

ISCA Supplementary Book

Including Recent Additions to ISCA Syllabus

Additions/Changes introduced in the ISCA syllabus:

There have been some additions in the ISCA syllabus. In this supplementary copy to ISCA book, I have made an attempt to cover all the additions. Please let me know your suggestions about the coverage which I have provided in this supplementary copy, I will improve the same in the revised edition of book.

**Best Wishes,
Dinesh Madan**

Chapter-1 Additions:

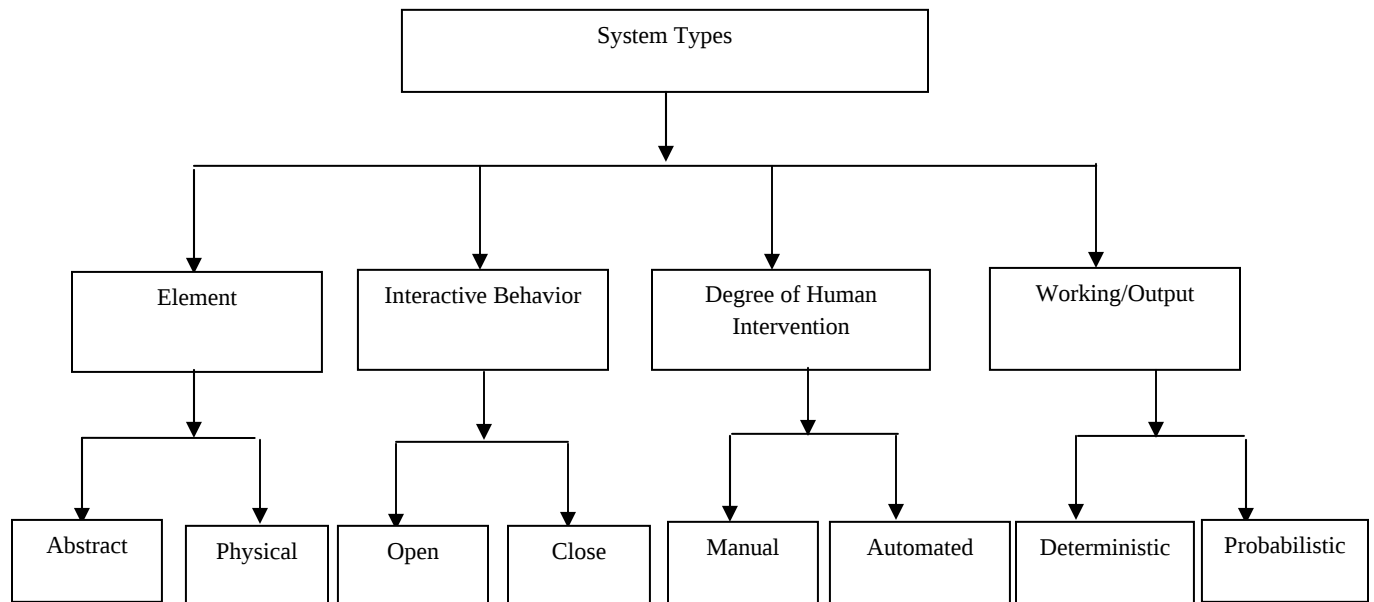
The following key additions are introduced in this chapter:

System Types:

Although this topic is already covered in the chapter, but a new system type has been added in the new book and that new system type is:

Manual or Automated System:

A system which includes manual operations for processing etc is known as manual system and the system which includes the automated processing (or computer based processing) is known as an automated system.



System Decoupling:

We have already covered all the sub-system concepts in the main chapter, for example:

- System Decomposition
- System Interface
- System Simplification
- System Stress or System Change
- Supra System

However, a new sub-system concept known as System Decoupling has been added in chapter-1

System Decoupling:

If two sub-systems are connected tightly with each other then very close co-ordination is required between them for their operations. For example, if raw material is placed directly into production the moment it arrives in the factory then raw material system is tightly coupled with production system. However, when a system functions independent of other systems then that concept is known as **system decoupling**. To achieve system decoupling the buffer, store or inventory technique is used which helps to maintain an **independency or decoupling** between the functioning of two systems.

Components of Computer Based Information System (CBIS):

The following key components are part of CBIS:

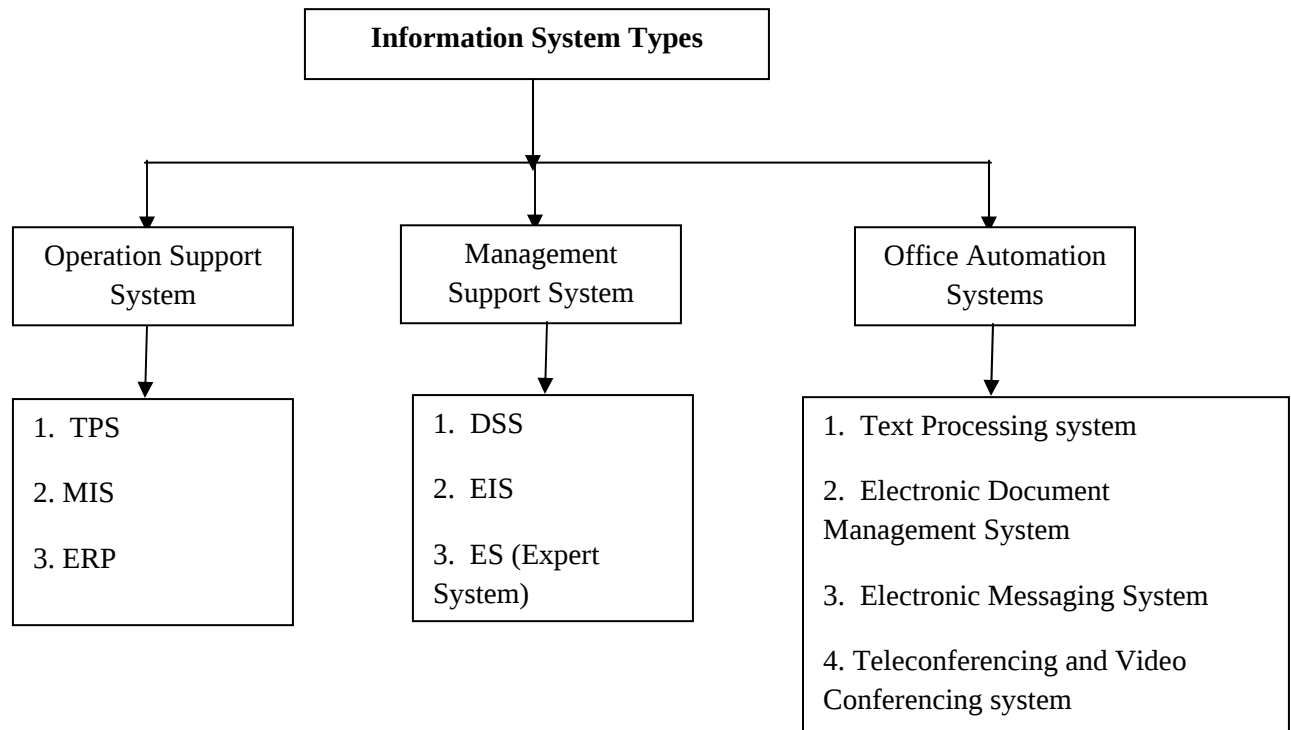
- (1) Hardware: such as CPU, RAM and Hard disk etc
- (2) Software: this includes system software like OS and application software which maintain logics for data processing
- (3) Data: this component includes facts and figures. In business, we can call this as transactions. Data is ultimately processed by CBIS to produce useful information
- (4) Procedures: These are policies and rules which govern the functioning of CBIS. In fact, the procedures provide an efficient working and use of CBIS.
- (5) People: This includes users, programmers, system analysts etc. The success of CBIS depends upon the people.

