
</tr>
<tr>
<td>f) Mobile computing</td>
<td>(i) Mobile computing</td>
</tr>
</tbody>
</table>

Role of IS auditor in evaluating logical access control:
- Security policies and procedures
- Risk assessment
- Access control administration
- Review password policy, e.g. does the system requires:
  i) Minimum length
  ii) Alfa-numeric
  iii) Mandatory change after certain days
  iv) Old password cannot be set again as new
  v) Limited number of unsuccessful attempts
- Potential access paths should be identified
- Access control at operating system level
- Access control at application program level.
- Redundant login ID’s

Control No 8. Physical access controls

Physical access issues and exposure:
Following can be the threats in an organization due to improper physical access:
- Unauthorized person getting access in restricted areas of the organization.
- Employees gaining access to unauthorized areas within the organization.
- Damage, theft or embezzlement of equipments.
- Abuse of systems resources.
- Improper disposal of computer and hardware devices.

Sources of physical access threat can be from:
- Unauthorized person: (thieves, hackers, former employees, competitors or ignorant persons)
- Employees: (disgruntled employees, employees on strike, employees under suspension)
Infrastructure to be protected:

i) Computer room
ii) Server room
iii) Network devices (switches and routers)
iv) Telecommunication equipments
v) LAN
vi) Firewalls
vii) Operators console
viii) Back-up storage media
ix) Disposal sites
x) UPS room

Physical access control mechanism: Physical access control is a three step process

Step I. Identification: The user gives his identification to the system

Step II. Authentication: The system authenticates the user on the basis of some information given by the user. For this purpose the user can use the following mechanism

<table>
<thead>
<tr>
<th>Remembered information</th>
<th>Name, account number, password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object possessed by the user</td>
<td>Badges, smart cards, key</td>
</tr>
<tr>
<td>Personal characters</td>
<td>Figure prints, voice prints, signature</td>
</tr>
</tbody>
</table>

Step III. Authorization: The system authorizes the user for various resources. This authorization can be by

- Ticket oriented approach: In ticket oriented approach the authorization matrix gives the authorization level for various users for various resources
- List oriented approach: In list oriented approach each resource has a list of users who can access the resources.

Physical access controls:

a) Locks on doors: Locks can be of following types

- Normal lock
- Cipher lock
- Electronic door locks
- Biometric door locks

b) Physical identification medium:

- Identification badges
- Personal Identification Number (PIN)
- Plastic cards

c) Maintenance of log:

- Manual logging
- Electronic logging

d) Other measures:

- Security guards
- Video cameras
- Dead man doors
- Controlled single point entry
- Security alarm
- Boundary fencing
- Visitor entry through escorts

Auditing physical access:

- Risk assessment
- Review of security policy
- Building plans, cable diagrams
- Camera locations, security guard location
- Control assessment
- Taking a tour of the organization
- Interviewing staff
- Examination of physical access logs
- Check all entry and exit points
- Glass windows, air ducts and false ceiling
Control No 9. Environmental controls

Information systems resources may be categorized as follows:

i) Hardware and Media
ii) Information Systems Infrastructure
iii) Computer rooms and server room
iv) Printer rooms and storage areas
v) Cabling ducts, Power source
vi) Heating, ventilation and air conditioning (HVAC)
vii) Important Documentation
viii) Supplies
ix) People

Common environmental threats, both natural and man made, are:

- Fire
- Natural disasters
- Extreme variation in temperature such as heat or cold, snow and light.
- Power spike, power failure.
- Electrical shock
- Air conditioning failure,
- Humidity, dust and smoke.
- Food particles, residues and smoking in computer room.
- Insects and rodents.
- Equipment failure
- Electro-magnetic interference.
- Radiations
- Chemical effects
- Bomb threat

Control over environment exposures:

- Documented policies and procedures
- Fire proof walls, floors and ceilings
- Concealed protective wiring
- Pest control
- Ventilation and air-conditioning
- Prohibition against eating, drinking and smoking
- Uninterrupted power supply (UPS)
- Electrical surge protector/spike busters/line conditioners
- Smoke and fire detectors
- Manual fire alarm
- Emergency power off
- Hand-held fire extinguishers
- Sprinkler system (Wet-pipe sprinkler, Dry-pipe sprinkler)
- Strategically locating the computer server room
- Regular fire inspection

Auditing environmental controls: Auditor review:

- Policy and procedures
- Building plans, wiring plans,
- Location of computer/server rooms
- Preventive maintenance
- Fire proof construction material
- Fire extinguishers (Location, date of refilling)
- Emergency procedures, evacuation plans
- BCP/DRP (business continuity plans and disaster recovery plans)
- Maintenance logs, AMC, Service records (of sprinklers, UPS, generators)
CHAPTER 4 – QRP

TESTING – GENERAL AND AUTOMATED CONTROLS

Introduction to Basis of Testing (Reasons for Testing):
- Testing is a scientific process performed to determine whether the
  - Controls are designed correctly (Test of Design - TOD)
  - Controls are working effectively (Test of Effectiveness - TOE)
- Testing involves understanding the process and the expected results
- Testing can be compliance testing and substantive testing
- Sampling is used

The Information Systems Control Audit involves the following three phases:

Phase I: Audit Planning
- Audit plan/program is prepared
- Examines the materiality and significance of different processes
- Determines the nature, timing and extent of audit procedures.
- Consider both quantitative and qualitative factors
- Planning is done during the audit work

Phase II: Audit Testing
- Decides the test plan
- Decide the nature, timing and extent of testing
- Decide the testing methodologies.
- Use of CAAT (computer assisted techniques)
- Use both valid and invalid test data
- Focus on high risk areas
- Use of documentary evidence, corroborating interviews and personal observation
- Information gathered during has to be validated (cross-checked)

IS Controls Audit Process:
- Understanding the organization
- Understanding the network
- Identifying the key areas of audit interest
- Assessing IS risk
- Identifying critical controls
- Preliminary understanding of IS controls, and
- Performing other audit planning procedures
Identify Key Areas of Audit Interest:

- Auditor should identify key areas of audit interest
- Key financial applications and data
- Critical systems and processes
- For each key area, the auditor should document general support systems
  - The operational location of each key system or file
  - Critical components of the system e.g. hardware, software, firewall, routers etc.
  - Other systems or resources that support the key areas of audit interest
  - Prior audit/problem reports
- Identify all access paths to/from key areas of audit interest.
- Prioritize critical systems, files, processes or locations
- Auditors documentation during preliminary understanding of controls include:
  - Documented security plans
  - Documented risk assessments
  - Identification of entity-wide controls
  - Identification of business process level controls
  - areas where such controls are missing
  - internal or third-party IS audit
  - special testing report
  - Managements action plan
  - prior years’ audit findings
  - IS incident
  - Certification and accreditation
  - BCP/DRP
  - third-party IT services
  - Applicable laws and regulations
  - communication with management
  - service auditors report

Performing Information System Control Audit Tests:

The auditor should identify and evaluate the controls at following three levels:

(i) **Entity wide or component level**
(ii) **System level**
    - Network
    - Operating system
    - Infrastructure applications
(iii) **Business process application level**
    - General controls
    - Application specific controls

Test Effectiveness of Information System Controls

- Testing is be done on tiered (Level) basis
- Ineffective controls at higher tier (Level) results in ineffective controls at the lower tier.
Test of General Controls at the Entity-wide and System Levels
- Procedures used - observations, inquiry and inspection
- Approvals can be checked on sample basis
- If entity-wide and system level controls are poor, the auditor should:
  (i) Determine the risks
  (ii) Check any manual controls that compensates
- Auditor should report the findings together with the recommendations

Test of General Controls at the Business Process-Application Level
- Evaluate and test the effectiveness of general controls at business process-application level
- If general controls are poor, business process application controls and user controls will be ineffective

Test of Business Process Application Controls and User Controls
- Perform the tests on business process application controls and user controls
- If IS controls are poor see the control risk
- Report the findings together with the recommendations
- IS controls that are not effective in design do not need to be tested

appropriateness of Control Tests: Appropriate mix of audit procedures includes:
- Inquiries
- Interview
- Questionnaires
- Observations
- Document review
- Inspection of approvals
- Analysis of system information (e.g. configuration settings, access control list etc.)
- Use of CAAT’s
- Re-performance using dummy data

Multiyear Testing Plans
- Prepared in case of recurring audit
- Audit plan is made for more than one year
- Should not cover more than three year period
- Re-evaluate the plans annually
- All the areas are not tested each year, but are spread during the multiyear period
- High risk areas should be covered every year
- Such multiyear plan may not be appropriate in following situations
  - First-time audits
  - Where business process applications or controls have not been tested within a sufficient recent period
  - Entities where entity-wide general controls are poor.

Documentation of Control Testing Phase
The auditor should document the following during control testing phase:
- Understanding of information systems
- Control objectives
- Control techniques
- Specific tests performed
- Compensating control
- Material weaknesses
Phase III: Audit Reporting

Audit Reporting: After completing the testing phase,
- summarizes the results
- draws conclusion
- report the result

Audit Objectives
- Determine which IS control techniques are relevant to the audit objectives
- Determine whether IS control technique is suitably designed to achieve the control objective
- Perform tests to determine whether such control techniques are operating effectively

Report Audit Results
- Evaluate the effect of identified IS control weaknesses
- Financial audits, attestation engagements and performance audits
- Consider other audit reporting requirements and related reporting responsibilities

Substantive Testing
- If controls are not effective, then substantive testing may be required
- Substantive testing gives the accuracy of information being generated by a process
- Computer aided audit tools (CAAT’s) can be used

Documenting Results
The final step involves evaluating the results of the work and preparing a report on the findings. The audit results should include the findings, conclusions and recommendations.