Common applications used in the Computer Based Information Systems are:

- (1) Finance and Accounts
- (2) Marketing and Sales
- (3) Production and Manufacturing
- (4) Inventory and store management
- (5) Human Resource Management

Information System Types:

This topic has been revised with some additions. For example, previously, there were TPS, MIS, DSS and EIS information system types covered in this topic. In the revised edition, this topic has been expanded as shown below. Though ERP is covered in detail in the chapter 7, but some new concepts related to ERP have been added in this chapter.



Transaction Processing Systems (TPS) Features:

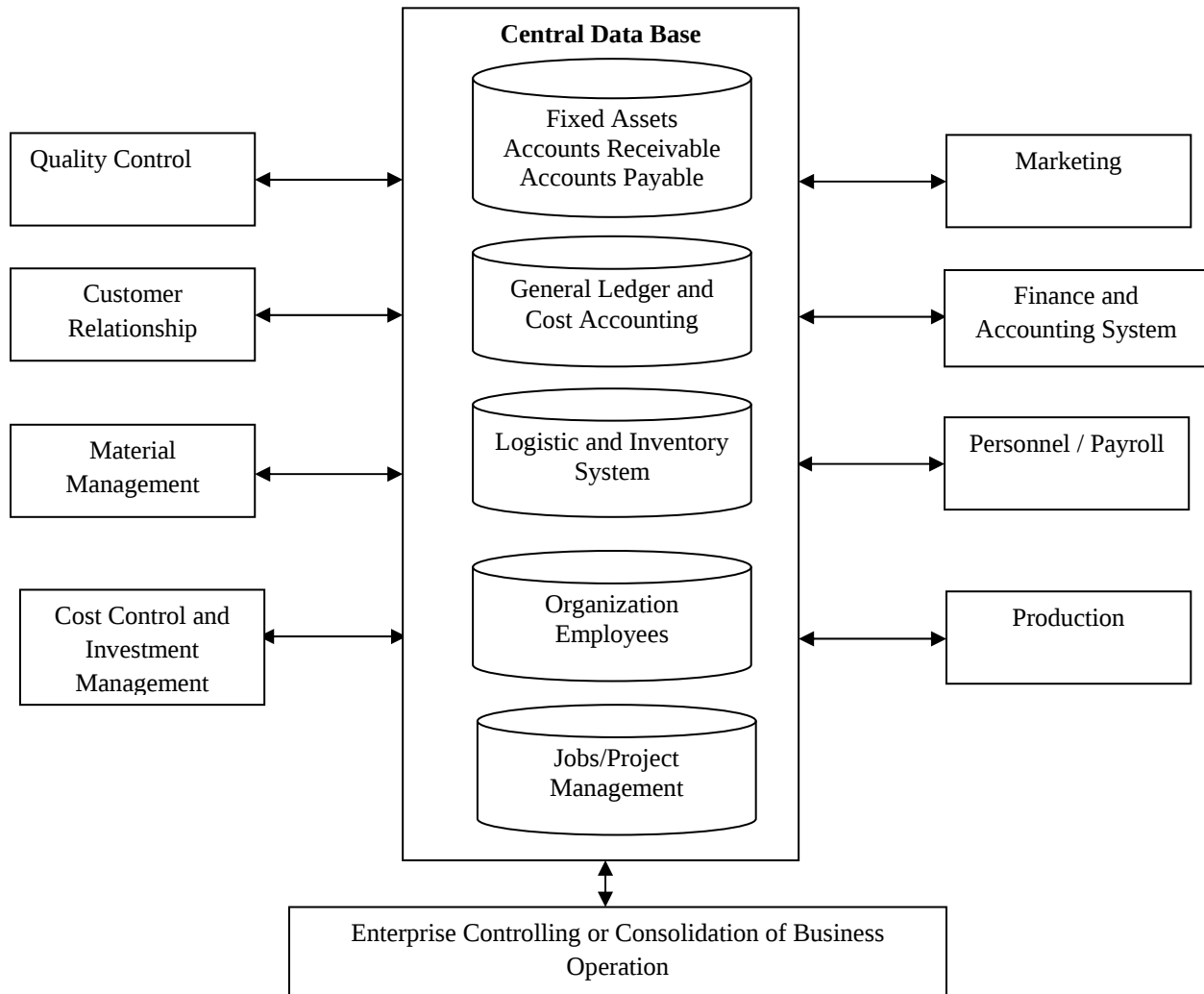
This topic is also covered in the main chapter except the following new additions:

Feature of TPS: TPS has the following key features:

- (1) Can handle large volume of data for processing
- (2) Help to automates routines or basic operations
- (3) Acts as base to other information systems or provides inputs to other information systems.
- (4) Provides easily measurable benefits like reduce workload on personals, etc.

ERP Model and its Limitations:

ERP provides a fully integrated management system in the organization. It helps to integrate the core business processes and functions of the organization. ERP integrates the various business processes as shown below in the ERP model.



ERP Model

Limitation of ERP:

- (1) ERP provides information on past and current status. Normally, it does not provide information on future trends.
- (2) ERP integration with other companies system results in conflict in use of system processes-- due to use of different methods. This integration also results in data quality issues.

Management Support Systems – Expert System:

These systems are categorized as systems which support management for effective decision making. DSS, EIS and ES are the three systems defined in this category. DSS and EIS are already covered in the chapter-1. Below is explanation of expert system.

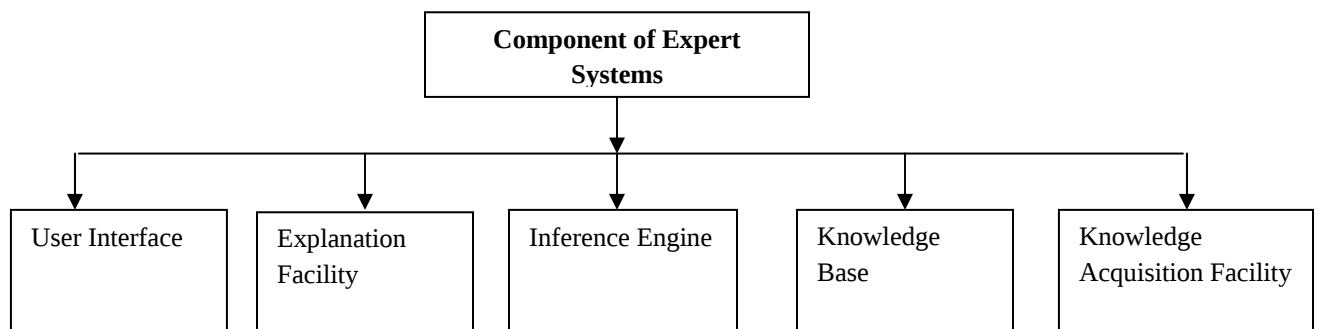
Experts Systems:

Expert system is a computer based information system which provides the advices or solutions of given problems just like the human experts. Expert system works on the principle of Artificial Intelligence to solve complex and unstructured problems normally in a specific problem area like audit etc—same as human experts.

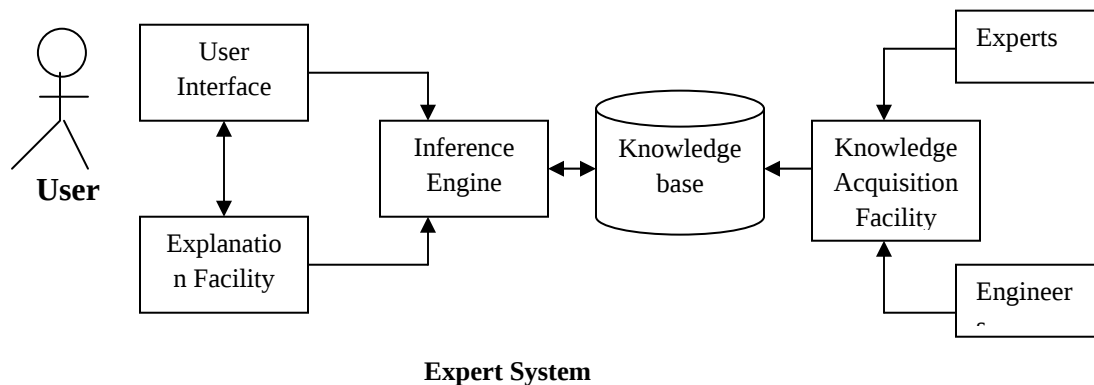
Expert systems are also known as knowledge based systems because these systems contain the knowledge of experts in an organized and structured manners to solve the problems.

Component of Expert Systems:

The followings key components are part of an Expert System:



- (i) **User Interface:** User Interface allows a user to provide or communicate the problem to expert system for solution.
- (ii) **Inference engine:** Inference engine is the most important component of expert system; it is like a search engine on internet. It contains various rules and logics to arrive at solution for problem provided by users by matching the problem solution from knowledge base.
- (iii) **Explanation Facility:** It is like a reporting system, it provides an explanation of logics to users for solution arrived by expert system.
- (iv) **Knowledge Base:** Knowledge base contains the past knowledge of experts for problem solutions in an organized manner.
- (v) **Knowledge Acquisition Facility:** This component is used for building knowledge base of an expert system. This component is used by programmers/engineers for collecting and organizing knowledge and expertise of human experts in the knowledge base.



Characteristics of Expert System:

- Expert System provides problem solution or provides advice like human experts.
- Expert System can be example based, rule based and frame based for providing problem solution or advice
- In example based expert system, it searches the appropriate match for present problem or case with previous cases and their solutions from knowledge base. In rule base, it uses if then else rules for series of questions from users to draw conclusion for problem solution. In frame base expert system, it divides every data, processes etc into logically linked units called frames to create the most logical solution.
- Expert System provide various level of expertise like
Assistant Level: Provide user attention on problem area
Peer Level: Discuss the problem with user to arrive at an agreement
True Expert: User accepts the solution without any questions. (Very difficult to develop)

Benefits of Expert Systems:

- Provide low cost solution or advice
- Provide solution or advice based on the knowledge of many experts.
- Always available for solutions and advice, there is no time restriction as it happen in the case of human experts
- Help users in better decision making and also improve their productivity

Limitation of Experts system

- Costly and complex system to develop, and also it takes a lot of time to develop expert system.
- It is difficult to obtain the knowledge of experts in terms of how they specify a problem and how they make the decisions.
- It is also difficult to develop the programs to obtain the knowledge of experts for problems' solutions.

Uses of Expert System:

- Indian Revenue Department uses Tax Expert System to investigate tax evasions and frauds on the basis of given tax returns details.
- Doctors use expert system to diagnose the patient disease by providing symptoms of disease to expert systems
- Audit expert systems are used by auditors for audit related problems.

Office Automation Systems (OAS):

This is another new topic which has been added to the chapter-1. In this topic, we have been explained different type of systems used by organizations in their day-to-day office management activities. As you are aware that in the day-to-day office management, we normally perform the following activities:

- Create Documents
- Receipt and Distribution of Documents
- Capturing/Recording (saving) of received documents
- Search, retrieve and follow up
- Calculations
- Message Communications

All the above activities can be automated by using different types of computerized applications such as MS-Word, MS-Excel and Email, etc. In fact, MS-Office is a product meant for automating day-to-day office activities. The office automation products like MS-Office provide many benefits; for example:

- Help to create quality documents efficiently
- Help to receive, transfer, store and retrieve required documents efficiently
- Provide efficient communication system within and between organizations
- Reduce the cycle time for preparation, receipt and communication of messages
- Reduce the cost of message communications
- Provide high accuracy in message communications

The following key office automation systems are described in this chapter.