Audit Findings
- Audit findings should be formally documented
- Recommendation in case of control deficiency
- Audit finding form can be used to document both control strengths and weaknesses
- The information can then be used to prepare the formal audit report

Analysis: Four steps in analysis are:
1. Re-examine the standards and facts
2. Determine the causes of deviations
3. Determine the materiality and exposure of the deviation
4. Determine possible recommendations for the corrective actions

Re-examination the standards and facts:
‘standard’ (for comparison to the facts) and the ‘facts’ (to compare to the standards)
- Standards Compliance: Standards are the procedures, operating guidelines, regulations, best practices or other pre-defined methodologies. Four situations may occur:
  i) No standard exists (this implies high degree of risk)
  ii) Standard exist but is not formal
  iii) Standard is formal and published but is redundant or expensive
  iv) Standard is formal and appropriate for evaluating the work performed
- Facts: Auditor must evaluate the gathered facts
  i) Adequately supported by photocopies or evidence
  ii) Get the agreement of the client
  iii) To ensure that findings are accurate the sample should be:
     o Large
     o Representative

****   ****   ****   ****   ****   ****
- Concurrent or continuous audit and embedded audit modules:
  - Audit evidence is collected at the time of processing of data
  - This techniques works in a paperless environment

I. Snapshots:
  - Audit module/software takes screen shots of the transaction
  - Screen shots of critical / material transaction
  - Screen shots are used for checking authenticity, accuracy and completeness
  - Precise timing of the screen shot
  - Examining and reporting mechanism of these screen shots

II. Integrated test facility (ITF):
  - ITF module creates dummy entities
  - Auditor uses these dummy entities to process dummy data
  - ITF should tag dummy data
  - Dummy data is removed later
  - ITF can also tag live data and apply test on it

III. System control audit review file (SCARF):
  - Audit software modules is embedded within the host application
  - Continuous monitoring of system’s transactions
  - Placed at predetermined points to gather information
  - Information is written onto the SCARF master file
Auditor might use the SCARF technique to collect the following information:
  i) Application systems errors
  ii) Policies and procedures variances
  iii) Exception transactions
  iv) Statistical samples
  v) Snapshots and extended records
  vi) Profiling data
  vii) Performance measurement

IV. Continuous and intermittent simulation (CIS):
  - Exception or unusual transaction are examined
  - CIS takes input data from the system to process the selected transaction
  - CIS now process the transaction by simulation
  - Results are compared to determine differences
  - Exceptions are written to a log file
  - CIS does not require modification to the application system.

Advantage of concurrent audit techniques:
- Timely audit
- Comprehensive and detailed testing
- Evaluating the system
- Effective where audit trail is missing
- Surprise test capability
- Can be used as training tool

Disadvantage of concurrent audit techniques:
- More resources are required
- Involvement of auditor
- Requires expert knowledge
- Works only in stable system
Hardware testing and review:

Hardware testing includes the following testing:
- Functional testing
- Performance testing
- Memory capacity testing
- Security testing
- Compatibility testing
- Capacity testing
- Recovery testing
- Accessibility testing.

The auditor needs to review hardware in following areas:

Hardware acquisition:
- Documented policy regarding H/W acquisition
- Specific criteria before acquiring new H/W
- Review purchasing procedure
- Check approvals for new purchases
- Cost-benefit analysis
- Documentation regarding H/W specifications, installation, warranties etc is properly maintained

Hardware change management:
- Documented policy regarding H/W change management
- Every change should have proper approval
- Review change procedure
- Review procedure for requesting change or updation
- Operation documentation is also updated when there is a change in H/W
- Proper coordination during change management between different departments

Hardware preventive maintenance:
- Check the frequency of preventive maintenance.
- Check whether service report is generated on every visit of service engineer.
- Review annual maintenance contracts (AMC).
- Check that preventive maintenance does not obstruct production environment.

Hardware general review:
- Check service level agreements for any H/W service taken from vendors.
- Check control procedures for safeguarding of H/W.
- Check performance and problem logs.

Operating system review: Auditor should consider the following issues:
- Approval procedure
- Change management policies.
- Selection procedure for acquiring OS.
- Cost-benefit analysis
- Test procedures
- Access control
- User authorization
- Operational documentation
- Staff training
- OS maintenance
- Vendor support.
- OS updating
- Problem log
- Service reports
- Audit trail
- Interface
- Application support
Network review:

The unique nature of each LAN makes it difficult to define standard testing procedures to effectively perform a review. The reviewer should identify the following:
- LAN topology (Bus, Ring, Star, Line, Mesh)
- Major LAN components (Servers, Switches, Routers, Modems etc.)
- LAN uses, major applications over LAN
- LAN administrator
- Major group of LAN users

While examining LAN the auditor should review the following:

Physical control:
- LAN documentation
- LAN operating manual
- Redundant nodes or empty jacks
- Structured cabling with casing
- Switch in a locked cabinet

Logical control:
- Password protected
- Data encryption
- Network monitoring tools
- Firewall
- Logout if inactive
- Network logs

Environmental control:
- Proper temperature and humidity
- UPS
- Fire extinguishers
- Fire and smoke detectors
- Static electricity guards

Best Wishes
## CHAPTER 5 – Quick Revision Points (QRP)

### RISK ASSESSMENT METHODOLOGIES AND APPLICATIONS

#### Basic Terms:

**Risk**: likelihood that vulnerability of an asset will be exploited by threat resulting in loss

The risk increases in IT environment due to following reasons:
- High rate of technological changes.
- Use of network like LAN and WAN.
- Use of internet
- Decentralization of management and control.
- Weak legal and regulatory framework for IT environment.
- New and unknown types of threats.

**Threat**: any event that can cause loss

**Vulnerability**: weakness in the information system

**Exposure**: expected loss

**Likelihood**: probability of occurrence

**Attack**: action that is meant to break the confidentiality, integrity, availability of system

**Residual risk**: risk that still remains after implementing the controls

#### Threats to computerized environment:

1. Power loss
2. Communication failure
3. Disgruntled employees
4. Errors
5. Malicious codes
6. Abuse of access privileges
7. Natural disasters
8. Theft or destruction
9. Downtime
10. Fire

#### Threats due to cyber crimes:

1. Embezzlement
2. Frauds
3. Theft of proprietary information
4. Denial of service
5. Sabotage
6. Computer virus
7. Intrusion

#### Risk management: systematic process to manage and control the risk for an organization

1. Risk identification
2. Risk assessment
3. Risk ranking
4. Develop risk mitigation and control plan
5. Implement risk management plan
6. Re-evaluate the risk

Risk management cycle
Risk management process:

Step 1: Identification of Information Assets
Step 2: Valuation of Information Assets
Step 3: Identifying the potential threats
Step 4: Information Risk Assessment
Step 5: Developing strategies for Information Risk Management

Step 1: Identification of Information Assets

Intangible Assets:
- Data / information
- Software

Tangible Assets:
- People
- Hardware
- Networking devices
- Building and infrastructure
- Documentation

Step 2: Valuation of Information Assets

Classify the information:
- Top secret
- Secret
- Confidential
- Sensitive
- Unclassified

Step 3: Identifying the potential threats

Common classes of threats are:
- Errors
- Malicious attack
- Fraud
- Theft
- Equipment / Software failure

Vulnerabilities can be:
- Lack of user knowledge
- Lack of security functionality
- Poor choice of passwords
- Untested technology
- Transmission over unprotected network

These threats could affect the following key characteristics of information:
- Confidentiality
- Integrity
- Availability

Step 4: Information Risk Assessment

- Vulnerability Assessment
- Probability or Likelihood Assessment
- Impact Analysis

Step 5: Developing strategies for Information Risk Management

- Risk Avoidance
- Risk Mitigation / Reduction
- Risk Transfer
- Risk Retention / Acceptance
**Types of risk:** Risk can be divided into two categories:

I. **Systematic risk:**
   - Unavoidable risks
   - Due to external factors
   - Beyond the control of the organization
   - Can only be reduced by management policy and initiative

II. **Unsystematic risk:**
   - Specific risks which relate to some technology
   - Can be mitigated by using some advanced technology

**Risk identification:**
- Try to locate all possible risk
- Comprehensive manner
- Cover all departments/processes/activities
- Internal/external risk factors.

Following questions will help in risk identification:
- What assets we need to protect
- What are the vulnerabilities of these assets
- What can go wrong with these assets
- How can someone disrupt our operations
- Which are the most complex activities
- What is our greatest legal, financial and operational exposure

Two primary questions for evaluating the risk inherent in a business function are:
1. What is the probability that things can go wrong?
2. What is the cost/loss if that thing goes wrong?

**Risk assessment:**

i) **Prioritization**

ii) **Identifying critical applications**

iii) **Assessing the impact**
   - Legal consequences
   - Impact on customer services
   - Direct loss
   - Opportunity loss
   - Likelihood of fraud

iv) **Identification of exposures and implications** (Risk = Probability x Exposure)

v) **Determining recovery time**

vi) **Assess insurance coverage**
   - All hardware and equipments and infrastructure
   - Software reconstruction cost
   - Extra expenses incurred till restoration of normal activities
   - Business interruption i.e. loss of profit
   - Valuable papers and records
   - Loss due to errors and omissions
   - Fidelity coverage for illegal acts of employees
   - Loss of back-up media

vii) **Development of recovery plan**

**Risk evaluation:**
The purpose of risk evaluation is to:
- Identify the probability
- Calculate the exposure
- Make control recommendations
Following five techniques are used for risk evaluation:

i) Judgment and intuition
ii) Delphi technique
iii) Scoring technique
iv) Quantitative techniques
v) Qualitative techniques

**Risk ranking:**

Weighted risk factor = Wt 1 X Wt 2

(Wt 1 = Probability of occurrence
Wt 2 = Impact / Exposure)

Considerations in risk ranking:

i) Past frequency of threat
ii) Degree of predictability
iii) Speed of disaster
iv) Duration of disaster
v) Find out the impact of disaster on
   - Critical records
   - Persons
   - Operating capability
   - Assets
   - Other infrastructure
vi) Determine the level of back-up facilities
vii) Estimate potential loss including:
   - Increased operating cost
   - Opportunity loss
   - Loss of assets
   - Loss of income
   - Loss of goodwill
   - Legal consequences
   - Loss of competitive edge
viii) Estimating potential losses to each business function separately
ix) Determine the cost of contingency planning.

**Risk mitigation:** Risk mitigation means systematic reduction of risk to an acceptable level

Risk mitigation measures are:

o Self assessment of risk.
o Creating environment which supports risk mitigation.
o Strengthening internal controls.
o Financial strength in the form of reserves.
o Establishing business continuity plan and disaster recovery plan (BCP/DRP).
o Creating a separate risk management department.
o Proper insurance.
o Outsourcing of services.

Common risk mitigation techniques are:

i) Insurance:
ii) Outsourcing:
iii) Service level agreements:

**Balancing Risk and controls:**

<table>
<thead>
<tr>
<th>Excessive risk results in:</th>
<th>Excessive controls results in:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Loss of assets</td>
<td>- Increased bureaucracy</td>
</tr>
<tr>
<td>- Poor business decisions</td>
<td>- Reduced productivity</td>
</tr>
<tr>
<td>- Non-compliance</td>
<td>- Reduced efficiency</td>
</tr>
<tr>
<td>- Increased frauds</td>
<td>- Increased complexity</td>
</tr>
<tr>
<td>- Instability</td>
<td>- Increase in cost</td>
</tr>
</tbody>
</table>
CHAPTER 6 – Quick Revision Points (QRP)

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

Business continuity planning:

Definition: BCP is the activity which involves designing and implementing plans that protect against business disruption in case of crises and disasters.