1. Text Processors and Related Systems
2. Electronic Document Management Systems
3. Electronic Message Communication Systems
4. Teleconferencing and Video Conferencing Systems

Text Processors and Related Systems:

- This is the most frequently useable OAS. This system helps in creating office documents

- This system automates the process of development of documents such as reports, letters and memos etc.
- This type of systems mainly uses the software like MS-Word, Corel Draw and Adobe Acrobat Writer to develop quality documents.
- These systems provide many features (like copy, paste, font type and size etc) to produce high quality documents efficiently.
- These systems are normally supported by laser printers and scanners for producing high quality documents.

Electronic Document Management Systems:

- In this type of systems, the office documents are captured (scanned) and stored in the computer for efficient management.
- This type of system provides many advantages over manual management of documents, for example:
 - Lesser space requirements (stored in hard disk)
 - Low cost document management (due to low memory cost)
 - Provides remote access of documents from anywhere, when documents are stored in networked servers
 - Provides secured document management i.e. access of documents as per user access rights and with login-id and password
 - Provides fast/prompt access of required documents

Electronic Message Communication Systems:

Business organizations are using different type of systems for sending and receiving the messages. These include telephone, email, voice mail and facsimile (Fax).

Three important components of Electronic Message Communication Systems are:

- Email
- Facsimile
- Voice Mail

(1) Email: Email has become the most popular electronic message communication system. It helps to transfer messages immediately and with high reliability. Email provides an economic method of message communication. Email services provide many features for efficient message communication, for example:

- Editor: Provide an efficient editor to edit the new or existing emails.
- Reply: This option helps to reply a received mail by writing the message in received mail itself.
- Forward Mail: This option allows forwarding a received email to another user.

- o Address Book: It helps to maintain mail addresses of friends and customers and it helps in mass mailing.
- o Block Sender: This option helps to block the addresses of unwanted senders from sending any email to your inbox.
- o Attachment: This feature helps to attach documents with mail message.

(2) Facsimile:

It provides an electronic communication of documents over telephone lines. The computer based Fax system automates the Fax communication and allows sharing of Fax facilities. It uses special Fax server to send and receive Fax from users' computers. The servers normally have the capability to scan the incoming Fax and reroute them to its appropriate recipient. The Fax servers help to maintain a centralized facsimile system.

(3) Voice Mail:

Voice mail is an extension of email services. In this, messages are transmitted as digitized voice. Sender transmits the message in a recorded voice form which is stored in voice mail box. Receiver can receive intimation of received voice mails which receiver can download and play to receive the voice messages.

Teleconferencing and Video Conferencing Systems:

Teleconferencing:

The term teleconferencing refers to electronic meetings that involves people at different physical locations. The telecommunication technologies of present days allow meeting participants to interact with each other from remote locations without traveling to same location for meetings. The teleconferencing can be audio or video type with or without the help of computers. Although computer based teleconferencing helps to communicate better and allows the recording of message and display of presentation.

Video Conferencing:

Video conferencing uses display screens, video cameras, computers and communication systems (High Speed ISDN Telephone Line, Satellite Link with Dish Antenna for dedicated video conferencing or internet) to link participants based at different locations. In this case participants can hear as well can see each others.

Chapter-2 Additions:

The following key additions are introduced in this chapter:

Approaches to System Development:

Currently, in chapter-2, the following system development approaches are described:

1. Pure SDLC or Traditional Approach

Alternative Approaches

2. Prototype Approach
3. End User System Development Approach
4. System Development Approach for Small Organization
5. Rapid Application Development (RAD)

In the new edition, this topic now includes the following system development approaches:

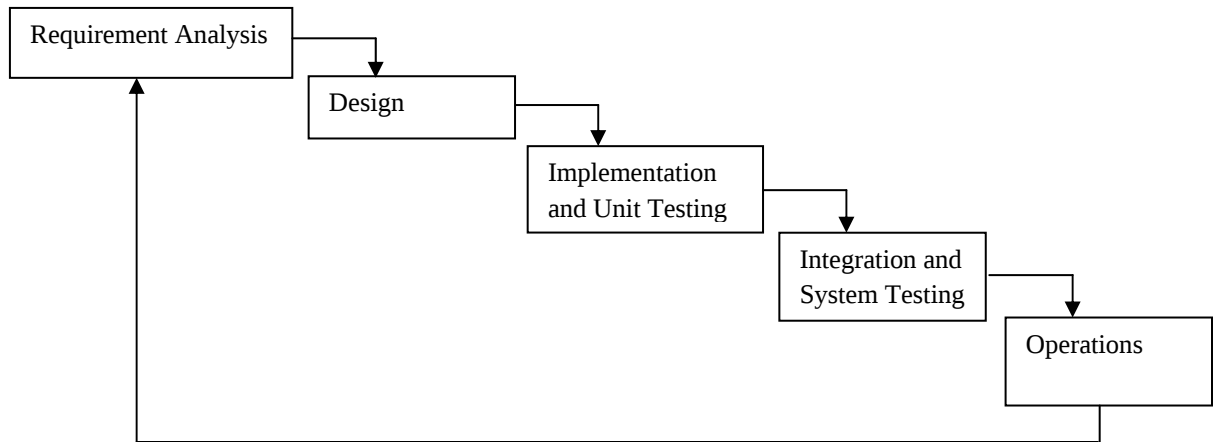
- (1) Water Fall or Traditional System Development Approach
- (2) Prototype Approach
- (3) Incremental Approach
- (4) Spiral
- (5) RAD (Rapid Application Development)
- (6) Agile Methodologies

Considering the revised system development approaches, we need to learn the following three additional system development approaches:

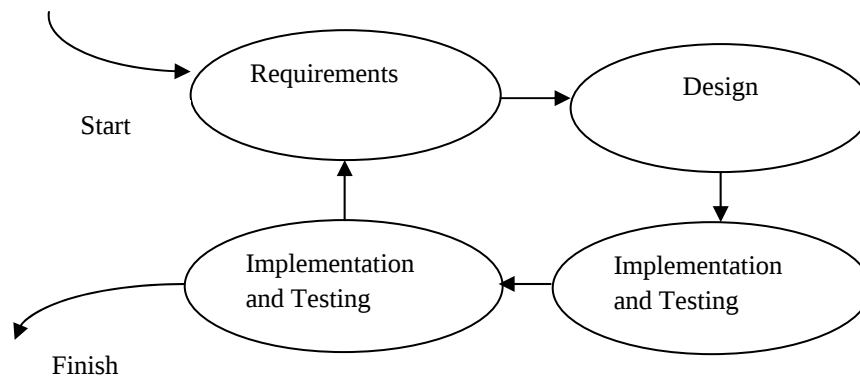
- (1) Incremental Approach
- (2) Spiral
- (3) Agile Methodologies:

Incremental Approach:

This model combines the approaches of water fall and prototype. In this model, the software product is built incrementally through different iterations. In this approach, a series of mini waterfall models are performed to provide the finished product.



An iterative or incremental lifecycle model does not attempt to start with a full specification of requirements. Instead, development begins by specifying and implementing just part of the software which can then be reviewed in order to identify further requirements. This process is then repeated, producing a new version of the software for each cycle of the model. Consider an iterative lifecycle model which consists of repeating the following four phases in sequence:

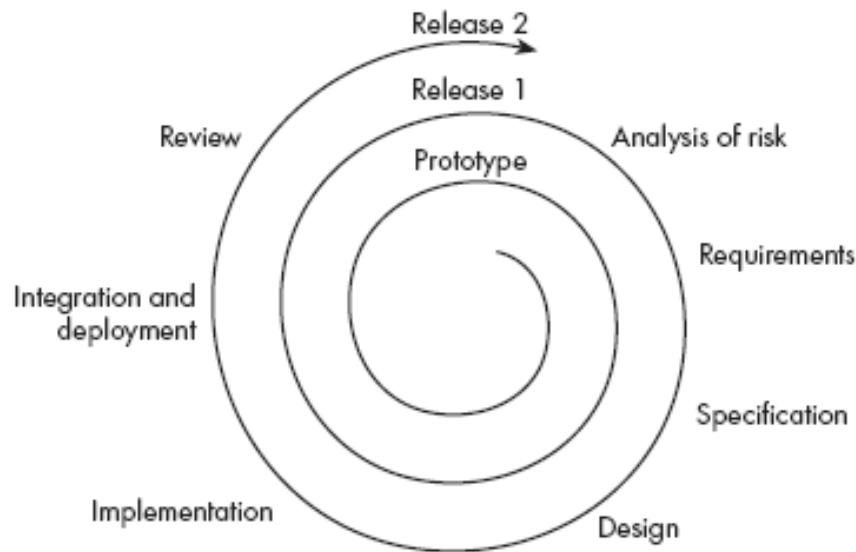


Spiral Model:

Spiral model is similar to incremental model but with more thrust on risk analysis and resolution. Spiral model is considered an evolutionary model and it also combines the features of the prototyping model and water fall model for project development. In this model, project development activities are represented as spiral rather than as sequence of activities with backtracking. Each loop in the spiral acts as phase in the process. No fixed phases such as system specification and design exist in this model; phases are selected depending upon what is required. The risks are explicitly assessed in each spiral's loops; and risks are resolved throughout the spiral process.

There are four key tasks (area) in the spiral model.

- (1) Objective Setting
- (2) Risk Assessment and Reduction
- (3) Development and Validation
- (4) Planning:



Spiral model is primarily used for complex and large projects and it provides following advantages and disadvantages:

Advantages:

- Estimates (i.e. Budget, schedule, etc.) become more realistic as work progresses, because important issues are discovered earlier.
- Software engineers can get their hands in, and start working on a project earlier.
- Prototyping in this model is used as a risk reduction mechanism
- After final iteration, all risks are resolved and the “requirements” are ready for development.

Disadvantages:

- The spiral model is intended for large, expensive and complicated projects.
- Highly customized model and it limits the re-usability of work performed in the previous projects.
- Risks of not meeting budget or schedule are fairly large due to long spiral process.
- Requires considerable expertise in risk evaluation and reduction.
- Complex, relatively difficult to follow strictly

Agile Methodologies:

All the other methodologies described in chapter -2 are based on the principles that any software development process should be predictable and repeatable to an extent, although prototype approach is also used where predictability is less known until prototype is ready. The main criticism of those methodologies is that those methodologies put more emphasis on following the particular procedures and preparing documentation. Therefore, those methodologies are considered heavyweight or extensive (rigorous) and also include excessive thrust on following the particular structure. With all these constraints for system development, a movement known Agile Software Movement started, which provides a conceptual framework for undertaking software engineering projects.

This approach describes that software development is essentially a human activity and will always include variations in processes and inputs; therefore model should be flexible enough to handle the variations. Thus, the Agile Methodology incorporates iteration and the continuous feedback that it provides to successively refine and deliver a software system. It involves continuous planning, continuous testing, continuous integration, and other forms of continuous evolution of both the project and the software. It is a lightweight (especially compared to traditional waterfall-style processes), and inherently adaptable. As important, it focuses on empowering people to collaborate and make decisions together quickly and effectively.

Some of the common characteristics of Agile Methodology are as follows:

- Includes time bound iterative cycles
- Includes iterative processes with short cycles enabling fast verifications and corrections
- Includes modular development process
- Users or people oriented approach
- Collaborative and communicative working approach
- Incremental and convergent approach that minimizes the risks and facilitates functional additions.

Some of the popular Agile Methodologies are: Scrum, FDD (Feature – Driven Development), Crystal and XP (Extreme Programming)

Other Key Additions in this Chapter:

The following additions have been introduced in this chapter relative to the previous chapter-2

(1) SDLC phases are increased to seven from existing six phases:

SDLC phases have increased to seven from six phases, although the seventh phase introduced as **Post Implementation Evaluation** is already covered in the sixth phase of existing chapter so I will say other than naming Post Implementation Evaluation as seventh phase there is no addition in this.

(2) Role of different persons during SDLC phases has been introduced, for example:

Steering Committee: Steering Committee provides an overall direction and is responsible for all costs and time schedules. Also, it makes regular review of project development and takes corrective actions accordingly.

Project Manager: He is a person responsible for liaisons with clients/users. He is responsible for delivery of project with given time and budgets. He conducts regular review with project leader and team leader for progress of project

Project Leader: A project manager may be responsible for many projects at the same instance, but project leader is solely dedicated to particular project. He monitors day-to-day progress of project.

Module Leader/Team Leader: A project development is normally divided into many modules and each module is assigned to a team and responsible person for that team is known as team leader or module leader

System Analyst/Business Analyst: System analyst is a person responsible to understand users' requirements and communicate that to programmers.

Programmer/Coder/Developer: Writes programs / codes or converts the design or requirements into programs by using some programming language. They are also responsible for initial debugging and testing of programs.

Database Administrators (DBA): This person is responsible for creating an efficient and secured database. He is also responsible to monitor the performance of database.

Quality Assurance Team: This team sets the standards for development of project and team check the compliance for standards from time-to-time.

Tester: Tester is a junior level quality assurance person. Tester tests the programs and modules, and prepares the test reports.