Business continuity planning covers the following areas:

I. Business resumption planning
II. Disaster recovery planning
III. Crises management

Business continuity planning life cycle:

Objectives and goals of business continuity planning:
1. Safety to employees
2. Identify critical business functions
3. Identification of weaknesses in the system
4. Resume critical business operations
5. Minimize duration of disruption
6. Implementing disaster preventive program
7. Minimize losses
8. Establish key roles
9. Simplify recovery activities
10. Facilitate coordination

Developing a business continuity plan:

Generally BCP consist of eight phases which are as follows:
1. Pre-planning activities
2. Vulnerability assessment
3. Business impact analysis
4. Requirement definitions
5. Plan development
6. Plan testing
7. Plan implementation
8. Plan maintenance
1. Pre-planning activities
   - Understanding the present and projected system
   - Scope of BCP
   - Policy to support BCP
   - Steering committee
   - Business continuity manager
   - BCP awareness

2. Vulnerability assessment
   - Identify critical processes
   - Identifying threats and vulnerabilities
   - Evaluate the existing controls
   - Evaluate any existing emergency plans
   - Report to steering committee

3. Business impact analysis (BIA): assess the degree of potential loss
   - Estimate the impact of threat and disaster
   - Tangible exposure
   - Intangible exposure
   - Interdependent processes
   - Maximum allowable downtime
   - Report to steering committee
   Methodology used for doing business impact analysis:
   i) Questionnaires
   ii) Workshop
   iii) Interviews
   iv) Examination of documents

4. Requirement definitions
   - Recovery alternatives
   - Resources required
   - Scope, objectives and assumptions

5. Plan development
   - Overall recovery strategies
   - Business recovery strategies
   - Technical recovery strategies
   - Document the plan
   - Changes in procedures
   - Roles and duties
   - Changes in vendor contracts

6. Plan testing
   - Recovery procedures are complete and workable
   - Staff is trained
   - Resources are adequate
   - Manual procedures are also workable

7. Plan implementation
   - Implementing individual components of the plan
   - Assigning job roles and duties
   - Providing emergency guideline
   - Scheduling test activities

8. Plan maintenance
   - Ownership
   - Maintenance and Monitoring
   - Change management procedures and version control
■ Types of BCP/DRP plan:

I. **Emergency plan**
   1. Who is to be notified immediately (management, police, fire department, hospital)
   2. Action to be taken (shutdown of equipment, termination of power, removing files)
   3. Evacuation procedure
   4. Return and restart conditions and procedures

II. **Back-up plan**
   1. Personnel
   2. Hardware
   3. Data/information
   4. Documentation
   5. Facilities
   6. Application and system software
   7. Supplies

III. **Recovery plan**
   1. Creation of a recovery committee
   2. Assigning roles and responsibilities
   3. Recovery guideline
   4. Deciding the priority
   5. Appointing member
   6. Periodic review

IV. **Test plan**
   1. Paper walkthrough
   2. Specific component
   3. Full simulation
   4. Acid test

■ Threats and risk management:

1. **Lack of integrity**: (unauthorized changes in the information). Controls:
   - Security policies, procedures and standards
   - Encryption
   - Data validation
   - Logical access controls
   - Physical access controls
   - Security awareness
   - Training
   - Audit logs
   - Antivirus software

2. **Lack of confidentiality**: (unauthorized disclosure). Controls:
   - Security policy, procedures and standards
   - Encryption
   - Employees awareness
   - Training program
   - Non-disclosure agreements
   - Password
   - Secure storage of data

3. **Lack of availability**: (system is not available on timely basis). Controls:
   - Software configuration controls
   - Fault tolerant system
   - Backup
   - Incident logging
   - Backup power supply
4. Unauthorized access: (unauthorized users gain access into the system). Control:
   - Boundary control
   - Passwords
   - Biometrics
   - smart cards
   - Firewall and intrusion detection system
   - Encryption

5. Hostile software: (malicious codes like virus, Trojans and worms). Controls:
   - Anti-virus
   - Anti-spyware
   - Firewall
   - Checksums

6. Disgruntled employees: (frustrated, unhappy and dissatisfied employees). Controls:
   - Physical and logical access controls
   - Training
   - Security awareness
   - Motivation
   - Job enrichment and job rotation

7. Hackers and computer crimes: Control:
   - Firewall and intrusion detection system
   - Passwords
   - Encryption
   - Logging

8. Terrorism and industrial espionage: (spying). Controls:
   - Encryption
   - Traffic padding and flooding
   - Intrusion detection system

■ Single point failure analysis (Technology risk assessment):
   - Locate single point of failure
   - Single point failure is any single factor which can cause an entire system to fail
   - Controls for single point of failures
     - Resilient technology
     - back-up arrangements

Benefits of technological risk assessment:
   i) Identify, quantify and manage risk
   ii) Future improvement
   iii) Framework to select correct technology
   iv) Reduction of risk
   v) Single point of failure are not built in the overall systems architecture

■ Software and data back-up techniques:

   I. Full back-up
   II. Differential back-up
   III. Incremental back-up
   IV. Mirror back-up

■ Alternate processing facility arrangement: (Off-site)

   1. Cold site (Ready within 2 to 8 days)
   2. Hot site (Ready within 2 Hrs to 24 Hrs)
   3. Warm site (Ready within 1 to 2 days)
   4. Reciprocal arrangement
Important considerations while using third party location as off-site:
- Facilities available at the site.
- How soon the site will be made available after the disaster occurs.
- Number of organizations that will be using the site concurrently.
- Period during which the site will be available.
- Conditions in which the site can be used.
- Security measures and controls available at the site.

**Back-up redundancy:**

Back-up redundancy means that back-up should be done in more than one way

**Following points should be taken care of while doing back-up:**
1) Multiple back-up media
2) Off-site back-up
3) Where to keep the back-up
4) Media rotation

**Type of back-up media:**
1) Floppy disk
2) Compact disk (CD)
3) Tap drives
4) Hard disk drive (HDD)
5) Removable disk
6) DAT (Digital Audio Tape) drives
7) Optical jukebox
8) Autoloader system
9) USB flash drive
10) Zip drive
11) DVD
12) Blu-ray disk

**How to select back-up media:** Following factors can be considered while considering
1) Speed.
2) Reliability
3) Capacity
4) Extensibility
5) Cost

**Back-up tips:**
1) Simple and easy to understand back-up plan.
2) Step by step guideline
3) Record of back-up media.
4) Labels on back-up media.
5) Software utilities for automatic back-up
6) Verify back-up files
7) Right of restoration to administrator
8) Multiple back-up media.
9) Off-site backup
10) Keep back-up media in fire proof vaults

**Disaster recovery procedural plan:**

**Disaster:** The term disaster can be defined as an incident which exposes business operations and human life to risk. It could be due to human causes (i.e. sabotage) or natural causes.
Disaster recovery procedural plan (DRP manual): Step by step guideline for disaster recovery

1) Conditions for activating the DRP process.
2) Emergency procedures to be taken at the time of disaster.
3) Evacuation procedure
4) Fallback procedure
5) Resumption procedure
6) Procedures for testing and updation of DRP
7) DRP awareness and education programs for employees
8) Assigning roles and responsibility for DRP activities to individuals
9) Location of DRP manual and its distribution list
10) Emergency contact numbers of employees
11) Emergency contact numbers of police / fire / medical emergency department
12) Emergency contact numbers of vendors
13) Medical procedure
14) Back-up location agreement
15) Insurance papers and claim forms

Insurance:

Insurance is a mechanism of risk sharing. Following losses can be generally covered in an insurance policy:
  1) Equipment
  2) Facilities
  3) Storage media
  4) Business interruption
  5) Extra expenses
  6) Valuable papers
  7) Accounts receivable
  8) Third party losses

Kinds/Types of insurance:

![Diagram of Types of Insurance]

Testing methodology and checklist:

Following are the components of DRP testing:
(i) Hypothetical testing
(ii) Component testing
(iii) Module testing
(iv) Full testing

Steps in testing:
  1) Setting objectives
  2) Defining the boundaries
  3) Scenarios
  4) Test criteria
  5) Assumptions
  6) Test prerequisites
7) Briefing sessions
   Briefing should be done on following issues:
   - Nature of test
   - Disaster scenario
   - Time and location
   - Prerequisites
   - Assumptions
   - Restrictions

8) Checklists

9) Analyzing the test

10) Debriefing sessions
   Debriefing should be done on following issues:
   - Overall performance
   - Specific team performance
   - Observations
   - Areas of concern
   - Planning for next test
   - Test reports
   - Test logs

11) Test report

- **Audit tools and techniques:**
  1) Automated tools
  2) Internal control auditing
  3) Disaster and security checklist
  4) Penetration testing

- **Audit of the disaster recovery/business plan:** following issues are covered:
  
  1) **Audit of BCP/DRP development phase:**
     - well documented
     - Steps taken
     - Business impact analysis
     - Level of participation
     - Validity of assumptions
  
  2) **Audit of backup and recovery procedure:**
     - Procedures are sufficient
     - Resources available
     - Backup arrangements
     - Data backup
     - Alternate processing arrangements.
     - Check the network and telecommunication backup lines.
     - Review the locations where BCP/DRP manual is kept.

  3) **Audit of test plan:**
     - Review the test plan.
     - Check the extent to which BCP/DRP has been tested.
     - Check the test logs.
     - Review the BCP/DRP test report

  4) **Audit of administrative procedures:**
     - Review the team composition of BCP/DRP function.
     - Review the training mechanism for team members.
     - Is there a designated emergency operation center where the incident can be reported.
     - Review the emergency contact person list and their roles and responsibilities.
CHAPTER 7 – QRP (Quick Revision Points)

AN OVERVIEW OF ENTERPRISE RESOURCE PLANNING

» ERP – Definition:

- Enterprise resource planning (ERP) is an integrated computer-based system used to manage internal and external resources including assets, financial resources, materials, and human resources.