Domain Specialist: Whenever a project team develops a project which is new to them in terms of application logics, they take the help of domain specialist. For example, if a team undertakes a project for banking industry then they will take the help of a person who has expert knowledge of banking system working.

IS Auditor: As a member of project team, IS auditor ensure that adequate controls are observed while developing and testing applications.

(3) Addition of various Testing Techniques in System Testing phase:

In system testing phase, many software testing techniques are included; for example, unit testing, integration testing, system testing and acceptance testing. But these are almost already covered in the same form in the chapter-4 i.e. Testing of General and Automated Controls. So, we are not discussing these over here

(4) Addition of new maintenance types in the System Implementation and Maintenance phase:

In the System Maintenance phase, the following maintenance types are included—other than existing Schedule and Rescue maintenance types.

Corrective Maintenance: which is actually correcting errors or fixing bugs

Adaptive Maintenance: Refers to changes in the system as per the changes in the environment, and here environment refers to operating system and hardware components.

Perfective Maintenance: This is related to maintenance that helps to increase the performance of system.

(5) An introduction to operational manual is added:

A small new topic **operational manual** is added in this chapter:

Operational Manual:

A user's guide for software or hardware is known as operational manual. It is a technical document which guides users for use of particular system. It is normally written by a technical writer with assistance from programmer and project managers.

An operational manual normally includes the following: (the coverage is similar to any book; like ISCA Book!!!)

- A cover page, a title page and copyright page
- A preface
- An Index Page or Content Page
- Summary of key functions of system and their use.
- Sections which explain the use of system functions and troubleshooting
- Frequently Asked Questions (FAQ)
- Glossary, etc

(6) Organizational Structure of IT Department:

Though this is not a new topic but this is not covered in the current edition of ISCA book. So I am providing a brief introduction of this topic over here.

Organization Structure of IT department can be divided into two categories:

1. Information Processing Management
2. System Development and Maintenance

So we can say that IT department structure is related to operation management and project management.

(1) Information Processing Management Functions and Persons:

Data Entry Supervisor: Data entry Supervisor is responsible for ensuring use of authorized, complete and accurate data entry into the system.

File Librarian: The file librarian is responsible for recording, issuing, receiving and safeguarding all programs and data files that are maintained on computer tapes or disks

Control Group: The control group manages the flow of data and is responsible for the collection, conversion and control of inputs and the distribution of outputs to the users.

Operation Group: Operations management is responsible for the daily running of hardware and software facilities so that the production application system can accomplish their work and development staff can design, implement and maintain systems. The operations group within the IT department undertakes seven major functions, like

- Computer operations.
- Communication network control.
- Data preparation
- Performance monitoring.

Security Administrator: The security administrator in a data processing organization is responsible for matters of physical security.

LAN Administrator: LAN administrator is responsible for technical and administrative controls over the Local Area Network.

Help Desk: Help desk administration is responsible for monitoring, improving and controlling system performance in mainframe and client/server hardware and software.

(2) System Development and Enhancement Functions and Responsible Persons:

These are almost same persons as we discussed above in the Role of persons involved in SDLC.

Database Administrator: A person responsible for creating database and database security, and also responsible for performance monitoring.

Quality Assurance Group: QA group is responsible for testing and verifying whether the programs, program changes and documentation adhere to standards and naming conventions before the programs are moved into production

System Analysts: System analysts are responsible for determining the requirements of users from system to be developed or enhanced.

Application Programmers: Applications programmers are responsible for developing new programs for new systems.

System Programmers: System programmers are responsible for system software maintenance like operating systems.

(7) A final change is in system development tools where a few flowcharts and decision tables have been explained (which have already been covered at PE-II/IPCC/PCC levels).

Chapter-3 Additions

If we look at this chapter for new additions then no significant new concepts are added to this chapter, only existing concepts have been expanded to an extent. But some new additions are there in this chapter which we will discuss over here.

The IS Audit Process:

The IS audit process includes evaluation of the controls, logics and operation of Information System. Specifically, the IS audit process includes the following:

- Assessment of internal controls for validity, reliability and adequacy
- Assessment of effectiveness and efficiency of IS environment

Responsibility of IS Auditor:

A set of skills generally expected from IS auditors include:

- Auditor should have sound knowledge of business operations, practices and compliance requirements
- Should have requisite professional technical qualifications
- Should have good understanding of information system risks and controls
- Should have knowledge of IT policies, particularly security policy
- Should possess good knowledge of standards and best practices of IT controls and security
- Should have ability to understand the technical controls

Functions of IS Auditor:

Primarily, IS auditors review the risks related to IT systems; for example:

- Auditors check whether information security is inadequate
- Auditor review and check whether IT resources are efficiently utilized
- Review and check IT related frauds
- Review and check whether organizations have adequate IT related policies
- Review and check whether system development and maintenance process is controlled processes or not

Categories of IS Audits:

IS audit is categorized in five types, i.e. an IS auditor audit the following broad area of information system:

(1) System and Applications: verify that system and applications are appropriate, efficient, valid and reliable.

(2) Information Processing Facilities: Verify that information facilities timely and correctly process the data.

(3) System Development: Ensure that system development meet the objectives of business and is controlled activity

(4) Management of IT and Enterprise Architecture: Ensure that IT management has developed an adequate organization structure and procedures to control the activities

(5) Telecommunications, intranet and internet: Verify that data communication is secured

Steps in Information Technology Audit:

Different organizations go for IS audit in different ways; in general, IS audit can have the following six steps:

- Scoping and Pre-audit survey: Determine main focus area for audit
- Planning and Preparation: Planning the tasks in details for audit to cover the focus area or the risks.
- Audit work / Fieldwork: Conducting audit as per planning
- Analysis: This includes analysis of audit results
- Audit Reporting : Reporting results to management
- Closure Notes: Closing audit assignment with required follow ups.

Audit Standards:

ICAI issuance of **AAS (SA)** for audit can also be used for IS audit. **ISA 315** (International Standard on Auditing) also mention about standards for IS audit.