The Components of an ERP System:

Evolution of ERP:

<table>
<thead>
<tr>
<th>Timeline</th>
<th>System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1960s</td>
<td>Inventory Mgt &amp; Control</td>
<td>Inventory management</td>
</tr>
<tr>
<td>1970s</td>
<td>Material Requirement Planning (MRP)</td>
<td>Inventory management + Production requirement</td>
</tr>
<tr>
<td>1980s</td>
<td>Manufacturing Requirements Planning (MRP II)</td>
<td>Inventory management + Production requirement + Final product distribution</td>
</tr>
<tr>
<td>1990s</td>
<td>Enterprise Resource Planning (ERP)</td>
<td>multi-module integrating all departments</td>
</tr>
</tbody>
</table>
Enabling technologies:

ERP system is based on three-tier client-server architecture:
I. **Client** – i.e. the user interface tier
II. **Application server** – i.e. the business logic tier
III. **Database** – i.e. the data storing tier

![Three-tier client-server architecture diagram]

ERP characteristics:
1) Flexibility
2) Modular & open
3) Comprehensive
4) Beyond the company
5) Best business practices

Features of ERP:
1) Supports both strategic and functional planning
2) Supports multi-currency accounting
3) Supports end-to-end supply chain management.
4) Integrates all functional areas
5) Integrate companies under the same management
6) Increases customer service and support
7) Reduces information gap
8) Supports new technologies
9) Supports tools like DSS and EIS

Why companies undertake ERP:
1) Integrated Financial Information
2) Integrated supply Chain Information
3) Standardize and speed up manufacturing operation
4) Reduce Inventory
5) Standardize HR Information

Benefits of ERP:
1) Facilitates day-to-day management
2) Improves productivity
3) Reduce inventory levels
4) Improves financial controls
5) Reduce operating costs
6) Supports strategic planning
7) Fast generation of reports
8) More accuracy in reports
9) Less requirement of workforce
10) Faster tracking of customer orders
11) Suitable for global operations
12) Helps in complying with requirements such as IFRS, Sarbanes-Oxley, or Basel II.
Business process reengineering (BPR):
- BPR is fundamental rethinking and radical redesign of business processes
- BPR improves
  o Cost
  o Quality
  o Service
  o Speed
- Information technology plays an important role in BPR concept:
  o Enables Product & Service Innovations
  o Improve Operational Efficiency
  o Coordinate Vendors & Customers in the Process Chain
- BPR is one of the fundamental steps undertaken prior to ERP implementation

Business engineering:
When BPR and information technology are combined together then it is called business engineering.

Business engineering is the rethinking of Business Processes to improve speed, quality and output of materials or services.
Efficient redesigning of company's value added chains

Business modeling:
- Use of quantitative and computer methods for planning the business process
- Use of advanced computing technology to model, analyses and simulate various business process has made a significant impact in the business.

Business model:
- Business model is a diagrammatical representation of business
- Use of tables and flowchart

ERP Implementation:

Key planning and implementation decisions:
Before taking up the ERP implementation task, the organization has to decide on various issues:
1) ERP or no ERP
2) Follow software's processes or customize
3) In-house or outsource
4) Big-bang or phased implementation

ERP implementation methodology: steps in implementing ERP are as follows:
1) Identifying the needs:
   - What user wants
   - Will ERP improve efficiency, reduce cost
2) Evaluating the present processes:
   - Time taken by particular process
   - Number of departments/processes
   - Flow of information
   - Reporting points
3) Deciding the desired situation:
   - Set the goals for ERP
   - Benchmarks are set for quality, cost, service, customer satisfaction, delivery time
4) Business process reengineering:
   - BPR is done to make the structural changes in the process

5) Evaluation of various ERP packages:
   Various ERP packages are evaluated as per the following criteria:
   - Flexibility
   - Comprehensiveness
   - Integrated
   - Beyond the company
   - Best business practices
   - New technology
   - Price of package and implementation
   - Ease of implementation

6) Finalization of ERP package:

7) Finalization of implementation consultant: Criteria:
   - Skill set
   - Industry specific experience
   - Cost of hiring

8) Installation of hardware and network:

9) Implementation of ERP package: Step involves:
   - Formulation of team
   - Preparation of plan
   - Mapping of business processes to package
   - Gap analysis
   - Customization
   - Test run
   - Data migration
   - User documentation
   - Post-implementation support
   - Monitoring

**Guidelines for successful ERP implementation:**
1) Understanding the business needs
2) Doing BPR
3) Establishing a good communication network
4) Motivating employees
5) Creating a balanced team
6) Training end users

**Post implementation:**

Some post implementation problems in ERP relate to wrong expectations and fears about ERP which people have in their mind.

Some of the popular expectations are:
- Improvement in processes
- Increased productivity
- Total automation
- Improvement of all key performance indicators
- Real time information is available to all people
- Total integration of all operations

Some fears that relate to ERP are:
- Loss of job or change in job profile
- Increased stress due to greater transparency
- Individual fear of loss of authority
- Difficulty to implement proper controls
Risk and governance issue in an ERP: Increase in business risk

1) Single point of failure
2) Structural changes
3) Job role changes
4) Online, real-time
5) Change management
6) Distributed computing experience
7) Broad system access
8) Dependency on external assistance
9) Program interface and data conversion:
10) Audit expertise
11) Single sign-on
12) Data content quality
13) Privacy and confidentiality

Why do ERP projects fail?

1) Lack of education in end-users
2) Lack of top management commitment
3) Inadequate requirements definition
4) Poor ERP package Selection
5) Inadequate resources
6) Internal resistance by users
7) A Poor fit between the software and users procedures
8) Unrealistic expectations of the benefits and the ROI
9) Inadequate training
10) Unrealistic time frame expectations

How does ERP fit with e-commerce?

- Earlier ERP it was confined to internal users only
- As the interconnectivity increased ERP was extended to external users also
- Uses e-commerce channel to link customers, vendors etc.
- ERP vendors developed simple web-applications for e-commerce
- Used for transactions like order booking, order tracking, making payments etc.

Life after implementation:

- Implementation methodology should be good
- User training and awareness
- Make a list of critical success factors (CSF) and their corresponding key performance indicators (KPI)
- KPI measures the performance of CSF
- CSF are those factors the success of the organization depends, example can be:
  - Product delivery time
  - Service delivery time
  - Transaction processing time
  - Quality of product
  - Energy efficient products
  - Low product cost
- ERP helps an organization to work towards improving their KPI for various CSF.

Some specific tasks to be done after implementing ERP are:

1) Develop new job description and organizational structure to suite the new ERP system
2) Determine the skill gap between the existing jobs and the new jobs
3) Assess training requirement and conduct such training
4) Develop new HR, finance and operations policies as required by the ERP.
Post implementation problems in ERP which needs some correction:

1) Ever changing business environment requires reconfiguration in ERP
2) Change in business process requires change in ERP configuration.
3) Change in technology requires change in ERP infrastructure.
4) New additions to business may require extra functionality in ERP

Sample list of ERP vendors:

1) Baan Corporation – Baan:
   • Used by major aircraft company ‘Boeing’.
   • Suitable for all manufacturing companies.
   • Broad functional scope.
   • Tools for business process analysis.
2) Business Planning and Control System (BPCS):
   • Developed by SSA Global Technologies
   • Targets manufacturing companies
   • Good for Kanban (JIT) Manufacturing
   • Problem of slow development schedule
3) Marcam Corporation – Mapics XA:
   • 40 modules with good functionality
   • Robust and easy to implement
   • Value for money
4) MFG Pro (QAD):
   • Originally designed for MRP II
   • Reliable manufacturing functionality
   • Simple implementation
5) Oracle Applications (Oracle Corporation):
   • Internet-enabled computing
   • One-stop-shop, i.e. it offers database, tools, applications and implementation
   • Can run on wide range of hardware
6) Marcam Corporation – Prism:
   • Specialist ERP for process manufacturing solutions
   • Operates on IBM AS/400 platform
   • Outdated now
7) R/3 SAP:
   • Market leader
   • Matching business process to Modules
   • Offers wide range of functions
   • It is complex
8) System 21 (JBA):
   • Less expensive
   • Does not offers leading-edge technology
   • Reliable for manufacturing solution
ERP software package – SAP:

- SAP stands for – Systems Applications and Products
- Developed by – SAP AG Germany.
- Provides support for more than 25 industries with industry-specific features.

<table>
<thead>
<tr>
<th>SAP R/3 (12 Major modules)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Finance (Financial Accounting)</td>
</tr>
<tr>
<td>2) Controlling</td>
</tr>
<tr>
<td>3) Investment Management</td>
</tr>
<tr>
<td>4) Treasury</td>
</tr>
<tr>
<td>5) Enterprise Controlling</td>
</tr>
<tr>
<td>6) Product Data Management (PDM)</td>
</tr>
<tr>
<td>7) Sales and Distribution</td>
</tr>
<tr>
<td>8) Production Planning</td>
</tr>
<tr>
<td>9) Material Management</td>
</tr>
<tr>
<td>10) Human Resource Management</td>
</tr>
<tr>
<td>11) Payroll Accounting</td>
</tr>
<tr>
<td>12) Internet and Intranet</td>
</tr>
</tbody>
</table>

1) Finance (Financial Accounting)
   - General Ledger
   - Accounts Receivable
   - Accounts Payable
   - Fixed Assets Accounting

2) Controlling
   - Overhead Cost Control
   - Cost Centre Accounting
   - Activity Based Costing
   - Product Cost Control
   - Cost Object Controlling
   - Profitability Analysis

3) Investment Management
   - Corporate wide budgeting
   - Appropriation requests
   - Automatic settlement to fixed assets
   - Depreciation forecast

4) Treasury
   - Cash Management
   - Market Risk Management
   - Funds Management

5) Enterprise Controlling (Holding Subsidiary Accounting)
   - EC-CS (Consolidations)
   - EC-PCA (Profit Center Accounting)
   - EC-EIS (Executive Information System)

6) Product Data Management (PDM)
   - Primarily used by engineers
   - Keeps track of all master data related to a product
   - Supports Document Management System
   - Quickly gives product structure information
   - BOM (Bill of Material) Management

7) Sales and Distribution
   - Shipping Management System (Picking, Packing, Loading and Delivery)
   - Transport Module
   - Foreign Trade Processing
   - Billing
   - Sales Information System
8) Production Planning
   - Sales and Operations Planning
   - Production Control Module
   - Quality Management
   - Project System
   - Project Information System

9) Material Management
   - Purchasing
   - Inventory Management
   - Warehouse Management
   - Invoice Verification
   - Inventory Control using Purchase Information System
   - Quality Management
   - Plant Maintenance
   - Service Management

10) Human Resource Management
    - Personnel Administration
    - Employee master data
    - Recruitment management
    - Selection and hiring
    - Travel management
    - Benefits administration
    - Personnel cost planning

11) Payroll Accounting
    - Payroll processing
    - Integration
    - Global solutions
    - Time management
    - Time management review
    - Shift planning
    - Qualification matching with available positions
    - Training

12) Internet and Intranet
    - This allows SAP to be accessed over internet

Best Wishes
CHAPTER 8 – QRP (Quick Revision Points)

INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

■ ISO 27001 – Information Security Management Standard:

<table>
<thead>
<tr>
<th>Information Security Management System (ISMS) – Three Steps</th>
<th>Ten areas of focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i) Establishing Management Framework</td>
<td>1. Security policy</td>
</tr>
<tr>
<td>- Information security policy</td>
<td>2. Organizational security</td>
</tr>
<tr>
<td>- Scope of ISMS</td>
<td>3. Asset classification and control</td>
</tr>
<tr>
<td>- Risk assessment</td>
<td>4. Personnel security</td>
</tr>
<tr>
<td>- Identify areas of risk and degree of assurance required</td>
<td>5. Physical and environmental security</td>
</tr>
<tr>
<td>- Select appropriate controls</td>
<td>6. Communications and operations management</td>
</tr>
<tr>
<td>- Statement of Applicability (SoA)</td>
<td>7. Access control</td>
</tr>
<tr>
<td>(ii) Implementation</td>
<td>8. Systems development and maintenance</td>
</tr>
<tr>
<td>(iii) Documentation</td>
<td>9. Business continuity management</td>
</tr>
<tr>
<td>- Document control</td>
<td>10. Compliance</td>
</tr>
<tr>
<td>- Record control</td>
<td></td>
</tr>
</tbody>
</table>

■ CMM – Capability Maturity Model:

- Developed by software engineering institute (SEI) of US.
- Fundamental concepts underlying process maturity:
  - Software process: Activities, methods and practices to develop software
  - Software process capabilities: Expected results
  - Software process performance: Actual results
  - Software process maturity: Clearly defined, managed and controlled process

Level 1 – Initial: Processes are adhoc, localized, disorganized
Level 2 – Repeatable: Stable environment, project management techniques, tracking of cost and schedule
Level 3 – Defined: Documented process, training, tracking of cost schedule and quality
Level 4 – Managed: Quantitative goals, measured, reduction in variations, predict trends
Level 5 – Optimizing: Continuous improvement, innovations, removal of inefficiencies
COBIT – Control Objectives for information and related technology

- Developed by “Information System Audit and Control Association” (ISACA).
- Used by managers, auditors, and IT users

Three dimensions (vantage point) of COBIT are depicted in the figure below:

**Executive Summary:** Summary of COBIT for senior executives.
**Framework:** Structure of COBIT
**Control Objectives:** 210 specific control objectives for 34 IT processes.
**Management Guidelines:** Maturity models to measure key performance indicators (KPI’s)
**IT Assurance Guide:** How auditors should evaluate the controls

**COBIT Structure:**
- Current version: COBIT 4.1
- Domains: 4
- Process covered: 34
- Control Objectives: 210

Four domains of COBIT are:
1. Planning and organization (PO) – Covers 10 process.
2. Acquisition and implementation (AI) – Covers 7 process.
3. Delivery and support (DS) – Covers 13 process.
4. Monitoring and evaluation (ME) – Covers 4 process.

I. Planning and organization (PO): Planning and organization IT infrastructure
   - PO1 - Define a Strategic IT Plan
   - PO2 - Define the Information Architecture
   - PO3 - Determine Technological Direction
   - PO4 - Define the IT Processes, Organization and Relationships
   - PO5 - Manage the IT Investment
   - PO6 - Communicate Management Aims and Direction
   - PO7 - Manage IT Human Resources
   - PO8 - Manage Quality
   - PO9 - Assess and Manage IT Risks
   - PO10 - Manage Projects
II. Acquisition and implementation (AI): Acquire and Implement IT infrastructure
   - AI1 - Identify Automated Solutions
   - AI2 - Acquire and Maintain Application Software
   - AI3 - Acquire and Maintain Technology Infrastructure
   - AI4 - Enable Operation and Use
   - AI5 - Procure IT Resources
   - AI6 - Manage Changes
   - AI7 - Install and Accredit Solutions and Changes

III. Delivery and support (DS): IT service deliver and support
   - DS1 - Define and Manage Service Levels
   - DS2 - Manage Third-party Services
   - DS3 - Manage Performance and Capacity
   - DS4 - Ensure Continuous Service
   - DS5 - Ensure Systems Security
   - DS6 - Identify and Allocate Costs
   - DS7 - Educate and Train Users
   - DS8 - Manage Service Desk and Incidents
   - DS9 - Manage the Configuration
   - DS10 - Manage Problems
   - DS11 - Manage Data
   - DS12 - Manage the Physical Environment
   - DS13 - Manage Operations

IV. Monitoring and evaluation (ME): Monitoring and Evaluation of IT
   - ME1 - Monitor and Evaluate IT Performance
   - ME2 - Monitor and Evaluate Internal Control
   - ME3 - Ensure Regulatory Compliance
   - ME4 - Provide IT Governance

COBIT and other standards:

- **COBIT Val IT and Risk IT:**
  - COBIT – IT Controls
  - Val IT – Value for IT
  - Risk IT – Manage IT related risks

- **COBIT and ISO 27002:**
  - ISO 27002 – Information security (Specific and detailed)
  - COBIT – IT controls (Wider but not detailed)

- **COBIT and Sarbanes Oxley:**
  - Sarbanes-Oxley Act 2002 – US act applicable on companies listed in US and requires some disclosures and compliance
  - These disclosures and compliance can be fulfilled by adopting COBIT or COSO
  - Securities Exchange Commission (SEC) of US recommends COSO

- **COBIT and COSO:**
  - COSO – financial controls (used by management at large)
  - COBIT – IT controls (used by IT management)
  - COSO is the official framework

- **COCO – Guidance on controls**
  - General controls
  - Issued by The Canadian Institute of Chartered Accountants
  - CoCo is a superset of COSO (wider than COSO)
  - Four elements of internal control: Purpose, Capabilities, Commitment and Monitoring
ITIL (Information Technology Infrastructure library):

- Best practices in IT service management
- Developed by United Kingdom’s Office of Government Commerce (OGC)
- ITIL Version 2 – 8 books

1. Service Support: (Day to day issues)
   (i) Service desk
   (ii) Incident management
   (iii) Problem management
   (iv) Configuration management: Five basic activities in configuration management are
       ▪ Planning
       ▪ Identification
       ▪ Control
       ▪ Status accounting
       ▪ Verification and audit
   (v) Change management
   (vi) Release management

2. Service Delivery: (Long term issues)
   (i) Service Level Management
   (ii) Financial Management for IT Services
   (iii) IT Service Continuity Management
   (iv) Availability Management
   (v) Contingency Planning
   (vi) Capacity Management

3. ICT Infrastructure Management

4. Security Management

5. The Business Perspective

6. Application Management

7. Software Asset Management

8. Planning to Implement Service Management

Systrust and Webtrust:

- Attestation services developed jointly by American Institute of Certified Public Accountant (AICPA) and the Canadian Institute of Chartered Accountants (CICA).
- Provide assurance to the third parties
- Issued by CPAs and Chartered Accountants
- Systrust – for any business system
- Webtrust – for e-commerce system.

Control criteria of trust services:
1. Security
2. Online privacy
3. Availability
4. Confidentiality
5. Processing integrity

Each of the above control criteria is examined under four areas:

a) Policies
b) Communications
c) Procedures
d) Monitoring
HIPAA – Health Insurance Portability and Accountability Act

- Enacted by the U.S. Congress in 1996
- Title I – Health insurance coverage for workers and their families when they change or lose their jobs.
- Title II – Administrative Simplification (AS) provisions, national standards for electronic health care transactions

HIPAA Security rules: The three types of security safeguards are:

a) Administrative Safeguards: Policies and procedures to comply with the act
   - Documented privacy policy
   - Privacy officer
   - Authorization procedure for PHI
   - Training for PHI
   - Vendor also have to comply with HIPAA
   - Contingency plan
   - Internal audit

b) Physical Safeguards: Controlling unauthorized access
   - Physical protection
   - Control over introduction and removal of hardware and software.
   - Securing workstations
   - Training
   - Visitor sign-in and Escorts
   - Control over contactors/agents entry

c) Technical Safeguards: Controlling transmission of PHI
   - Documentation control
   - Access control
   - Authorization control
   - Protecting data integrity
   - Protection from intrusion
   - Data encryption
   - Risk analysis

SAS 70: Audit of Service Organisation

- Issued by American Institute of Certified Public Accountants (AICPA).
- Service organization’s in-depth audit of controls.
- SAS 70 reports issued by service auditor for the benefit of
  - Service organization
  - User organization
  - User auditor
- There are two types of SAS 70 reports:
  - **Type I** – Summary report, description of controls at a specific point in time
  - **Type II** – Detailed report, description of controls and also detailed testing of controls over a minimum six month period

Benefits to the Service Organization:
- Effectiveness of controls
- Build trust
- User organization’s is not required to send auditor
- Satisfy the user auditor's requirements.
- Improvements in many operational areas.

Benefits to the User Organization:
- Rely on the effectiveness of service organization controls
- Saves cost of sending own auditor
CHAPTER 9 – Quick Revision Points (QRP)

DRAFTING OF I.S. SECURITY POLICY, AUDIT POLICY,
I.S. AUDIT REPORTING – A PRACTICAL PERSPECTIVE

Why is information system security important:

There is a gap between the “required degree of protection” and the “actual degree of protection applied” to the information system. This gap is caused due to the following factors:

- Widespread use of technology
- Interconnectivity of systems
- Elimination of distance, time and space as constraints
- Unevenness of technological changes
- Decentralization of management control
- New trend towards electronic attacks
- Week legal and regulatory requirement

Threats to information systems may arise from:

- Technical reasons: Program errors, bugs and crashes etc
- Natural disasters: Floods, earthquake, thunderbolts etc.
- Environmental conditions: Power failure, brown-out, surge, pests etc
- Human factors: Negligence, lack of awareness, lack of training etc.
- Unauthorized access: Hacking, intrusion, virus, Trojan horse, worms etc.
- Business dependencies: Loss of management control over outsourced activities.

What is information system security?

- Information systems security relates to the protection of valuable information systems assets against loss, disclosure, or damage.
- Security includes both physical security like doors, locks, fences, insurance etc and logical security like user ID, password, firewalls etc.

Security objective:

The objective of information systems security is to protect the interest of the user of information systems who use the information generated by the information system in some or the other form. This objective is met when following three criteria’s relating to information are met:

1. Confidentiality
2. Integrity
3. Availability

What information is sensitive?

In any organization following types of information is generally sensitive information which needs to be protected carefully:

- Strategic plans
- Business operations
- Finances

Establishing better information protection:

Following points needs to be considered before designing information protection mechanism:

(a) Not all data has the same value (i.e. classify it)
(b) Know where the critical data resides
(c) Develop an access control methodology
(d) Protect information stored on media
(e) Review hardcopy output
Protecting computer-held information system:

Basic rules for information protection:
Rule 1: Scope - what the information systems are and where these are located.
Rule 2: Classification - value of the information
Rule 3: Authorization - who is authorized to access the information
Rule 4: Availability - how quickly information should be made available

Two types of information protection that an organization can use:

Information protection

I. Preventive information protection
   - Physical control
   - Logical control
   - Administrative controls

II. Restorative information protection
   - Backup and recovery procedures

Information security policy:

An information security policy is a set of laws, rules and practices that regulates how assets including sensitive information are managed, protected and distributed within the organization.

Issues to be addressed in information policy:
- Definition of information security
- Why information security is important to the organization
- Goals and principles of information security
- Brief description of various information security standards
- Defining all relevant information security responsibilities
- Reference to any supporting document or standard

Auditor’s role regarding information security policy:
- Policy is readily accessible to all employees
- Employees are aware and understand its contents.
- Employees sign the declaration
- Policy has an owner

Members of security policy:
- Management experts: economic feasibility
- Technical experts: technical feasibility
- Legal experts: legal feasibility

Types of information security policies and their hierarchy:
1) **Information security policy**: It is a wide policy covering all broader aspects of information security in an organization. This policy provides a definition of information security, its overall objectives and its importance to all the users.