ISACA (Information System Audit and Control Association) is a global leader in information system governance, control, security and audit. ISACA has developed the following to assist auditors:

IS auditing standards: ISACA issued 16 auditing standards which define the mandatory requirements for IS auditing reporting and guidelines

IS Auditing Guidelines: ISACA provides 39 guidelines for applying IS audit standards

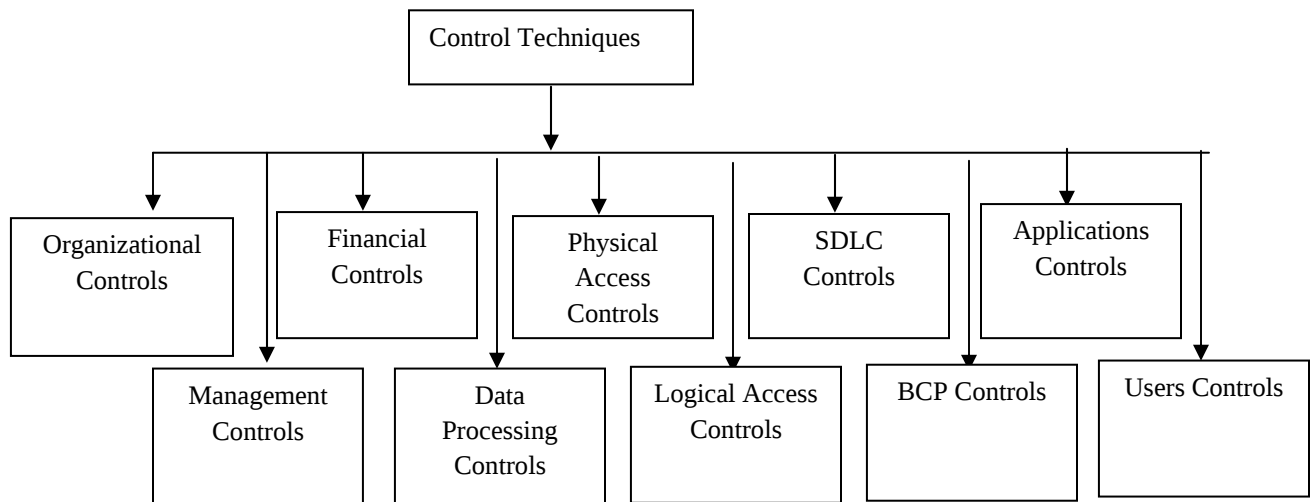
IS Auditing Procedures: ISACA issued 11 procedures for auditors to follows for conducting audit of information system

COBIT: is a framework contains good business practices related to information system

Like COBIT there are some other standards for information security and operations like **ISO 27001 (or BS 7799) and ITIL** etc which have been discussed in detail in chapter-8.

Information System Control Techniques:

Though this topic is covered through preventive, detective, corrective and compensatory controls in the existing chapter-3, but some more control techniques are discussed and many of those are repetitive.



Organization Controls:

These controls help in a structured decision making process and also help to avoid the frauds and misuse of resources in the organizations. These controls are implemented by creating policies and assigning responsibilities or duties. The following are the key organization controls

- Clearly defining responsibilities and objectives
- Establishing policies, standards, procedures and practices
- Defining clear job descriptions
- Segregations of duties

IS Management Controls:

These controls are extension of Organization Controls. These controls ensure that the management has the responsibility to establish controls for error free working of information system, and development of new Information System. These controls are primarily implemented by creating an IS organization structure. The following are key management controls:

- (1) Responsibility: Having IS management responsible within the overall organization structure of organization for IS controls
- (2) Adopting an official IS structure: With all staff deliberated on their roles and responsibilities.
- (3) An IT Steering Committee: Establishing a steering committee having members from IT departments and other business operations for direction of overall IT operation.

Financial Controls:

In general, these controls have very wide coverage but over here these controls have been defined as procedures established for source documents or transaction origination before their input to system and controls on output documents are also considered over here. The following key controls are defined as financial controls.

- Authorization
- Use of source documents in sequence
- Input / Output verifications
- Supervisor review
- Segregation of Duties
- Safekeeping of documents
- Document each task including cancellation
- Establishing Budget

Data Processing Environment Controls:

These are hardware and software related controls in which procedures are established for efficient online data entry, database administration and application program changes etc. These controls, to an extent, are similar to Data Integrity Controls

Physical Access Controls: Explained in existing Chapter-3

Logical Access Controls: Explained in existing Chapter-3

SDLC Controls (System development, acquisitions and maintenance controls): Explained existing in Chapter-3

BCP (Business Continuity Planning) Controls: Explained in existing Chapter-6

Application Controls:

Application Controls deals with exposure or risks with the application in terms of input, processing and output; for example, risks with payroll application and accounting applications etc. Application controls can be manual procedures, or programmed modules written into applications.

Primarily, application controls can be divided into three categories.

- Input Controls
- Processing Controls
- Output Controls

User Controls:

Applications provide an interface to users for data processing. For example, a bank's employee works through banking application for data processing. Although many controls are established in the application for correct data processing, still controls are required on users also to ensure authorized, efficient and effective data processing and use of information system. The following key controls can be established as user controls.

(1) Boundary Controls: These are primarily access controls mechanism. The following three key access control mechanism are used as boundary controls.

- **Identification:** Name, account number, address, card number
- **Authentication:** ID and Password, PIN, Finger Prints
- **Authorization:** Access rights for access of resources
- **Data Encryption:** Transfer of Data between users and system in a coded form

(2) Input Controls:

Input controls ensure that input data is valid, accurate and complete. Data codes like account number etc are used for accurate and efficient data entry. However there can be errors in entry of data codes also.

There can be two types of error in data code entry and which can cause processing errors.

1. Transcription Errors

2. Transposition Errors

Transcription error is incorrect digits use while data input, and it falls into three categories:

Addition Error: When an extra digit is added to the code like item no. 83276 is written as 832766

Truncation Error: When a digit is removed from the end of code like item no. 83276 is written as 8327

Substitution Error: One digit of code is replaced with another digit like item no. 83276 is written as 83277.

Transposition error is change of adjacent or non-adjacent digits:

There are two types of transposition errors

Single and Multiple Transposition Error: Occur when two adjacent digits are exchanged like item no. 83276 is written as 38276 and multiple transposition error occur when nonadjacent digits are exchanged like 83276 is written as 87236.

Addition and Truncation errors can be controlled using **fixed length digits** code, e.g. 16 digits account number.

Substitution and Transposition errors can be controlled by using **check digit control** method.

(3) Processing Controls:

These controls ensure correct processing of input data. Normally, these controls for users are implemented through data validation (i.e. validating data before processing) and database management system i.e. to accept correct data

only (in terms of size, mix of characters etc). But some of the processing controls which can be implemented for users are:

Format completeness Check: Check that all the required data entry fields (mandatory fields) exist during processing

Exception reports: to provide errors during processing

Transaction Log: To maintain audit trail of processed and rejected transactions

(4) Output Controls:

These controls ensure that error free output is delivered to authorized users and in a secured manner. Controls can be for different form of outputs (for printed and display), and can be for batch processing and online system. Some of the key output controls are:

- **Maintaining log** of output programs execution to know the details of communicated outputs
- **Spooling/Queue medication control:** Controls should be there on spooling/queue section to avoid unauthorized access of these sections. You might have experienced that many jobs to a single printer from multiple users get arranged in a queue and that queue is known as spooling section.
- **Controls over printing:** Selection of printer (in terms of its location and time of printing when organization has many printers in the network mode) should be such that disclosure of confidential information should be avoided.
- **Report Distribution:** Report distribution to authorized users should be in a secured form
- Secured maintenance of sensitive printed output forms/records.