2) **User security policy**: This policy sets out the responsibilities and requirements for all IT systems users. It provides security terms of reference for users, line managers and systems owners which they should follow in their day-to-day working.

3) **Acceptable usage policy**: This policy defines rules for the use of email and internet services by the employees. (e.g. games/songs should not be downloaded)

4) **Organizational information security policy**: This policy consists of group of policies for the security of information assets and information systems in the whole organization. It is the main IT security policy covering all aspects of information security.

5) **Network and systems security policy**: This policy defines the rules for network and data communication and related security issues. It covers security over firewalls, IDS, VPN, VoIP, routers, switches, LAN/WAN links, etc.

6) **Information classification policy**: This policy defines the rules for classification of information. For example, information can be classified as confidential, proprietary, etc.

7) **Conditions of connections**: This policy defines the rules and terms & conditions for giving access to outside entities like vendors and distributors into the organization's network.

**Components/contents of security policy**: A good security policy usually contains/COVERS:

(i) Purpose and scope of the policy and its audience.
(ii) Security organization structure.
(iii) Classification and inventory of information assets.
(iv) Systems development and maintenance controls.
(v) IT operations and communication management.
(vi) Identity management and access control.
(vii) Physical and environmental security.
(viii) Incident reporting mechanism.
(ix) Business continuity planning.
(x) Legal compliance.
(xi) Monitoring and auditing requirement.

1. **Purpose and scope**:
   Purpose defines what the organization is trying to achieve through the policy, and scope defines its applicability and audience.

2. **Security organization structure**:
   The organizational structure of IT department should be defined and accordingly their responsibilities and line of reporting should be defined. Following team/group is generally found in IT department:

   a) Group security officer (GSO)
   b) Assistant group security officer (AGSO)
   c) Information security forum (ISF)

   ![Diagram of Information Security Forum](image)

   d) Information security management group (ISGM)
e) IT management
f) IT security officer (ITSO)
g) Installation security officer (ISO)
h) Personnel security officer (PSO)
i) Facilities management security officer (FMSO)
j) Divisional system security officer (DSSO)
k) Systems security officer (SSO)
l) Systems owners
m) Line managers
n) Users

3. **Responsibility allocation:**
   (i) Owner should be appointed for each information asset.
   (ii) Staff awareness
   (iii) Approval of new network links
   (iv) Contact list of vendors/external agencies
   (v) Risk assessments for all third party access
   (vi) Limited and controlled access by third parties
   (vii) Security over outsourcing contracts

4. **Asset classification and security classification:**
   (i) H/W and S/W inventory
   (ii) Information Classification Policy
   (iii) The originator or ‘owner’ of information should provide a security classification
   (iv) Handling of information in secure manner
   (v) Exchanges of data and software between organizations must be controlled
   (vi) Classified waste must be disposed of securely

5. **Logical access control:**
   (i) Access controls must be in place to prevent unauthorized access
   (ii) Access must be given as per the business requirement
   (iii) System Owners are responsible for approving access
   (iv) Actual access controls in place must be audited on a regular basis
   (v) Registration and de-registration should be approved
   (vi) Deletion of user ID for individuals who leave the jobs
   (vii) Each individual should be provided with a unique user id
   (viii) Sharing of user ID should not be permitted
   (ix) PCs and terminals should never be left unattended
   (x) Passwords Policy should be defined
   (xi) Passwords must be kept confidential and never disclosed to others
   (xii) Secure Mobile computing
6. **Incident handling:**
   (i) Defined method of Security incident reporting
   (ii) Incidents are recorded
   (iii) Recurrence is analyzed to identify trends
   (iv) Staff awareness

7. **Physical and environmental security:**
   (i) Identify all vulnerable areas within each site.
   (ii) IT infrastructure must be physically protected.
   (iii) Access to secure areas must remain limited to authorized staff only
   (iv) Valuable assets must be securely locked
   (v) Computers must never be left unattended while logged on
   (vi) Supplies and equipment must be delivered and loaded in an isolated area
   (vii) Systems must not be taken off-site without proper authorization
   (viii) Location of the equipment/server rooms must not be obvious.

8. **Business continuity management:**
   (i) Business Continuity Plan (BCP) must be maintained, tested and updated
   (ii) All staff must be made aware of it
   (iii) Business Impact Analysis must be conducted annually.
   (iv) SLA for network services

9. **System development and maintenance control:**
   (i) System development must have appropriate security controls
   (ii) Security controls must be identified and agreed prior to the development

**Audit policy:**
Audits may be conducted to ensure integrity, confidentiality and availability of information and resources. The Audit is done to protect entire system from the most common security threats which includes the following:
   (i) Unauthorized access to confidential data
   (ii) Unauthorized access of the computer department
   (iii) Password disclosure
   (iv) Virus infections
   (v) Denial of service attacks
   (vi) Unnecessary open ports, which may be accessed by outsiders
   (vii) Unrestricted modems

**Objectives of IS audit:**
   (i) Safeguard the Information System Assets/Resources
   (ii) Maintain the Data Integrity
   (iii) Maintain the System Effectiveness
   (iv) Ensure System Efficiency, and
   (v) Comply with Information System policies and guidelines

**Scope of IS audit:**
- **General scope:**
  To check adequacy and effectiveness of the system of internal control
- **Additional scope:**
  To check quality of performance by the information system
Categories of IS Audit:

(i) Data – Data/Information/Reports in whichever form.
(ii) Application systems – Business software/ERP and other support S/W
(iii) Technology – Network/Servers/Devices
(iv) Facilities – Infrastructure/Building/Server room etc
(v) People – Employees/Contract workers/Vendors/Customer

The information system auditor will examine, among others, the following:

(i) Information system mission statement, goals and objectives
(ii) Assessment of the risk
(iii) Information system strategic plans and their monitoring
(iv) Information system budgets and their monitoring
(v) High level policies for information system use
(vi) Major contract approval
(vii) Monitoring of performance against service level agreements
(viii) Acquisition of major information systems
(ix) Impact of external influences such as internet, merger of suppliers or liquidation etc.
(x) Review of past technical reports on Information System
(xi) Business Continuity Planning, Testing thereof and Test results
(xii) Compliance with legal and regulatory requirements
(xiii) Appointment and succession planning for senior information system staff

What audit policy should do?

The audit policy should lay down the audit responsibility as follows:

(i) Policy should lay out the periodicity of reporting and the authority to whom the reporting is to be made
(ii) Professional qualification and experience of systems auditor
(iii) System auditors will sign a declaration of fidelity and secrecy
(iv) Policy may lay out the extent of testing to be done during
   - Planning
   - Compliance Testing
   - Substantive Testing
(v) A documented audit program would be developed including the following:
   - Documentation of the information system auditor’s procedures for collecting, analyzing, interpreting, and documenting information during the audit.
   - Objectives of the audit.
   - Scope, nature, and degree of testing required to achieve the audit objectives in each phase of the audit.
   - Identification of technical aspects, risks, processes, and transactions which should be examined.
   - Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.
(vi) Policy would define the access rights to be given to the auditors:
   - User level, system level access to any computing or communications device
   - Access to information (electronic, hardcopy, etc.)
   - Access to work areas (labs, offices, cubicles, storage areas, etc.)
   - Access to reports / documents created during internal audit.
   - Access to interactively monitor and log traffic on networks.
(vii) The Policy should outline the compliance testing areas e.g.
   - Organizational and Operational Controls
   - Security Management Controls
   - System development and Documentation Controls
   - Application Controls
   - Physical and Environmental Controls
   - Access Controls
   - Business Continuity Controls, etc.
(viii) The auditor will carry out substantive testing wherever the auditor observes weakness in internal control or where risk exposure is high. The auditor may also carry out such tests to gather additional information necessary to form an audit opinion.

(ix) The Audit Policy would define the compulsory audit working papers to be maintained and their formats.

**Audit working papers and documentation:**

Working papers should record the audit plan, the nature, timing and extent of auditing procedures performed, and the conclusions drawn from the evidence obtained. All significant matters which require the exercise of judgment, together with the auditor’s conclusion thereon, should be included in the working papers.

The form and content of the working papers are affected by matters such as:

- The nature of the engagement,
- The form of the auditor’s report,
- The nature and complexity of client’s business, and
- The nature and condition of client’s records and degree of reliance on internal controls.

**Working papers:**

Permanent audit file normally includes:

(i) Organization structure of the entity
(ii) IS policies of the organization
(iii) Historical background of the information system in the organization
(iv) Extracts of copies of important legal documents relevant to audit
(v) Record of the study and evaluation of the internal controls
(vi) Copies of audit reports and observations of earlier years
(vii) Copies of management letters issued by the auditor, if any

Current file normally includes:

(i) Acceptance of appointment and the scope of the work
(ii) Evidence of the planning process of the audit and audit program
(iii) Record of the nature, timing, and extent of auditing procedures performed
(iv) Communication with management
(v) Letters of representation and confirmation received from the client
(vi) Conclusions reached by the auditor concerning significant matter
(vii) Copies on the data and system being reported on

**Planning the documentation:**

The following three parameters would help in planning a documentation process:

(i) The importance of planning and understanding the planning process requires identifying three planning questions:
   a) Knowing Your Resources
   b) Defining the Scope and Audience
   c) Using a Scope Definition Report

(ii) The Documentation Writer: The qualities and skills that the documentation writer would need should be judged. The requirement may often be legal in nature.

(iii) Rules to guide documentation writing:
   a) Writing in Active Voice: Using active voice in documentation.
   b) Giving the Consequences: Giving the consequences of the reader's action.
   c) Writing from General to Specific: Designing the documentation from general to specific.
   d) Consistency: Using of style, order and format consistently.
Gathering information:
To be able to have a good documentation, it is necessary to get information about the reader and the requirement of the document.
   (i) About the Reader
   (ii) About the Subject

Organizing information:
   (i) Selecting Information: Selecting ‘what the reader needs to know’. Organizing the information into a useful sequence.
   (ii) Organizing the Documentation: The sequence of document can be according to:- subject, difficulty, chronological, importance and analytical.
   (iii) Dividing Into Sections: Dividing documentation into chapters or sections.
   (iv) Dividing Into Subsections: Dividing sections or chapters into subsections.

Finalizing documents:
   (i) Reviewing and Testing: Selection of reviewer of the documentation involves identification of subject and communication skill. The reviewer must be provided with adequate information regarding the audience and object of the report. In order to ensure objectivity it is recommended that the reviewer be a person who has not been involved in the documentation process.
   (ii) Generating the Glossary and Index: Compilation of a glossary and generation of an index are two major tasks for a complete documentation. In order to achieve this task it is necessary to mark the Index and glossary entries at the stage of documentation itself. Word processing software comes with an inbuilt ability of creating an index from the identified text in the body of the document.
   (iii) Formatting and Production: The idea of creating a good document is not possible without first deciding on a good design for the same. This involves choosing effective formatting options for headings, sub-headings, section breaks, formatting, and allied. It is also important to select an appropriate binding style that would aid filing and ease of consultation.

**IS audit report: Structure / Format**

   (i) Cover and Title Page
   (ii) Table of Contents
   (iii) Executive Summary
   (iv) Introduction
       o Context
       o Purpose
       o Scope
       o Methodology
   (v) Findings
   (vi) Opinion
   (vii) Appendices
CHAPTER 10 – QRP (Quick Revision Points)

INFORMATION TECHNOLOGY (AMENDMENT) ACT 2008

Objectives of the Act are:
1) To grant legal recognition to
   - Electronic records
   - Electronic transactions
   - Digital signature
2) Electronic filing with Government
3) Electronic fund transfer
4) Book of accounts by banker’s in electronic form.
5) To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY
1. Negotiable instrument other than a cheque.
3. Trust.
4. Will
5. Contract for the sale of immovable property

Section 2: Definitions

- **Access**: Gaining entry into (instructing or communicating with the logical, arithmetical, or memory function resources of) computer system or computer network

- **Addressee**: A person who is intended by the originator to receive the electronic record but does not include any intermediary

- **Asymmetric Crypto System**: A system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature

- **Certification Practice Statement**: A statement issued by a Certifying Authority to specify the practices that the Certifying Authority uses in issuing Electronic Signature Certificates

- **Communication Device**: Cell Phones, Personal Digital Assistance, or any other device used to communicate, send or transmit any text, video, audio, or image

- **Computer**: Any electronic, magnetic, optical or other high-speed data processing device which performs logical, arithmetic, and memory functions and includes all input, output, processing, storage, computer software, or communication facilities connected to it

- **Computer Network**: The interconnection of one or more Computers or Computer systems or Communication device through -
  (i) the use of satellite, microwave, terrestrial line, wire, wireless and
  (ii) terminals consisting of two or more interconnected computers or communication device

- **Computer Resource**: Computer, communication device, computer system, computer network, data, computer database or software

- **Computer System**: A device or collection of devices, including input and output support devices (excluding calculators which are not programmable), which contain computer programs, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions
- **Cyber Café:** Any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public

- **Cyber Security:** Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction

- **Data:** A representation of information, knowledge, facts, concepts or instructions which have been prepared in a formalized manner and has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer

- **Digital Signature:** Authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3

- **Digital Signature Certificate:** A Digital Signature Certificate issued under sub-section (4) of section 35

- **Electronic Form:** Any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device

- **Electronic Record:** Data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche

- **Electronic signature:** Authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature

- **Information:** Includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche

- **Intermediary:** Any person, who on behalf of another person receives, stores or transmits a record or provides any service with respect to a record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes

- **Key Pair:** In an asymmetric crypto system there is a private key and a related public key, which are so related that the public key can verify a digital signature created by the private key

- **Originator:** A person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary

- **Secure System:** Computer hardware, software, and procedure that -: (a) are reasonably secure from unauthorized access and misuse (b) provide a reasonable level of reliability and correct operation (c) are reasonably suited to performing the intended functions; and (d) adhere to generally accepted security procedures

- **Verify:** In relation to a digital signature means to determine whether (a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber; (b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.
CHAPTER-II: DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

Section 3: Authentication of Electronic Records:
3(1) Electronic record can be authenticated by affixing his Digital Signature
3(2) Authentication is done by the use of asymmetric crypto system and hash function
3(3) Can be verified by public key of the subscriber
3(4) Private key and the public key are unique to the subscriber

Section 3A: Electronic Signature:
3A Electronic record can be authenticated by electronic signature which –
   (a) is reliable and
   (b) specified in Second Schedule
3A(2) Electronic signature is reliable if
   (a) Signature creation data linked to the signatory
   (b) Signature creation data is under the control of the signatory
   (c) Alteration to the electronic signature is detectable
   (d) Alteration to the information detectable
   (e) Fulfills such other conditions as prescribed
3A(3) Central Government may prescribe the details
3A(4) Central Government add to or omit any electronic signature from the second schedule;
3A(5) Notification issued under sub-section (4) shall be laid before Parliament

CHAPTER-III: ELECTRONIC GOVERNANCE

Section 4: Legal Recognition of Electronic Records:
Where any law requires any information in writing / typewritten / printed form, then such information can be –
   (a) made available in an electronic form; and
   (b) accessible for a subsequent reference

Section 5: Legal recognition of Electronic Signature:
Where any law requires signature on any document then digital signature can be used in such manner as may be prescribed by the Central Government.
Explanation – For the purposes of this section, "Signed", mean affixing of his hand written signature or any mark on any document

Section 6: Use of Electronic Records and Electronic Signature in Government and its agencies:
6(1) Where any law provides for –
   (a) filing of any form, application or any other document with any Government department
   (b) issue of any license, permit, sanction
   (c) receipt or payment of money
   then, such transactions can be done in electronic form as may be prescribed by the appropriate Government
6(2) Appropriate Government may prescribe rules for sub-section (1)

Section 6A: Delivery of Services by Service Provider (Inserted vide ITAA-2008):
6A(1) Appropriate Government may service provider to perform specified services for public
   Explanation – Service provider can be individual, private agency, private company, partnership, sole proprietor etc.
6A(2) Appropriate Government can take service charge
6A(3) Appropriate Government can take service charge even if there is no express provision for such charges in the respective Act
6A(4) Different service charges can be there for different services
Section 7: Retention of Electronic Records:
7(1) A document can be retained in the electronic form. Three conditions -
   (a) remains accessible so as to be usable for a subsequent reference;
   (b) retained in the format in which it was originally generated, sent or received
   (c) origin, destination, date and time of dispatch or receipt are available in the electronic
record:
7(2) This section shall not apply to any law where some other provision is there for retention of
  electronic records.

Section 7A: Audit of Documents etc in Electronic form:
Applicability of audit on electronic document also.

Section 8: Publication of rules, regulation, etc, in Electronic Gazette:
- Government will publish gazette in manual and electronic form also
- Date of notification will be – whichever is earlier

Section 9: Sections 6, 7 and 8 Not to Confer Right to insist document should be accepted in
electronic form:
Person cannot insist any government department to do transaction in electronic form

Section 10: Power to make rules by Central Government in respect of Electronic Signature:
The Central Government may prescribe rules for
   (a) type of Electronic Signature
   (b) how Electronic Signature shall be attached
   (c) how Electronic Signature will be verified
   (d) control procedures
   (e) any other matter

Section 10A: Validity of contracts formed through electronic means:
Contract can be formed by means of an electronic record

CHAPTER-IV: ATTRIBUTION, ACKNOWLEDGMENT AND DISPATCH OF ELECTRONIC
RECORDS

Section 11: Attribution of Electronic Records:
An electronic record shall be linked to the originator
   (a) if it was sent by the originator
   (b) by his authorized representative
   (c) by an information system programmed by him

Section 12: Acknowledgement of Receipt:
12(1) If originator has not specified the method for sending acknowledgment, then
   acknowledgment may be given by -
   (a) any communication from addressee (automated or manual)
   (b) any conduct of the addressee
12(2) If originator has specified that acknowledgment is compulsory, then electronic record will be
   valid only if acknowledgement is sent by the receiver
12(3) If originator has not specified that acknowledgement is compulsory and the receiver has not
   sent any acknowledgement, then the originator can give a first notice to the receiver
   regarding the non-receipt of acknowledgement and if no acknowledgement is received then
   after giving second notice treat the electronic record as cancelled
Section 13: Time and place of dispatch and receipt of electronic record:
13(1) Time of dispatch is when electronic record enters a computer resource outside the control of
the sender
13(2) Time of receipt of an electronic record shall be –
(a) if the addressee has designated a computer resource
   (i) receipt occurs at the time when the electronic record enters the designated computer
   resource; or
   (ii) if the electronic record is sent to a some other computer resource, receipt occurs at the
   time when the electronic record is retrieved by the addressee
(b) if the addressee has not designated a computer resource, receipt occurs when the
   electronic record enters the computer resource of the addressee.
(3) Place of dispatch – Place of business of sender
Place of receipt – Place of business of receiver
(4) Place where the computer resource is located may be different from the place where the
electronic record is deemed to have been received under sub-section (3).
(5) For the purposes of this section -
(a) If more than one place of business, the principal place of business is place of business
(b) if there is no place of business, his usual place of residence is place of business
(c) For a company "Usual Place of Residence" means the place where it is registered

CHAPTER-V: SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES

Section 14: Secure Electronic Record:
An electronic record on which security procedures have been applied

Section 15: Secure Electronic Signature:
An electronic signature shall be deemed to be a secure electronic signature if-
(i) signature creation data was under the control of signatory only
(ii) signature creation data was stored and affixed as prescribed
Explanation – In case of digital signature, the "signature creation data" means the private key of the
subscriber

Section 16: Security procedures and Practices:
The Central Government may prescribe procedures for sections 14 and 15

CHAPTER-VI: REGULATION OF CERTIFYING AUTHORITIES

Section 17: Appointment of Controller and other officers:

Section 18: Functions of Controller (CCA):
CCA specifies the following for CA (Certifying Authority)
- certifying public keys of the CA
- standards for CA
- qualifications and experience of employees of CA
- how CA shall conduct their business;
- content of advertisement of CA
- Format of Digital Certificate
- accounts of CA
- auditors of CA
- Help CA in implementing their system
- resolving any conflict between CA and subscribers
- duties of CA
- data-base of disclosure record of CA

Section 19: Recognition of foreign Certifying Authorities: Previous approval of the CG required

Section 21: License to issue electronic signature certificates:
CA applies to CCA and submits prescribed form and prescribed fees and other documents to CCA.
Section 22: Application for license:
CA to submit certification practice statement, proof of identity and fees not exceeding 25000

Section 23: Renewal of license: Fees not exceeding Rs.5,000

Section 24: Procedure for grant or rejection of license:
No application shall be rejected unless the applicant has been given a reasonable opportunity of being heard

Section 25: Suspension or Revocation of License:
Controller may revoke/suspend license of CA if
- wrong information is given to controller, or
- violation of act
Opportunity of being heard will be given to CA before revocation. If suspension is done for more than 10 days then opportunity of being heard will be given to CA

Section 26: Notice of suspension or revocation of license:
Controller shall publish a notice of suspension/revocation of license on its website for public

Section 27: Power to delegate:
Controller may appoint Deputy Controller, Assistant Controller or any officer

Section 28: Power to investigate contraventions:
Controller or any officer authorized by him in this behalf shall investigate any violation