(5) Database Controls (These are more applicable for batch processing which is not in much use these days)

These controls are used for protecting integrity of database when users update database through application.

Database controls are categorized as update controls and report controls.

Update Controls:

- Sequence check when transaction file update the master file to ensure correct updation
- Ensure all records in the transaction files are processed
- Ensure multiple updations for a single record occurs in a correct order
- Maintain suspense account for transactions not having their master.

Report Controls:

- Maintain integrity of internal tables used for various calculations, e.g. price list etc, through regular review
- Print run-to-run controls: i.e. option to print each step of transaction processing
- Printing of suspense account to view orphan transactions
- Review existence of backup and recovery controls to ensure safe recovery of data in any adverse situation

Chapter-10 Additions:

Additions to this chapter are already covered in the latest edition of ISCA book; however, I am again inserting this revision over here

Information Technology (Amendment) Act, 2008

Information Technology Act 2000 has been amended by Information Technology Amendment Bill 2006. The Bill was passed in Lok Sabha on December 22nd and in Rajyasbha on December 23rd of 2008. According to a recent Ministry of Communication & Information Technology news release, the Information Technology (Amendment) Act, 2008 has come into effect in India from October 27, 2009.

The primary objectives of IT (Amendment) Act, 2008 are:

- To include **Electronic Signature** for authentication of electronic documents and transactions instead of previous technology driven **Digital Signature** only
- To include more **electronic offences** which were not covered in the previous IT Act. For example, Cyber Terrorism and Video Voyeurism
- Provide power to central and state governments for **interceptions, monitoring and investigations** of electronic data for cyber security and electronic offences.
- To include more provisions for **protection of personal data and information**
- To harmonize the act by including and changing provisions to respond to changing need due to widespread use of information technology.

Electronic Signature v/s Digital Signature

Implementation of IT Act 2000 has given widespread use of information technology enabled services like e-governance, e-commerce and e-transactions applications. The use of these applications also facilitated the use of security practices like PIN (Personal Identification Number), Bio-signature, etc. Previous IT act only relied on the use of technology driven **Digital Signature** for authentication of electronic transactions and documents. In the amended act these security practices are also included for authentication of electronic transactions. In the IT (Amendment) Act, 2008 the Digital Signature is one of type of technology coming under the wider term known as Electronic Signature and other accepted security technologies are PIN, Bio-Sign (based on physical features like thumb impressions, eyes' retina, etc) and codes on magnetic strip (like smart card).

Added new electronic offences to the existing list of electronic offences:

- Sending offensive messages through a computer or mobile phone (Section 66A),
- Receiving stolen computer resource or communication device (Section 66B)
- Punishment for identity theft (Section 66C)
- Punishment for cheating by personate ng using computer resource (Section 66D)
- Punishment for violating privacy or video voyeurism (Section 66E)
- Cyber Terrorism (Section 66F)
- Publishing or transmitting material in electronic form containing sexually explicit act (Section 67A)
- Child pornography (Section 67B)

Database security and privacy:

Earlier, there was no clarity over data security and privacy issues in India, since this issue was not governed by any Act. There was no clarity when it came to the obligations of an enterprise which handles sensitive personal data (like credit card or medical information). With the new IT Act, the government necessitates that corporate bodies protect all personal data and information they possess, deal or handle in a computer resource. Sections 43A, 66E and 72A provide for personal data security and privacy.

Power of interception of electronic communication to the Government:

The amended Act empowers the state and central governments (sections 69A and 69 B) to issue directions for interception, monitoring, decryption of any information through any computer resource. It also empowers to order for blocking websites in the interest of national security, and friendly relations with foreign states. Further, it empowers the government to monitor, collect traffic data or information through any computer resource for cyber security. In the interest of national security and public interest etc., the central government may intercept/monitor any information transmitted through any computer resource for investigation of any offence.

Some Other Key Changes to IT Act Related to Electronic Offences:
--

Offences made bailable, less stringent:

Now most of the offences are considered Cognizable but Bailable and Compoundable. Now offences, punishable with imprisonment of more than three years are only non bailable.

The level of investigation brought down to the Inspectors from DSPs:

The level of investigation has been brought down to the level of *inspector from that of DSP*. It means, more IO are now available to investigate the cyber crime incidents.

Compensation Claims:

Compensation claim is no more restricted to rupees 1 crore only.

Intermediary Liability (ISP, Telecom Service Provider, Search Engines, Call Centers, etc):

A special liability has been imposed on call centers, BPOs, banks and others who hold or handle sensitive personal data. If they are negligent in implementing and maintaining reasonable security practices and procedures, they will be liable to pay compensation. The breach of confidentiality and leakage of data by intermediary is also punishable.

Abatement (Assist) and Attempt:

Abatement of the offences under the act is also made punishable. Any attempt to commit the offences under this act is punishable similar to the Indian Penal code.

Offence of hacking only if with dishonest or fraudulent intention: Hacking crime may face civil or criminal liability. If it is done dishonestly or fraudulently then it will face criminal liability; else it will face civil liability.

Cyber Terrorism

Newly inserted Section 66F in the IT (Amendment) Act, 2008 deals with Cyber Terrorism i.e. one who causes denial of access to computer resources, or has unauthorized access to a computer resource, or introduces a virus, with the intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in any section of the people is deemed to be committing cyber terrorism. If a person has unauthorized access to a computer resource with the intent to breach the security of the state, its sovereignty and integrity, and friendly relations with foreign states, then also he is deemed to be committing cyber terrorism.

Compounding of Offences:

In the IT Act, 2000, provisions were made only for compounding of contraventions and not for offences. The provision for compounding of offences has been made through a new Section 77-A of IT (Amendment) Act, 2008.

Examiner of Electronic Evidence:

The IT (Amendment) Act, 2008 establishes an examiner of electronic evidence to give expert opinion on electronic evidence. The examiner of electronic evidence may help the investigating agencies/or adjudicating officer to investigate the cyber violations/crimes.

Note: New IT (Amendment) Act, 2008 contains 124 sections (but serial number for section is from 1 to 90) instead of 94 sections of previous act, Sections 91 to 94 have been omitted.