Section 29: Access to computers and data:
Controller shall have access to any computer system if he has reasonable cause to suspect that any contravention has been committed

Section 30: Duties of Certifying Authorities:
Every Certifying Authority shall –
(i) make use of secure hardware and software
(ii) provide a reasonable level of reliability
(iii) follow to security procedures
(iv) be the repository of all Electronic Signature Certificates
(v) publish information regarding its practices and its Electronic Signature Certificates
(vi) observe other standards as prescribed

Section 34: Disclosure:
(1) Every Certifying Authority shall disclose –
   (a) its Electronic Signature Certificate
   (b) CPS (certification practice statement)
   (c) notice of revocation/suspension of its own digital certificate
   (d) any other material fact
(2) If any incident occurs in the system of CA, then CA shall -
   (a) notify this to any person who can be affected by that occurrence
   (b) act in accordance with its certification practice statement

CHAPTER-VII: ELECTRONIC SIGNATURE CERTIFICATES

Section 35: Procedure for issuing Digital Signature Certificate by Certifying authority:
Application is made by subscriber in the prescribed form and fee not exceeding Rs.25,000
Digital Signature Certificate shall be issued only when Certifying Authority is satisfied that –
(a) applicant holds the private key
(b) Private key is capable of creating a digital signature;
(c) public key can be used to verify a digital signature affixed by the private key

Section 36 : Representations upon issuance of Digital Signature Certificate
Certifying Authority should certify that it has complied with the provisions of the Act
Section 37: Suspension of Digital Signature Certificate:
Certifying Authority may suspend certificate in public interest. If suspension is more than 15 days than opportunity of being heard is given to subscriber

Section 38: Revocation of digital signature certificate:
CA can revoke the certificate under certain circumstances after giving opportunity of being heard to the subscriber

Section 39: Notice of suspension or revocation:
If digital certificate if suspended or revoked then CA will give public notice

CHAPTER-VIII: DUTIES OF SUBSCRIBERS

Section 40: Generating Key Pair:
Generating key pair is the duty of subscriber by applying security procedure

Section 40A: Duties of subscriber of Electronic Signature Certificate:
Duties as may be prescribed

Section 41: Acceptance of Digital Signature Certificate:
(1) Subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of Digital Signature Certificate -
   1. to one or more persons;
   2. or otherwise demonstrates his approval in any manner.
(2) By accepting a Digital Signature Certificate the subscriber certifies that –
   (a) the subscriber holds the private key
   (b) all information given by the subscriber to CA is true
   (c) all information in the Digital Signature Certificate is true.

Section 42: Control of Private key:
(1) It is the duty of the subscriber to protect and control Private Key
(2) If the private key is disclosed or lost, then inform to CA immediately

CHAPTER-IX: PENALTIES AND ADJUDICATION

Section 43: Penalty and Compensation for damage to computer, computer system, etc
A person shall be liable to pay compensation if he, without permission of the owner -
(a) accesses computer system
(b) downloads, copies or extracts any data
(c) introduces computer contaminant or computer virus
(d) damages data or computer system or network
(e) disrupts computer system or network
(f) denies access to any authorized person
(g) wrongly charges the services
(h) destroys, deletes or alters any information
(i) Steals or destroys or alters source code

Explanation - for the purposes of this section -
(i) "Computer Contaminant" means a program which can modify, destroy, record, transmit data or program residing within a computer system or by any means usurp the normal operation of the computer system
(ii) "Computer Database" means a collection of information, knowledge, facts, concepts or instructions in text, image, audio, video that have been prepared in a formalized manner to be used in a computer system
(iii) "Computer Virus" means any program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program is executed
(iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.
"Computer Source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form

Section 43A: Compensation for failure to protect data
If an organization has any sensitive personal data in its computer resource, then if it is negligent in implementing and maintaining reasonable security controls and thereby causes loss to any person, then such organization shall be liable to pay compensation, to the person so affected.

Section 44: Penalty for failure to furnish information, return, etc
a) Non-filing of return/document – Upto Rs 1,50,000
b) Late filing – Upto Rs 5000 per day
c) Non-maintenance of books of accounts – Upto Rs 10,000 per day

Section 45: Residuary Penalty:
If no penalty has been separately provided for any contravention than residuary penalty upto Rs 25,000 can be imposed

Section 46: Appointment and Powers of Adjudicating officer:
− Central government shall appoint an adjudicating officer for deciding penalty and compensation
− Person should have experience in the field of IT and Legal experience
− Adjudicating officer will decide on matters where claim is upto rupees five crores
− If claim exceeds rupees five crores then it will be decided by the court
− Adjudicating officer will give reasonable opportunity of being heard
− Adjudicating officer shall have the powers of a civil court

Section 47: Factors to be taken into account by the adjudicating officer:
While deciding the amount of compensation the adjudicating officer consider the following factors
(a) the amount of gain or unfair advantage made as a result of the default
(b) the amount of loss caused to any person as a result of the default
(c) the repetitive nature of the default

CHAPTER X: Cyber Regulation Appellate Tribunal
1) Central government shall establish
2) Tribunal shall consist of a Chairperson and judicial and non-judicial Members
3) Qualifications
− Chairperson: Judge of a High Court
− Non-judicial members: Persons, having special knowledge of and professional experience in, information technology, telecommunication, industry, management or consumer affairs.
− Judicial Members: Persons who is or has been a member of the Indian Legal Service
4) Tenure in office - five years or age of 65 years, whichever is earlier
5) Salary and allowances - as prescribed
6) Chairperson shall have powers of general supervision
7) Chairperson may distribute the business of the Tribunal amongst the Benches
8) Chairperson may transfer any case pending before one Bench to other Bench
9) Decision of the tribunal by majority of members
10) Vacancy in the office of the Chairperson/Member shall be filled by Central Government
11) Chairperson or Member can be removed by the Central Government after an inquiry has been made by a Judge of the Supreme Court

Section 57: Appeal to Cyber Regulations Appellate Tribunal:
1) Appeal can be filled against order made by a Controller or adjudicating officer
2) Appeal cannot be filled if order passed with the consent of the parties
3) Time limit for filling appeal is 45 days
4) Prescribed form, prescribed fees
5) Opportunity of being heard will be given
6) Tribunal can confirm, modify or set aside the order appealed against.
7) Effort shall be made to finish the appeal within six months.
Section 58: Procedure and Powers of the Cyber Appellate Tribunal:

Tribunal shall have the power of civil court -
(i) summoning and enforcing the attendance of any person and examining him on oath
(ii) requiring the discovery and production of documents or other electronic records
(iii) receiving evidence on affidavits
(iv) issuing commissions for the examination of witnesses or documents
(v) reviewing its decisions
(vi) dismissing an application for default or deciding it ex parte
(vii) any other matter which may be prescribed

Section 62: Appeal to High court:
- Appeal can be filled in High Court against the order of Tribunal within 60 days
- Appeal can be filled on question of fact or law

Section 63: Compounding of Contravention: Fine against penalty

CHAPTER XI: OFFENCES
- Section 65: Tampering with Computer Source Documents: Imprisonment up to 3 years or fine up to 2 lacks or both.
- Section 66: Computer Related Offences as per section 43: Imprisonment up to 3 years or fine up to 5 lacks or both.
- Section 66A: Sending offensive messages through communication service, etc: Imprisonment up to 3 years and fine.
- Section 66B: Dishonestly receiving stolen computer resource or communication device: Imprisonment up to 3 years or fine up to 1 lacks or both.
- Section 66C: Identity Theft: Imprisonment up to 3 years or fine up to 1 lacks or both.
- Section 66D: Cheating by personating by using computer resource: Imprisonment up to 3 years or fine up to 1 lacks or both.
- Section 66E: Violation of privacy: Imprisonment up to 3 years or fine up to 2 lacks or both.
- Section 66F: Cyber terrorism: Upto life imprisonment
- Section 67, 67A, 67B: Publishing or transmitting obscene material in electronic form: Imprisonment up to 5 years or fine up to 10 lacks or both.

Section 68 Controller may give directions to a Certifying Authority to take such measures as specified in the order. If any person fails to comply, he shall be liable to imprisonment up to 3 years or fine up to Rs.2 lakhs, or both

Section 69 Power of controller to intercept any information on computer network for security reasons

Section 69A Power of controller to block public access of any information through any computer resource for security reasons

Section 69B: Power of Central Govt to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security
"Traffic data" means network logs which can identify origin, destination, route, time, date, size, duration or type of underlying service or any other information

Section 70 empowers the appropriate Government to declare by notification any computer, computer system or computer network to be a protected system. Any unauthorized access of such systems will be punishable with imprisonment which may extend to ten years or with fine.

Section 70A National Nodal Agency: The central Government may appoint an organization of the Government as the National Nodal Agency in respect of Critical Information Infrastructure Protection. The agency shall be responsible for all measures including research and development relating to protection of critical information infrastructure.
Section 71 provides that any person found misrepresenting or suppressing any material fact from the Controller or the Certifying Authority shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both.

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

Section 73 provides punishment for publishing a Digital Signature Certificate false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both.

Section 75 provides for punishment for commission of any offence or contravention by a person outside India irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Section 76 provides for confiscation of any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto in respect of contravention of any provision of the Act, rules, regulations or orders made there under.

Indian Computer Emergency Response Team (CERT-In):
CERT-In to serve as national agency for incident response (Section 70 B):
- Appointed by Central Govt
- Central Govt shall appoint Director General and other officer. Salary and allowances as prescribed.
- Functions of CERT-In in the area of Cyber Security,
  (a) collection, analysis and distribute information on cyber incidents
  (b) forecast and alerts of cyber security incidents
  (c) emergency measures for handling cyber security incidents
  (d) coordination of cyber incidents response activities
  (e) issue guidelines, security practices, procedures for prevention of cyber incidents
  (f) such other functions as prescribed
- CERT may give order to service providers, intermediaries, data centers, body corporate
- Any person who does not comply with the order shall be punishable with imprisonment upto one year or with fine upto one lakh rupees or with both

Section 79: Intermediaries not to be liable in certain cases
Network Service Providers (Intermediaries) shall not be liable for any third party information or data made available by him if he proves that the offence was committed without his knowledge or consent.

Section 79A: Examiner of Electronic Evidence
For the purposes of providing expert opinion on electronic form evidence before any court or other authority, the central government may appoint an Examiner of Electronic Evidence.

Section 85: Offences by Companies:
- In case of company the person responsible for the conduct of business shall be liable
- However, he shall not be liable if he proves that the contravention took place without his knowledge or that he exercised all due care to prevent the contravention
- ‘Company’ includes a firm or other association of persons and ‘director’ in relation to a firm means a partner in the firm

Section 88: Cyber Regulation Advisory Committee:
- Constituted by Central Govt
- Consist of Chairperson, Official and Non-official members
- Gives advice to Central Govt and CCA
- Allowances as prescriber